

(別紙1) 機能要件一覧 (共通機能要件)

■重要度

S: 必須かつ実現不可の場合、失格

A: 必須

B: 重要

C: 希望

No	大分類	機能要件	重要度
1	1. トップ画面	ログインしたシステム利用者の予定が、スケジュール又は、カレンダーで閲覧できること。	A
2		上記項番1について、責任職は、所属内の全システム利用者のスケジュール又は、カレンダーが閲覧できること。	A
3		お知らせを登録することにより、通知や留意事項などのお知らせが、複数件表示できること。	A
4		継続支援中の児童または家族のいずれかに住民基本台帳の異動が生じた場合、お知らせ事項として表示できること。	A
5		次回対応予定日がシステム利用時の日を基準に過去日となっている場合、お知らせ事項として表示されること。	A
6		上記項番5について、責任職は、所属内の全システム利用者のお知らせ事項が表示できること。	A
7	2. 検索	カナ氏名、漢字氏名、住所、生年月日、電話番号で対象者の検索が行えること。また、複数項目による複合検索ができること。	A
8		カナ氏名検索では清音・濁音の区別なく検索ができること。	C
9		検索する際に、「ゃ」、「や」などの大文字小文字、清音・濁音等の表記ゆれに対応すること。	A
10		前方一致、後方一致等のあいまい検索ができること。	B
11		全ての相談情報、支援記録の文言や添付しているExcelやWordに記入されている文字も含めて全文からフリーワード検索できること。	A
12		検索履歴を表示でき、履歴の一覧から各対象者のページに遷移できること。	B
13	3. CSV出力	CSV出力用の抽出条件及び出力項目をパターン登録して、呼び出しができること。	B
14		児童票情報を担当者ごとや部署ごとにCSVを出力できること。 (例: 担当者Aが〇月〇日から〇月〇日までに処理した通告対応をCSV出力し、処理内容及び件数を把握可能。)	A
15		次回対応予定日から遅延しているケースの一覧がCSV出力できること。	S
16		会議予定日から遅延しているケース一覧がCSV出力できること。	S
17		継続支援中、終結などのステータス状況に応じた児童一覧がCSV出力できること。	A
18		終結後、n年経過等の児童一覧がCSV出力できること。	S
19		相談種別ごとの児童をCSV出力できること。	A
20		会議種別ごとの実施件数や、取り扱い児童数が集計できるCSVを出力できること。	A

No	大分類	機能要件	重要度
21		月ごとに相談受理した対象者一覧がCSV出力できること	A
22		福祉行政報告例の集計の元になるデータがCSV出力できること。	S
23		相談の受付情報の一覧をCSV出力できること。(受付年月日・相談種別・終結状況 等)	A
24		要保護児童等として登録中の児童一覧をCSV出力できること。新規登録日(登録月)・ランク・担当区・年齢・虐待種別・相談経路等の情報が出力できること。	A
25		要保護児童等の管理終了児童の一覧をCSV出力できること。新規登録日(登録月)・ランク・年齢・虐待種別・相談経路等・台帳管理終了日(登録月)等の情報が出力できること。	A
26	4. 住民記録システム連携	住民記録システムとの連携を行い、児童と家族の基本情報の登録ができること。	S
27		住民記録システム連携時に使用する住居宛名検索について、氏名カナの大文字・小文字を区別しない検索ができること。	A
28		相談登録された児童について他の世帯員がいた場合、他の世帯員を個別検索して画面遷移するのではなく、児童管理画面上で対象者を選択でき、各世帯員画面へ遷移できること。	A
29		住民記録システムの情報と世帯情報(住所、世帯員の増減等)で差がある対象者の一覧を確認でき、任意で更新ができること。	A
30		住民基本台帳事務における支援措置対象者は、アラートが表示されること。	S
31	5. 児童等情報	氏名や住所に変更があった対象者について、任意で最新の住民記録システムの情報に一括更新ができること。	A
32		相談のあった児童・保護者の(氏名、通称、郵便番号、住民票の住所地・続柄、居住地、生年月日、性別、本籍地、電話番号、所属、学年、緊急連絡先等)の情報を管理できること。	A
33		市内に住民登録がない場合でも、上記項番32と同様の情報を入力でき、管理できること。	A
34		要保護児童等の場合、登録されていることが児童の個人画面で表示されること。	A
35		市内区役所、各児童相談所間でケース移管が行えること。	S
36		家族の基本情報(続柄、氏名、生年月日、職業、同居の有無等)が入力できること。	A
37		相談のあった児童の生年月日、性別が不明な状態でも登録できること。	A
38		居所不明児童の登録と検索ができること。	A
39		氏名の入力により、自動的にカナが入力されること。	B
40		氏名の漢字について外字に対応できること。	A
41		児童の過去の相談歴の有無が、画面上で確認できること。	S
42		継続支援中の児童以外の世帯員についての過去の相談歴の有無についても、児童の画面上で確認できること。	A
43		既登録済の児童の情報を複製して他の児童の登録を可能とする機能を有すること。	A
44		同一世帯に2人以上の対象児童がいた場合、世帯員一覧の画面から対象児童を選択でき、直接当該世帯員の画面へ遷移できること。	A
45		住所は郵便番号から自動入力できること。	C
46		生年月日を入力すると自動的に現在の年齢と学年が自動で表示できること。	A

No	大分類	機能要件	重要度
47		年齢は、相談受理時の年齢（〇歳〇か月）と、現在の年齢（〇歳〇か月）の両方が管理できること。	A
48		児童氏名（カナ）と生年月日と同じ児童の相談データが既に存在する場合は、自動的にチェックし注意を促すこと。	B
49		世帯員の氏名や住所の変更を履歴管理できること。	A
50		世帯員ごとに備考内容を管理できること。	B
51		住民基本台帳上の世帯員ではない者を、世帯員として管理できること。また、住民基本台帳上での世帯員ではないことが分かるよう区別して表示できること。	A
52		ヤングケアラーの該当有無が管理できること。また、支援の開始日と支援の終了日を管理できること。	C
53		システムのアドオン機能としてジェノグラムを作成できること。	A
54		ジェノグラムの画像ファイルを取り込むことができること。	A
55		ジェノグラムにコメントを貼り付け、図形や線に着色できること。	B
56		ジェノグラムは各種帳票に出力ができること。	A
57		世帯員区分（児童、通告者等）、所属（〇〇保育園、幼稚園等）、学年、小学校区、中学校区、最終学歴、職業等が管理できること。	A
58		新たな管理項目を任意に追加できること。	A
59		児童の進級処理を一括で職員の手動操作でも行えること。	B
60		校区設定により小学校から校区の中学校へ進学させることが一括でできること。	B
61		複数の連絡先情報を登録できること。	B
62		外国人情報として、本名、併記名、通称名、国籍、在留期間、在留資格等の情報を別途管理できること。	A
63		住民基本台帳と現住所が異なる場合、居住区、現住所、本籍地、住民票住所等の管理ができること。	A
64		対応注意の対象者について、任意でアラート設定ができ、その内容が確認できること。	A
65		学校の出欠状況（出席日数、遅刻日数、早退日数、遅早日数、欠席日数、コメント）を月ごとに登録管理できること。	C
66		身長、体重を履歴管理できること。また成長曲線としてグラフ表示できること。	B
67		生活保護世帯の該当有無が表示できること。	A
68		各種障害者手帳の資格情報（資格の有無、手帳記号、手帳番号、種別、主たる障害、等級、交付年月日）を表示できること。	A
69		各種手当（児童手当、児童扶養手当、特別児童扶養手当等）の認定、受給状況を表示できること。	A
70		市民税情報、保育所入所情報を表示できること。	S
71		障害福祉システムの支給決定情報（決定の有無、受給者証番号、内容）が表示できること。	A
72		個別支援記録管理システムの相談記録の有無について表示できること。	A
73		特定妊婦の相談登録ができること。	S

No	大分類	機能要件	重要度
74		健康状態、経済因子、環境因子、個人因子等の情報が登録できること。	A
75		相談のあった児童の家族の生年月日が不明な状態でも登録できること。	A
76		また、身元が判明した場合、紐づけができること。	A
77		住民基本台帳の続柄とは別に、対象者から見た家族の続柄が登録できること。	A
78		家族に対しても福祉サービス、保健情報、備考、添付資料を登録できること。	A
79		同一世帯に2人以上の対象児童がいた場合の家族の氏名や住所の変更は、1回の操作で変更できること。	B
80		児童記録票の情報として、「要保護児童等に関する情報共有システム」における児童記録票第1面～第8面の情報が管理できること。	A
81	6. 統計・帳票等	上記項番79の「要保護児童等に関する情報共有システム」における児童記録票第1面～第8面の情報について、システムと連携する情報を選択できること。	B
82		福祉行政報告例の以下について、集計と印刷ができること。 <ul style="list-style-type: none"> ・第43児童相談経路別児童受付 ・第44児童相談種類別児童受付 ・第45児童相談種類別対応件 ・第46児童相談所における措置停止・措置中等の調査・診断・指導・措置解除 ・第47一時保護児童、第48児童相談所における調査・診断及び心理療法・カウンセリング等 ・第49児童相談所における養護相談の理由別対応件数 ・第49-2市町村における養護相談の理由別対応件数 ・第50児童福祉施設・在所者 ・第52助産施設・母子生活支援施設在所者 ・第56里親及び小規模住居型児童養育事業（ファミリーホーム） ・第57里親及び小規模住居型児童養育事業（ファミリーホーム）に委託されている児童 	S
83		上記項番81の統計情報は各区・各児童相談所ごとに集計ができること。	S
84	7. 相談情報管理	相談情報として、受付年月日、ケース番号、主訴、相談区分、相談種別、相談種別詳細、相談方法、相談経路、相談経路詳細、担当者等を登録できること。	A
85		国が定義する相談種別には該当しないが、フォローが必要なケースを「統計外相談」として選択して登録できること。	A
86		相談区分の選択内容によって、相談種別と詳細の選択肢が自動選択できること。	A
87		相談種別の選択内容によって、入力する必須項目を切り替えることができること。（例：虐待相談の時の必須項目と、虐待以外の必須項目を切り替える 等）	A
88		相談者・通告者の氏名、対象者との関係性、電話番号、住所、今後の協力の可否等の情報が登録できること。	A
89		虐待（通告）内容、主たる虐待者、従たる虐待者、重症度、虐待種別、子どもの状況、通告日時、安全確認情報等の虐待情報が登録できること。	A
90		通告があった場合、「対象者に対する通告内容の告知」を管理できること。（通告者の氏名も含めて可 / 通告者の氏名を隠して可）	A
91		相談登録された対象者について、ステータス管理（支援継続中か終了しているかどうか等）ができること。	A
		同一児童に対する複数の相談を並行して管理できること。	B

No	大分類	機能要件	重要度
92		アセスメント結果（緊急度・重要度・共有ランク表のランク）がドロップリストで登録できること。	A
93		所属や職位に応じて権限設定をして管理することができること。	A
94		既登録済みの相談情報をコピーして登録できること。	A
95		関係機関は種別が選択できること。	A
96		関係機関情報はマスタ管理・参照ができること。	B
97		児童福祉法に定める家庭支援事業について時系列に履歴管理できること。	B
98		相談に関する電子ファイル(画像ファイル（拡張子 gif, jpg, png など）、Word, Excel, PowerPoint, PDF等)を複数管理できること。	A
99		簡易な電話面接や情報提供などの対応内容を登録できること。	A
100		児童のCA情報（居所不明児）を登録・照会できること。	B
101		よこはま虐待ホットライン及び夜間・休日対応の相談票の検索・閲覧・印刷ができること。	A
102		移管情報（移管日及び移管を受けた児童の情報等）の登録ができること	B
103		要保護児童等進行管理台帳に最新状況として世帯状況、実施した支援内容、アセスメント、今後の支援方針、最新ランク・相談種別・虐待者・虐待種別、次回アセスメント時期が記録できること。また、履歴も閲覧できること。	A
104		児童記録票の内容について、要保護児童等進行管理台帳への登録に反映できること	A
105		要保護児童等進行管理台帳は区と児童相談所と共通で使用できること。	S
106		要保護児童等進行管理台帳の一覧を閲覧・出力できること。また、入力条件より検索し、一覧表示できること。	A
107		虐待通告ごとの氏名等の情報、通告内容、対応状況、対応結果等の進捗管理状況を表形式で表示し、管理できること。	A
108	8. 支援記録	支援記録として、「支援日時」「タイトル」「支援方法（訪問・面接等）」「支援場所」「支援内容（フリー入力）」等を任意に設定した相談カテゴリごとに登録できること。	A
109		支援記録については、1件あたり8,000文字程度の保存ができること。	B
110		支援記録は、入力欄にひな形等を使用できること。	C
111		複数の担当者名を選択登録できること。	A
112		支援記録の登録にあたっては、予定と実績が管理できること。	A
113		支援が継続する児童については、次回対応日の登録が漏れない仕組みであること。	A
114		次回対応予定日が過去日であるものを遅延ケースとして検索・抽出できること。	A
115		遅延ケース（次回対応日が過去日であるケース）については、担当者及び責任職に通知される仕組みであること。	A
116		既登録済の支援記録をコピーして登録できること。	A
117		支援記録一覧の出力・印刷ができること。	A
118		きょうだいなどの支援経過を一元的に把握するため、同一世帯内の全員の支援記録を時系列に沿って表示できること	B

No	大分類	機能要件	重要度
119		支援記録に関する電子ファイル(画像ファイル(拡張子 gif, jpg, png など), Word, Excel, PowerPoint, PDF等)を複数管理できること。	A
120		支援記録ごとに、連携した関係機関種別や連携方法が登録できること。	A
121		支援記録は、電子供覧ができること。	S
122		責任職に電子供覧されているとき、トップページに通知が表示されること。	A
123		案件ごとに回議ルートが設定できること。	S
124		支援記録の供覧完了後は原則修正できないが、必要な場合は責任職の許可のもと、実施できる仕組みとすること。	A
125		支援記録と会議情報を一つの画面上で日時順で一覧表示できること。	A
126		障害児の相談記録(野線)に決裁欄(供覧用)を設けること。	A
127		障害児通所支援等の支給決定にかかる帳票を保管できること(PDF等)。	A
128		対象者が特定不可能な場合や、匿名の相談についても登録できること	S
129		住登外で作成していた記録について、住民票の登録が行われた場合はその住民票に転記することができること。	B
130		入力途中の情報の一時保存機能があること。	B
131		各種帳票と支援記録の連携またはコピーが容易にできること	A
132	9. 会議情報	会議情報(開催日、議題、議事録等)の管理ができること。	S
133		会議情報(結果、次回報告日等)が管理できること。	S
134		10種類以上の会議票の作成ができること。	A
135		次回報告日・次回評価日等を元に、会議対応の遅延管理ができること。(上記日程が過去日になっているものを抽出してメニュー画面上で表示する、CSV出力等で対象者を出力する等)	A
136		会議種別(受理会議・個別ケース検討会議・判定会議・援助方針会議・弁護士検討会・ケース検討会議・定期的アセスメント・進行管理会議等)ごとに会議票を作成・管理できること(10種類以上を想定)	A
137		会議情報として、「備考」が自由入力できること	B
138		各種会議種別ごとに、対象児童の一覧が画面表示できること。	A
139		開催日ごとに、会議対象者一覧が画面表示できること。	A
140		システム上で会議が進行できるように、会議対象者一覧画面上から、各個人画面に遷移できること。また、各情報が閲覧できること。	A
141		会議に関する電子ファイル(画像ファイル(拡張子 gif, jpg, png など), Word, Excel, PowerPoint, PDF等)を会議情報ごとに、複数管理できること。	A
142		登録した会議結果の修正登録ができること。	A
143		虐待で受理・登録した児童の緊急受理会議の実施の管理(実施の有無表示)ができること。	A
144		受理した(システム登録した)児童の受理会議提出の管理(実施の有無表示)ができること。	A

No	大分類	機能要件	重要度
145		きょうだい児で会議を実施した際、結果等を一方の児に入力したときに、もう一方の児の記録や会議票にも自動もしくは簡易に反映させることができること。	A
146		会議の参加者を定型文やチェックボックス機能等を用いて、簡易に登録できること。	A
147	10. 他システム連携	こども家庭庁の情報共有システムに連携可能な情報を出力できること。	A
148		こども家庭庁の情報共有システムにて採番された対象者番号を取り込むことができること。	A
149		こども家庭庁の情報共有システムにて連携に必要な管理項目については、必須項目の設定や、データ形式の制限等によって、連携エラーが防げる工夫があること。	A
150		関連システムと情報連携ができること(記録の取込を含む)	S
151		「国の要保護児童等に関する情報共有システム」との情報連携は、主担当の区ごとのCSVと児童相談所ごとのCSV出力されること。	A
152		こども家庭庁にて実装予定の「児童相談所におけるAIを活用した緊急性の判断に資する全国統一のツール」への連携する仕組みを備えること。	A
153		司法審査や戸籍調査等を実施する際、登録データから必要な情報を、帳票に出力できる機能があること。	B
154	11. 担当者	担当者情報はマスタ管理できること。	A
155		担当者、担当SVの一括変更及び個別変更ができること。 また、現在担当しているケースを一覧で確認できること	A
156		主担当者、副担当者、担当弁護士、一時保護担当者などの担当者の登録ができること。	A
157	12. その他	入力中に別児童の照会があった場合に照会用画面の展開もできるなど、一つのIDで二画面同時展開が可能で別の操作ができること。	C
158		制度改正・法改正等に対応可能なシステムであること。	A
159		相談情報、支援記録、一時保護情報、会議情報等について、年数や履歴数の制限なく管理できること。	B
160		業務手引きや様式集などのシステム利用者全員で共有したいファイルをシステム(ヘルプ画面等)より随時ダウンロードできること。	B
161		全ての画面から直接ログアウトできること。	B
162		ドロップダウン入力や参照入力によりキーボード入力量の減少を図っていること。また日付はカレンダーで入力できること。	B
163		日付の入力は和暦で入力できること。また日付の画面表示は和暦で表示し、データ(CSV)出力は「和暦、西暦」の選択ができること。	B
164		必須入力項目については、システム画面で必須であることが明示されていること。	A
165		システム画面の入力可能文字数が『(〇〇文字)』と明示されていること。また、入力作業中に入力済文字数が明示されていること。	A
166		一覧画面については任意の一覧項目により行ソートができること。	B
167		施設・保護者以外にも学校など任意に指定した宛先に通知書を印刷することができること。	B
168		通知書のように送付の必要がある帳票については、窓空き封筒用の住所が印字されること。	B
169		印刷する前にプレビュー画面で印刷内容の確認ができること。	A
170		ページ指定で印刷ができること。	A
171		画面印刷ができること。	A

No	大分類	機能要件	重要度
172		保護者向けの通知書関係の帳票に印字する宛名を複数登録できること	B
173		相談種別や対応結果により定められた廃棄年限について、児童毎に管理し、児童記録の保存年限の管理及び削除ができること。	B
174		作業中の相談記録等に対し、別の職員は閲覧のみで更新ができないようにすること。また、作業中であることを画面に表示することができること。	A
175		システム管理者が操作ログを確認できること。	S
176		決定事項等（相談受理、処理、終結、会議記録、一時保護決定・解除等）について、電子決裁ができること。	A

(別紙1) 機能要件一覧 (こども家庭センター)

■重要度
 S: 必須かつ実現不可の場合、失格
 A: 必須
 B: 重要
 C: 希望

No	大分類	機能要件	重要度
1	5. 児童等情報	児童画面を表示した際に、児童票の起票状況、要保護児童としての登録状況、過去（直近の）情報がわかること。	B
2	6. 統計・帳票等	こども家庭センターにかかる、各種帳票がシステムから出力できること。	A
3		こども家庭センター業務に関する統計が作成、出力できること	A
4		こども家庭相談で受けた相談について、区別に相談受付方法、相談者、対象者、対象者の性別・年齢、相談内容、相談時間、支援内容等の集計、出力できること	A
5		入力済みデータを任意の様式で出力できること。	A
6		7. 相談情報管理	こども家庭相談の内容を記録する際に、「虐待」「障害」など複数選択ができ、市独自の相談区分がドロップリスト（約40項目）で管理できること。 また、相談区分の選択肢はマスタにて修正ができること。 ※国が定義する相談種別とは別
7	こども家庭センターにかかるサポートプランや支援台帳等の情報が管理できること。	S	
8	サポートプラン対象者の選定、作成、手交の進捗状況がシステム上で確認できること	A	
9	育児支援ヘルパーの決定及び通知書の発行、実績入力ができること。	A	
10	女性相談の世帯調査票の作成・閲覧・更新・保管ができること	A	
11	女性相談の記録入力にあたっては職員ごとに権限を設定できること。	S	
12	保護者を対象者とした相談記録の作成ができること（ひとり親支援、女性相談等の支援を想定）	S	
13	女性相談・助産・母子生活支援施設に関連した入所情報（利用制度・施設名・利用期間）を管理できること。	A	
14	母子生活支援施設、助産施設の相談は、母、または妊婦で登録（児童を世帯員として登録）できること。	A	
15	母子生活支援施設、助産施設の相談者の基礎情報（氏名、住所、生年月日等）が様式に印字されること。	A	
16	12. その他	システム上で関係部署間の書類の送付、送付の連絡ができること。	B

17

ケース番号は主担当区ごとに自動採番できること。

A

(別紙1) 機能要件一覧 (児童相談所)

■重要度
 S: 必須かつ実現不可の場合、失格
 A: 必須
 B: 重要
 C: 希望

No	大分類	機能要件	重要度
1	1. 記録等	診断情報 (心理診断・社会診断・行動診断・医学診断) を履歴登録できること。	A
2		各診断の所見が自由入力できること。	A
3		養育支援ヘルパーの決定及び通知書の発行、実績入力ができること。	A
4		児童相談所で共通のケース番号を自動採番できること。	A
5		児童情報の初期表示画面からは、児童の基本情報、過去の受付・対応の経過、一時保護の経過などの履歴が見やすく一覧でき、詳細画面への遷移ができること。	A
6	2. 進捗管理	「ケース取扱状況表」「受付相談表」「在宅児童指導表」「施設入所児童等指導表」「里親等委託児童指導表」を出力できること。	A
7		虐待通告ごとの安全確認者、安全確認時期、ランクなどの進捗管理情報を表形式で表示し、管理できること。	C
8		ログイン後の初期画面等の一定の時期に、以下の注意喚起表示ができること。 ・1ヶ月以内に18歳、20歳を経過 (措置入所・里親委託期間延長中児童) ・一時保護開始7日目、1週間以内に一時保護期間が40日・経過2カ月を経過等	C
9	3. 相談処理業務	福祉行政報告例の集計に沿った対応 (助言指導、継続指導、他機関あっせん、児童福祉司指導、児童福祉施設入所措置、里親委託など) を登録できること。また履歴管理できること。	A
10		措置停止、措置停止解除、措置延長の登録ができること。また履歴管理できること。	A
11		各処理に応じた通知書が出力できること。	A
12		各通知書は過去のものについても再度いつでも印刷ができること。	A
13		当該対応に伴う総合診断 (自由記述、字数上限あり) が入力できること。	C
14		入所時に、住民票を移したかどうか、マイナンバーを受理したかどうか等の入力ができること。	C
15		児童福祉法第28条 (第1項、第2項) の各件数 (請求、承認、却下、取下げ)、親権喪失審判の各件数、親権停止審判の各件数、児童福祉法第33条第1項による一時保護件数及び2か月を超えた件数、同法第33条第5項の件数、少年法第6条の6第1項 (第1号、第2号) の各件数など福祉行政報告例の対象ではない項目について、入力できること	A
16		4. 一時保護業務	一時保護の開始日時、解除日時、一時保護先、同意の有無、同意の確認の有無、職権、保護先の開示、一時保護終了後の経路などが登録できること。また履歴管理できること。
17	一時保護の理由、一時保護解除の理由が登録できること。		A
18	一時保護先変更の登録・処理ができること。		A

No	大分類	機能要件	重要度
19		受診券情報と紐づけができること。	A
20		夜間や休日の所内一時保護開始の場合、児童情報が未入力の新規ケースの場合は、一時保護所が新規に最低限の児童情報を登録できること。また、一時保護決定の入力がなされていないなくとも、一時保護所において暫定的に記録入力でき、後に児童情報と紐づけできること。	A
21		各処理に応じた通知書が出力できること。	A
22		一時保護の2ヶ月超え（同意、家裁申立て）の管理ができること。（一時保護が2か月を超える日が自動計算・表示されること。）	A
23		一時保護状の請求の管理ができること。（一時保護を開始した日から7日目が自動計算・表示されること等。）	A
24		所内における、翌日に向けた引継ぎ情報が登録できること。	A
25		所内における引継ぎ情報は、前日以前の情報が複写できること。	A
26		一時保護開始時の主担当員、心理担当員、医師担当員が登録できること。	C
27		身体情報（身体検査日、身長、体重、既往歴、通院状況等）の登録ができること。	B
28		医務情報（アレルギー情報、服薬情報、受診経過等）の登録ができること。	A
29		一時保護所における毎日の行動記録や、行動観察記録の登録ができること。	A
30		一時保護に関する電子ファイル(画像ファイル(拡張子 gif, jpg, png など), Word, Excel, PowerPoint, PDF等)を複数管理できること。	C
31		委託費用の計算ができ、関係書類の印刷ができること。	A
32		委託費用計算用に、虐待加算の児童を検索でき、検索結果をCSV出力できること。	A
33		一時保護先ごとに対象者を検索でき、検索結果をCSV出力できること。	A
34		一時保護の同意の有無の一覧がCSV出力できること。	A
35		期間を指定して（年度、月毎など）、当該機関の一時保護件数や保護日数等、一時保護情報（相談種別や保護先等）と紐付けて集計、出力ができること	A
36		施設・里親に委託した一時保護児童の情報を一覧でCSV出力できること	A
37	5. 施設入所	入所・委託先の施設、認定状態（措置開始、措置停止、措置変更、措置解除等）の登録ができること。	A
38		入所に伴う、資料が作成できること	A
39		措置先別に一覧をCSV出力できること。	A
40	6. 里親業務	里親の基本情報、家族情報、認定日、更新日、取消日、研修受講歴の登録ができること。	A
41		里親の種別を複数登録できること。	C
42		里親が登録されれば、自動で児童相談における措置先、一時保護委託先、レスパイト先として表示できること。	A

No	大分類	機能要件	重要度
43		里親の勤務先や性格等の特徴が入力できること	B
44		里親の基本情報、里親種別、更新時期などから検索ができること。	A
45		里子の希望（受入期間、年齢、性別、障害受入の可否及び動機等）が登録できること。 なお、ラジオボタンや年齢もリストから選ぶようにして、CSVで吐き出すことを想定した運用ができること。	B
46		里親管理番号が世帯ごとに採番されること	A
47		里親を管理する台帳があること	A
48		里親委託履歴が見られること	A
49		検索結果から里親申請者と里親登録者が区別できること。	C
50		検索結果から児童を受託している里親とそうでない里親の情報を区別できること。	A
51		里親情報の初期表示画面からは、里親の基本情報、支援の経過、委託児童の一覧などの経過が見やすく一覧でき、詳細画面への遷移ができること。	A
52		ファミリーホームの登録ができること。	A
53		委託中ケースのレスパイトを管理できること	A
54		里親に対するヘルパー派遣について、決定及び通知書の発行、実績入力ができること。	A
55		子どもとのマッチングを管理できること	A
56		委託中、一時保護委託中、レスパイト中の児童の氏名、年齢、性別、委託先の里親名、委託開始・解除年月日、委託日数、担当児童相談所（児童・里親）が一覧で確認できること。	A
57		里親に対する支援記録が登録できること。	A
58		職員が作成した電子ファイル（画像ファイル（拡張子 gif, jpg, pngなど）、Word, Excel, PowerPoint, PDF等）を里親に紐づけ、管理できること。	A
59		「里親賠償保険について」の連絡票を出力できること。	C
60		里親の記録を委託児童だけでなく、一時保護委託児童や候補児童の記録と紐づける。また児童と同様、記録に関して過程訪問や電話等詳細なものを記載できること。	A
61		里親一覧を、種別や認定情報で条件指定してCSV出力できること。	A
62	7. 受診券発行業務	一時保護や措置等の対応方針が決定した児童について、定められた様式で受診券が発行できること。	A
63		保護先、施設種別、施設名、保険の種類、保険証番号、保険者名、受診券発効日などが登録できること。	A
64		返納、再発行、作成取消しができ、状況が管理できること。	A
66		受診券交付台帳を作成し、出力できること。	A
67	8. 療育手帳判定業務・心理士業務	療育手帳交付申請に対し、判定結果等の情報を入力し、関係書類を作成できること。	B

No	大分類	機能要件	重要度
68	療育	療育手帳判定書・判定記録・判定結果等がシステム入力できること。	B
69		頻繁に利用する療育手帳判定台帳はCSV出力だけでなく画面上で直接確認できること。	B
70		心理検査の実施状況を及び検査情報の登録が入力できること。	A
72		心理診断については、検査方法によって所見用の定型文が変更できること。	C
73		検査結果に関する電子ファイル（画像ファイル（拡張子gif, jpg, pngなど）Word, Excel, PowerPoint, PDF等）添付ができること。	A
74		児童相談受付 主たる相談種別「障害・知的障害」の細目に応じた定型文を主訴入力欄に反映できること。	B
75		療育手帳判定書の効率的な入力ができ、IQ計算間違いのチェックができること。	C
76		療育手帳に関する帳票（受付件数・処理件数）を必要な項目別に出力できること。対象データを、受付日ベースか処理日ベースかで選択できるようにすること。	A
77		処理日数を自動計算できること。処理日数には土日、祝日及び年末年始（12/29～1/3）を処理日数に含まないこと。	B
78		処理日数などにより進行管理ができること。	B
79	9. 障害児	障害児施設利用契約情報（受付日、支給決定日、入所日、施設名、退所日等）の登録が行えること。	A
80		障害児施設給付費の支給決定処理ができること。	A
81		障害児施設給付費にあたり市民税や扶養情報がリンクされ、計算シートをもとに自動で費用が計算されること。	A
82		重度障害児支援加算等の支給決定処理ができること。	A
83		重度障害児支援加算等の初回・更新決定時期に自動表示される、もしくは決定作業を促すアラートが発動すること。	A
84		重度障害児支援加算等の条件が適用される状況の時に該当の加算の種類が表示される。もしくは、誤った決定作業時にアラートがでること。	A
85		障害者手帳等障害に関する区の決定情報がリンクされていること。	A
86		被虐待児受入加算費の決定処理及び履歴管理ができること。	A
87		要援護通知の決定処理ができること。	B
88	10. 負担金情報管理	入所・委託を行った場合に発生する負担金を決定できること。（階層区分、徴収金月額、認定理由、債務者、適用年月日（適用は原則として適用年月日から6月30日までとする）が登録できること。	A
89		納入方法（納入通知書払い/口座振替）、口座情報を登録できること。	A
90		施設種別等によって、どの徴収金額基準額表で階層認定するか（児童施設（住民税）、障がい施設（住民税））を自動的に識別すること。また、地方税と所得税（旧表）で、どちらの徴収金基準額表により階層認定するか、選択できるようにすること。	A
91		負担金（徴収）の算定基準となる階層、負担金基準額は、入力した税情報を基に自動で算出し、徴収金月額は手動で修正もできること。	A
92		負担金の決定にあたっては、扶養義務者ごとに税情報の登録ができること。	A

No	大分類	機能要件	重要度
93		満額児が措置解除された場合、注意喚起表示ができること	C
94		扶養義務者と同一世帯の兄弟姉妹で入所・委託している場合に、満額児、減額児（徴収額を1/10とする取扱い）を設定できること。また、減額児を選択した場合は、自動的に徴収額が1/10として算出すること。	A
95		債務者あてに決定通知書が出力できること。	A
96		負担金見直しのための対象者に対して、一覧表を作成し、出力できること。	B
97		児童相談メニューの保護者住所等の修正に伴い、負担金メニューの債務者データも自動変更すること。	A
98		自立援助ホーム利用の負担金も管理できること。	A
99	11. 債権管理業務	認定情報から対象年月ごとの調定対象者（債務者及び徴収額）の情報を作成できること。	A
100		同一世帯のきょうだいで入所・委託している場合、徴収額を集約し、調定情報を作成できること。	C
101		認定後、適用年月日から6月30日までの間、または、措置解除するまでは、自動的に毎月調定対象者として登録されること。	A
102		月単位の措置停止中は、調定対象者からはずれること。その他、手動で月単位での徴収額の変更、調定の停止ができること。	A
103		横浜市指定の形式で納入通知書、口座振替ごとの調定データを作成できること。	A
104		納入通知書、口座振替ごとの収納情報を消込し、債権管理（調定、収納、督促、催告情報の登録）ができること。	A
105		債務者ごとの債権管理（調定、分納、収納、督促及び催告情報の登録）ができること。	A
106		上記の情報を基に債権管理簿を作成できること。	B
107		一部入金（分納）に対応できること。	A
108		債権管理について、紙による印刷を行わず進行管理ができること。	B
109		自立援助ホーム利用の債権も管理できること。	A
110		決算統計用資料データが作成できること。	A
111	12. その他	よこはま虐待ホットライン（通告日時、平日/休日、所要時間、通報者、児童氏名、性別、年齢、相談種別、虐待種別、虐待者、所管児相、市町村、内容など）の入力ができること。	A
112		夜間・休日対応（通告日時、平日/休日、所要時間、通報者、児童氏名、性別、年齢、相談種別、虐待種別、虐待者、所管児相、市町村、内容など）の入力ができること。	A
113		よこはま虐待ホットライン及び夜間休日対応の入力内容について、各所・各区と共有できること。（共有するものについては、任意で選択できること）	A
114		県警との情報共有のデータをCSV出力できること。	A

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス(指標)	メトリクス説明	クラウド調達時の扱い ¹	利用ガイドの解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと			
									-	*	0	1	2	3	4		5		
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データによりシステムのデータが復旧可能かどうか確認するための項目。 外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す(例:住民基本4情報については、住基ネットの情報がある等)。	○		2	システムの復旧に外部データを利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [-] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そこから抽出したデータによって情報システムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	外部データによりシステムの全データが復旧可能	外部データによりシステムの一部のデータが復旧可能	システムの復旧に外部データを利用できない					【注意事項】 外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。
C.2.3.5	運用・保守性	保守運用	OS等パッチ適用タイミング	OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、サーバー及び端末のOS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは即時に適用する。	○	P29	4	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除外し、定期保守時にパッチを適用するのが一般的と想定。 [-] 外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合(リスクの確認がとれている場合)。	仕様の対象としない	ベンダーによる提案事項	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	緊急性の高いパッチのみ即時に適用し、それ以外は障害対応時等適切なタイミングで適用を行う	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチがリリースされるたびに適用を行う	【注意事項】 リリースされるパッチの種類(個別パッチ/集合パッチ)によって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること(E.4.3.4)。また、マイナンバー利用事務系のOSについては最新のパッチを速やかに適用すること。 なお、事前検証なくパッチを適用しなければならないというわけではない。	
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 (例) ・情報セキュリティに関する法令 ・地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省) ・その他のガイドライン ・その他のルール	○		1	有り	セキュリティポリシー等を順守する必要があることを想定。 [-] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。	
E.2.1.1	セキュリティ	セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○		1	重要度が高い資産を扱う範囲	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [-] 重要情報の漏洩等の脅威が存在しない(あるいは許容する)場合 [+] 情報の移動や状態の変化が大きい場合	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲	対象全体				【レベル1】 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める(重要度が最高位のものと等)。	
E.4.3.4	セキュリティ	セキュリティリスク管理	ウイルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウイルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	P30	2	定義ファイルリリース時に実施	ウイルス定義ファイルは、ファイルが公開されるとシステムに自動的に適用されることを想定。 [-] ウイルス定義ファイルが、自動的に適用できない場合(例えばインターネットからファイル入手できない場合)。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				【注意事項】 事前検証なく定義ファイルを適用しなければならないというわけではない。 最新のウイルス定義ファイル適用時に、ウイルス検索エンジンのアップデートも検討すること。	
E.5.1.1	セキュリティ	アクセス・利用制限	管理権限を持つ主体の認証	資産を利用する主体(利用者や機器等)を識別するための認証を実施するか、また、どの程度実施するかを確認するための項目。 複数回、異なる方式による認証を実施することにより、不正アクセスに対する抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生体認証等がある。	○	P31	3	複数回、異なる方式による認証	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。 認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。 機器等(データ連携サーバ等)は多要素認証の対象としない。	

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス(指標)	メトリクス説明	クラウド調達時の扱い ¹	利用ガイドの解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと				
									-	*	0	1	2	3	4		5			
E.5.2.1	セキュリティ	アクセス・利用制限	システム上の対策における操作制限	認証された主体(利用者や機器など)に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例)ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○		1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する。 [-] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	不正なソフトウェアがインストールされる、不要なアクセス経路(ポート等)を利用可能にしている等により、情報漏洩の脅威が現実のものになってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 (操作を制限することにより利便性や、可用性に影響する可能性がある)	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する。							【注意事項】 利用者に応じて適切に、実行可能なプログラム、コマンド操作、アクセス可能なファイルを設定・管理すること。
E.6.1.1	セキュリティ	データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。	○	P31	2	重要情報を暗号化	インターネットに直接接続せず、内部ネットワークのみに接続する情報を想定。	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化					【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。 ガバメントクラウド及びISMAPクラウドサービスリストに登録されているクラウドサービスについては、ISMAPの認証の過程で通信のセキュリティ対策の実施を確認しているため、クラウドサービス内の伝送データの暗号化は必須ではない。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 (CRYPTREC暗号リスト: http://www.cryptrec.go.jp/list.html)。
E.6.1.2	セキュリティ	データの秘匿	蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○	P32	3	すべてのデータを暗号化	蓄積するデータについては、第三者に漏洩しないようすべてのデータの暗号化を実施する。	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化					【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 (CRYPTREC暗号リスト: http://www.cryptrec.go.jp/list.html)。 システム利用開始時点からの全データを暗号化すること。
E.7.1.1	セキュリティ	不正追跡・監視	ログの取得	不正を検知するために、監視のための記録(ログ)を取得するかどうかの項目。 なお、どのようなログを取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。	○		1	必要なログを取得する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する							【注意事項】 取得対象のログは、不正な操作等を検出するための以下のようものを意味している。 ・ログイン/ログアウト履歴(成功/失敗) ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ等

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時 の扱い ¹	利用ガ イドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと			
									-	*	0	1	2	3	4		5		
E.7.1.3	セキュリティ	不正追跡・ 監視	不正監視対 象(装置)	サーバ、ストレージ、ネットワーク機器、端末等 への不正アクセス等の監視のために、ログを取 得する範囲を確認する。 不正行為を検知するために実施する。	○		1	重要度が 高い資産 を扱う範 囲	脅威が発生した際に、それらを検知 し、その後の対策を迅速に実施する ために、監視対象とするサーバ、ス トレージ、ネットワーク機器、端末等 の範囲を定めておく必要がある。	仕様の対 象としない	ベンダーに よる提案 事項	無し	重要度が 高い資産 を扱う範囲	システム 全体					
E.10.1.1	セキュリティ	Web対策	セキュアコー ディング、Web サーバの設 定等による対 策の強化	Webアプリケーション特有の脅威、脆弱性に関 する対策を実施するかを確認するための項目。 Webシステムが攻撃される事例が増加してお り、Webシステムを構築する際には、セキュア コーディング、Webサーバの設定等による対策 の実施を検討する必要がある。	○	P32	1	対策の強 化	オープン系の情報システムにおい て、データベース等に格納されてい る重要情報の漏洩、利用者への成 りすまし等の脅威に対抗するた めに、Webサーバに対する対策を実施 する必要がある。 [-] インターネットに接続したWebア プリケーションを用いない場合	仕様の対 象としない	ベンダーに よる提案 事項	無し	対策の強 化						
E.10.1.2	セキュリティ	Web対策	WAFの導入 の有無	Webアプリケーション特有の脅威、脆弱性に関 する対策を実施するかを確認するための項目。 WAFとは、Web Application Firewallのことであ る。	○	P33	0	無し	インターネットに直接接続せず、内 部ネットワークのみに接続する情報 システムを想定。 [+] インターネットに接続したWebア プリケーションを用いる場合	仕様の対 象としない	ベンダーに よる提案 事項	無し	有り						

1 クラウド調達時の扱い

○:クラウドの対象と成り得る項目 △:クラウドの対象となる場合がある項目 -:通常クラウドの対象とならない項目

なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 利用ガイドの解説

Pxx: 利用ガイドのメトリクス詳細説明ページ

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス(指標)	メトリクス説明	クラウド調達時の扱い ¹	利用ガイドの解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと			
									-	*	0	1	2	3	4		5		
A.1.3.1	可用性	継続性	RPO(目標復旧地点)(業務停止時)	業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	P35	2	1営業日前の時点(日次バックアップからの復旧) [-] データの損失がある程度許容できる場合(復旧対象とするデータ(日次、週次)によりレベルを選定) [+] 選択レベルの時点(1営業日前の時点)での復旧では後追い入力が膨大に発生する等業務への支障が大きいことが明らかである場合	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点(週次バックアップからの復旧)	1営業日前の時点(日次バックアップからの復旧)	障害発生時点(日次バックアップ+一時保存データからの復旧)				【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認(例えば、バックアップ時点まで戻ってしまったデータを手修正する等)は別途ユーザが実施する必要がある。	
A.1.3.2	可用性	継続性	RTO(目標復旧時間)(業務停止時)	業務停止を伴う障害(主にハードウェア・ソフトウェア故障)が発生した際、復旧するまでに要する目標時間。ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P35	2	12時間以内 窓口対応等、システム停止が及ぼす影響が大きい機能の復旧を優先しなるべく早く復旧する。 [-] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、業務への支障が大きいことが明らかである場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内			【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認(例えば、バックアップ時点まで戻ってしまったデータを手修正する等)は別途ユーザが実施する必要がある。 目標復旧時間をSLAに定めていないクラウドサービスを利用する場合は、GSPがSLAで示す稼働率を元に業務停止時間の最大値を算出し、RTOを検討することが考えられる。	
A.1.3.3	可用性	継続性	RLO(目標復旧レベル)(業務停止時)	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル(特定システム機能・すべてのシステム機能)の目標値。ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P36	2	全システム機能の復旧 すべての機能が稼働していないと影響がある場合を想定。 [-] 影響を切り離せる機能がある場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧					【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。(例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。)	
A.1.4.1	可用性	継続性	システム再開目標(大規模災害時)	大規模災害が発生した際、どれ位で復旧させるかの目標。大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	P37	2	一ヶ月以内に再開 電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。また、復旧までの間、バックアップデータから必要なデータをCSV等で自治体が利用できる形式で提供(※)する。 ※住民記録システム等、住民の安全確認に必要なデータを持つシステムについては、発災後72時間以内に、必要なデータを自治体が利用できる形式で提供すること。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開			【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1	可用性	継続性	稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。一般的にサービス利用料と稼働率は比例関係にある。	○	P38	3	99.5% ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、業務への支障が大きいことが明らかである場合 [-] 地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%			【レベル】 稼働時間(バッチ処理等を含む運用時間)を平日のみ1日当たり12時間と想定した場合。 99.99%.....年間累計停止時間17分 99.9%.....年間累計停止時間2.9時間 99.5%.....年間累計停止時間14.5時間 99%.....年間累計停止時間29時間 95%.....年間累計停止時間145時間
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○		1	上限が決まっている 基幹系システムの場合は、業務ごとに特定のユーザが使用することを想定。	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用						
B.1.1.2	性能・拡張性	業務処理量	同時アクセス数	同時アクセス数とは、ある時点で情報システムにアクセスしているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○		1	同時アクセスの上限が決まっている 特定のユーザがアクセスすることを想定。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り						

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと		
									-	*	0	1	2	3	4		5	
B.1.1.3	性能・拡張性	業務処理量	データ量(項目・件数)	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○		0	すべてのデータ件数、データ量が明確である [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ件数、データ量が明確である	主要なデータ件数、データ量のみが明確である						【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民記録システムであれば住民データ・世帯データ・異動データ等がある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。
B.1.1.4	性能・拡張性	業務処理量	オンラインリクエスト件数	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○		0	処理ごとにリクエスト件数が明確である [+] 全部のオンラインリクエスト件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である						【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民記録システムの転入・転出処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。
B.1.1.5	性能・拡張性	業務処理量	バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○		0	処理単位ごとに処理件数が決まっている [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている						【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。
B.2.1.4	性能・拡張性	性能目標値	通常時オンラインレスポンスタイム	オンラインシステム利用時に要求されるレスポンス。システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。(例: Webシステムの参照系/更新系/一覧系など)	○	P39	3	3秒以内 管理対象とする処理の中で、通常時の照会機能などの大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] コストと実現性を確認した上で、業務への支障が大きいことが明らかである場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内			【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。測定方法、調達範囲外の条件(例えばネットワークの状態等)については、ベンダーと協議し詳細を整理する必要がある。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと	
									-	*	0	1	2	3	4		5
B.2.1.5	性能・拡張性	性能目標値	アクセス集中時のオンラインレスポンスタイム	オンラインシステム利用時に要求されるレスポンス。システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。(例: Webシステムの参照系/更新系/一覧系など)	○	P40	2 5秒以内	管理対象とする処理の中で、ピーク時の照会機能などの大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] コストと実現性を確認した上で、業務への支障が大きいことが明らかである場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内	【注意事項】 すべての処理に適用するのではなく、主な処理に適用されるものとする。測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要がある。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。	
B.2.2.1	性能・拡張性	性能目標値	通常時バッチレスポンス順守度合い	バッチシステム利用時に要求されるレスポンス。システム化する対象業務の特性を踏まえ、どの程度のレスポンス(ターンアラウンドタイム)が必要かについて確認する。更に、アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時(※)・ピーク時・縮退運転時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 (例: 日次処理/月次処理/年次処理など) ※「通常時」とは、運用保守期間のうち、繁忙期間(住基業務であれば転入・転出の多い年度末・年度当初、個人住民税業務であれば確定申告時期・当初課税時期等)及び想定量を超える処理が発生した期間を除いた期間をいう。	○		2 再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、エラーが発生するなどして処理結果が不正の場合、再実行できれば良いと想定。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
B.2.2.2	性能・拡張性	性能目標値	アクセス集中時のバッチレスポンス順守度合い	バッチシステム利用時に要求されるレスポンス。システム化する対象業務の特性を踏まえ、どの程度のレスポンス(ターンアラウンドタイム)が必要かについて確認する。更に、アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 (例: 日次処理/月次処理/年次処理など)	○		2 再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時のバッチ処理を実行し、エラーが発生するなどして処理結果が結果が不正の場合、再実行できる余裕があれば良いと想定。ピーク時に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
C.1.1.1	運用・保守性	通常運用	運用時間(平日)	業務主管部門等のエンドユーザが情報システムを主に利用する時間。(サーバを立ち上げている時間とは異なる。)	○	P40	4 24時間利用	開庁時間を定時と想定。 [-] 不定期に利用する情報システムの場合 [+] 定時外も頻繁に利用される場合、頻繁ではないが計画された稼働延長がある場合	仕様の対象としない	ベンダーによる提案事項	規定無し(不定期利用)	定時内での利用(1日8時間程度利用)	繁忙期は定時外も頻繁に利用(1日12時間程度利用)	定時外も頻繁に利用(1日12時間程度利用)	24時間利用	【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。	
C.1.1.2	運用・保守性	通常運用	運用時間(休日等)	休日等(土日/祝祭日/年末年始)に業務主管部門等のエンドユーザが情報システムを主に利用する時間。(サーバを立ち上げている時間とは異なる。)	○	P40	3 24時間利用	休日等の窓口開庁がある場合を想定。 [-] 休日の窓口開庁や休日出勤がない場合 [+] 定時外も頻繁に利用される場合	仕様の対象としない	ベンダーによる提案事項	規定無し(原則利用しない)	定時内での利用(1日8時間程度利用)	定時外も頻繁に利用(1日12時間程度利用)	24時間利用	【注意事項】 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。		

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと		
									-	*	0	1	2	3	4		5	
C.1.2.5	運用・保守性	通常運用	バックアップ 取得間隔	バックアップ取得間隔	○	P41	4	日次で取得 全体バックアップは週次で取得する。しかし、RPO要件である、1日前の状態に戻すためには、毎日差分バックアップを取得しなければならないことを想定。 [-] RPOの要件が[-]される場合 [+] RPOの要件が[+]される場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ		
C.4.3.1	運用・保守性	運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○		2	情報システムの通常運用と保守運用のマニュアルを提供する [-] 通常運用に必要なオペレーションのみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する				【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用(起動・停止等)にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業(部品交換やデータ復旧手順等)にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述(系切り替え作業やログ収集作業等)は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。 なお、クラウドサービス上でのメンテナンス(一部サービスの提供終了や廃棄を含む)への対応に関するマニュアルについても想定される。
C.4.5.1	運用・保守性	運用環境	外部システムとの接続有無	情報システムの運用に影響する他システムや外部システム(団体が管理に関与しないシステム)との接続の有無に関する項目。	○		1	他システムと接続する 庁内基幹系システムとして、住基と税などのように連携する他システムが存在することを想定。 [-] データのやり取りを行う他システムが存在しない場合 [+] 外部システムに接続して、データのやり取りを行う場合	仕様の対象としない	ベンダーによる提案事項	他システムや外部システムと接続しない	他システムと接続する	外部システムと接続する					【注意事項】 庁外の民間クラウド等で稼働する場合でも、内部ネットワークで接続する場合は庁内のシステムと位置づけること。 また、接続する場合には、そのインターフェース(接続ネットワーク・通信方式・データ形式等)について確認すること。
C.5.2.2	運用・保守性	サポート体制	保守契約(ソフトウェア)の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○		2	アップデート ソフトウェアがバージョンアップした場合に、ベンダーがアップデートすることを想定。 [-] アップデート権を必要としない場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート					
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。(例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。)	○		4	利用の少ない時間帯(夜間など) 業務が比較的少ない時間帯にシステム停止が可能。 [-] 停止を増やす場合	仕様の対象としない	ベンダーによる提案事項	制約無し(必要な期間の停止が可能)	5日以上	5日未満	1日(計画停止日を利用)	利用の少ない時間帯(夜間など)	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。(例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。) その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能を示す。レベル1以上は、システム停止に関わる(業務などの)制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。	

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時の 扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと
									-	*	0	1	2	3	4	
D.3.1.1	移行性	移行対象 (機器)	設備・機器の 移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○	P44	3	移行対象設備・機器のシステム全部を入れ替える 業務アプリケーションも含めた移行がある。 [-] 業務アプリケーション更改が無 い場合 [+] 業務アプリケーションの更改程 度が大きい場合	仕様の対 象としない	ベンダー による提 案事項	移行対象 無し	移行対象 設備・機器 のハード ウェアを 入れ替える	移行対象 設備・機器 のハード ウェア、 OS、ミドル ウェアを 入れ替える	移行対象 設備・機器 のシステム 全部を 入れ替える	移行対象 設備・機器 のシステム 全部を 入れ替えて、さらに 統合化する	【レベル】 移行対象設備・機器が複数あり、移行内容 が異なる場合には、それぞれ合意する こと。
D.4.1.1	移行性	移行対象 (データ)	移行データ量	旧システム上で移行の必要がある業務データの量(プログラム、移行データに含まれるPDF などの電子帳票類を含む)。	○	P45	*	ベンダー による提 案事項	仕様の対 象としない	ベンダー による提 案事項	移行対象 無し	1TB未満	10TB未満	10TB以上		【注意事項】 データベースの使用量をそのまま使用する と、ログデータなど移行には必要のない データも含まれる場合がある。
D.5.1.1	移行性	移行計画	移行のユー ザ/ベンダー 作業分担	移行作業の作業分担。	○		1	ユーザと ベンダー と共同で 実施 移行結果の確認等、一部を自治体 職員が実施する形態を想定。 [+] 標準仕様準拠のシステムから 標準仕様準拠のシステムに移行す る場合	仕様の対 象としない	ベンダー による提 案事項	すべて ユーザ	ユーザと ベンダーと 共同で実 施	すべてベ ンダー		【注意事項】 最終的な移行結果の確認は、レベルに 関係なくユーザが実施する。なお、ユー ザデータを取り扱う際のセキュリティに関 しては、ユーザとベンダーで取り交わしを 行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユー ザ/ベンダーの作業分担を規定すること。 特に移行対象データに関しては、旧シ ステムの移行対象データの調査、移行 データの抽出/変換、本番システムへの 導入/確認、等について、その作業分担 を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合に ついては、既存システムのベンダーと新 規システムのベンダーの役割分担を検 討する必要がある。	
F.1.1.1	システム環 境・エコロ ジー	システム制 約/前提条 件	構築時の制 約条件	構築時の制約となる庁内基準や法令、各地方 自治体の条例などの制約が存在しているかの 項目。 例) ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統 一基準 ・地方公共団体における情報セキュリティポリ シーに関するガイドライン(総務省) ・FISC ・プライバシーマーク ・構築実装場所の制限 など	○		1	制約有り (重要な制 約のみ適 用) 庁内規約などが存在する場合を想 定。 [-] 法や条例の制約を受けない場 合、もしくは業界などの標準や取り 決めなどが無い場合	仕様の対 象としない	ベンダー による提 案事項	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (すべての 制約を適 用)		【注意事項】 情報システムを開発する際に、機密情報 や個人情報等を取り扱う場合がある。こ れらの情報が漏洩するリスクを軽減す るために、プロジェクトでは、情報利用者の 制限、入退室管理の実施、取り扱い情報 の暗号化等の対策が施された開発用環 境を整備する必要がある。 また運用予定地での構築が出来ず、別 地に環境設定作業場所を設けて構築作 業を行った上で運用予定地に搬入しな ければならない場合や、逆に運用予定地 でなければ構築作業が出来ない場合など も制約条件となる。	
F.1.2.1	システム環 境・エコロ ジー	システム制 約/前提条 件	運用時の制 約条件	運用時の制約となる庁内基準や法令、各地方 自治体の条例などの制約が存在しているかの 項目。 例) ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統 一基準 ・地方公共団体における情報セキュリティポリ シーに関するガイドライン(総務省) ・プライバシーマーク ・リモートからの運用の可否 など	○		1	制約有り (重要な制 約のみ適 用) 設置に関して何らかの制限が発生 するセンターやマシンルームを前提 として考慮。ただし条件の調整など が可能な場合を想定。 [+] 設置センターのポリシーや共同 運用など運用に関する方式が制約 となっている場合	仕様の対 象としない	ベンダー による提 案事項	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (すべての 制約を適 用)			

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス(指標)	メトリクス説明	クラウド調達時の扱い ¹⁾	利用ガイドの解説 ²⁾	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと			
									-	*	0	1	2	3	4		5		
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのようなデータ損失に対して対応する必要があるかを示す項目。	○	P50	1	障害発生時のデータ損失防止 [-] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についてコストと実現性を確認した上で業務への支障が起きることは明らかな場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	職員の作業ミスなどによって発生したデータ損失防止						【注意事項】 職員が一度正常に処理したデータについては、回復するデータには含まれない。
C.1.3.1	運用・保守性	通常運用	監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア(業務アプリケーションを含む)に対する監視に関する項目。監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含まない。「E.7.1 不正監視」で別途検討すること。	○	P51	0	監視を行わない 夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [-] 障害時は管理者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] 通常よりも処理が集中されることが予想できパフォーマンス監視が必要な場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	レベル1に加えてエラー監視(トレース情報を含む)を行う	レベル2に加えてエラー監視(トレース情報を含む)を行う	レベル3に加えてリソース監視を行う	レベル4に加えてパフォーマンス監視を行う			【レベル】 死活監視とは、対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報を含む場合は、どのモジュールでエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループットについて判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。 また、定期報告会には、リソース監視結果、パフォーマンス監視結果の報告は必須ではない。
C.5.9.1	運用・保守性	サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の可否。	○		3	四半期に1回 [-] 保守に関する報告事項が予め少ないと想定される場合 [+] 保守に関する報告事項が予め多いと想定される場合	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上			【注意事項】 業務ごとの定期報告会の頻度を指す。また、障害発生時に実施される不定期の報告会は含まない。
C.5.9.2	運用・保守性	サポート体制	報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○		3	障害及び運用状況報告に加えて、改善提案を行う	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う					
C.6.2.1	運用・保守性	その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○	P52	1	ベンダーの既設コールセンターを利用する サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [-] 問い合わせ対応窓口を設置する必要がない場合 [+] コストと実現性を確認した上で、常駐作業員がいないと適切な保守・運用ができないと考えられる場合	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける						【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要がある。
C.6.3.1	運用・保守性	その他の運用管理方針	インシデント管理の実施有無	システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存のインシデント管理のプロセスに従う 運用管理業務のうちインシデントに対する管理として求める内容。 [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する						
C.6.4.1	運用・保守性	その他の運用管理方針	問題管理の実施有無	インシデントの根本原因を追跡するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の問題管理のプロセスに従う 運用管理業務のうち問題管理に対する管理として求める内容。 [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する						

システム非機能要件一覧(別紙2)

項番	大項目	中項目	メトリクス (指標)	メトリクス説明	クラウド 調達時 の扱い ¹	利用ガイ ドの 解説 ²	選択レベル	選択時の条件	レベル							備考 「利用ガイド」第4章も参照のこと			
									-	*	0	1	2	3	4		5		
C.6.5.1	運用・保守性	その他の運用管理方針	構成管理の実施有無	リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の構成管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する						
C.6.6.1	運用・保守性	その他の運用管理方針	変更管理の実施有無	ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存の変更管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する						
C.6.7.1	運用・保守性	その他の運用管理方針	リリース管理の実施有無	承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の実現方法については、有無の確認後に具体化して確認する。	△		1	既存のリリース管理のプロセスに従う [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合(既存のプロセスを見直す場合を含む)	仕様の対象としない	ベンダーによる提案事項	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する						
D.1.1.1	移行性	移行時期	システム移行期間	移行作業開始から本稼働までのシステム移行期間。	○		*	ベンダーによる提案事項 [-] 期間短縮の場合 [+] さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上			
D.1.1.3	移行性	移行時期	並行稼働の有無	移行作業から本稼働までのシステムの並行稼働の有無。	○		0	無し 移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [-] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	仕様の対象としない	ベンダーによる提案事項	無し	有り							【レベル1】 並行稼働有りの場合には、その期間、方法等を規定すること。
E.3.1.2	セキュリティ	セキュリティ診断	Webアプリケーション診断実施の有無	Webアプリケーション診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のこと。	○		*	ベンダーによる提案事項 内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [-] 内部犯を想定する必要がない場合、インターネットに接続したWebアプリケーションを用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施							

「非機能要件の標準」の使用方法について

- ・「非機能要件の標準」の活用シートでは、調達時に定めるべき非機能要件の項目を示しており、項目ごとにあり得るレベル(レベル0から5)を示している。
- ・各開発ベンダ・市町村が調達を行う際には、各項目について「選択時の条件」における「選択レベル」として示されたレベルを使用する。

例) 項番C.1.2.2「運用・保守性」(通常運用)の「外部データの利用可否」については、選択レベル2「システムの復旧に外部データを活用できない」を使用する。
 項番C.2.3.5「運用・保守性」(保守運用)の「OS等パッチ適用タイミング」については、選択レベル4「緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う」を使用する。

利用ガイドは、「非機能要求グレード(地方公共団体版)利用ガイド」(平成26年3月・JLIS作成)のことを指す。

項番	大項目	中項目	マトリクス(指標)	マトリクス説明	クラウド調達時の扱い	利用ガイドの解説 ²⁾	選択レベル	選択時の条件	レベル						備考 「利用ガイド」第4章も参照のこと		
									-	*	0	1	2	3		4	5
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データによりシステムのデータが復旧可能かどうか確認するための項目。 外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す(例:住民基本4情報については、住民基本4情報等)。	○		2	システムの復旧に外部データを利用できない [-] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そこから抽出したデータによって情報システムを復旧できるような場合	様の対応しない	ベンダーによる提案事項	外部データによりシステムの全データが復旧可能	外部データによりシステムの一部のデータが復旧可能	システムの復旧に外部データを利用できない				【注意事項】 外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。
C.2.3.5	運用・保守性	保守運用	OS等パッチ適用タイミング	OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、サーバー及び端末のOS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは即時に適用する。	○	P29	4	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う [-] 外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合(リスクの確認がとれている場合)。	様の対応しない	ベンダーによる提案事項	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	緊急性の高いパッチのみ即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチがリリースされるたひに適用を行う	【注意事項】 リリースされるパッチの種類(個別パッチ/集合パッチ)によって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること(E4.3.4)。 また、マイナーバージョンのOSについては最新のパッチを速やかに適用すること。 なお、事前検証なくパッチを適用しなければならないというわけではない。

各開発ベンダ・市町村が調達を行う際に使用する非機能要件のレベル

[-]は、選択レベルを下げる場合の条件
[+]は、選択レベルを上げる場合の条件を記載している。

別紙3 帳票要件一覧（こども家庭センター）※各種帳票については、Excel、CSVそれぞれで出力できるものとする。

No	帳票名	概要・備考	重要度
1	こども家庭支援課 相談・通告受付票	相談・通告を受けたケースに関する基本情報(児童・家族情報)や相談経路、相談履歴、通告者情報、通告内容等をまとめたもの。(※記録システム管理の場合は不要)	C. できれば欲しい帳票
2	児童虐待通告受付票	通告を受けたケースに関する基本情報(児童・家族情報)や相談経路、相談履歴、通告者情報、通告内容等をまとめたもの。(※記録システム管理の場合は不要)	C. できれば欲しい帳票
3	児童記録票	相談・通告を受けた児童に関する基本情報や、児童票の受理・処理内容をまとめた児童のフェイスシート。	A. 必須の帳票
4	支援記録	支援記録の一覧表。 ※経過記録情報と会議情報の両方を時系列に並べて出力する。 ※経過記録のみ、会議情報のみの出力も想定される。	A. 必須の帳票
5	各会議対象者一覧表	各会議(受理会議・ケース検討会議・進行管理会議)の対象者について、実施年月日毎に1人1行で児童情報を一覧表示したもの。 会議実施前の準備の際に使用する想定。	A. 必須の帳票
6	各会議録	各会議(受理会議・ケース検討会議・個別ケース検討会議)の会議票。 会議前に入力した情報を印刷して会議の手持ち資料として準備する。会議後にはシステムに結果を入力して、必要があれば、完成した帳票(結果が印字)を出力できる。	A. 必須の帳票
7	要保護児童等進行管理台帳	要保護児童等として登録している児童の基礎情報、最新状況、区福祉保健センター・児童相談所の支援状況・アセスメント、進行管理会議の会議結果の記載された台帳。 印刷時点の家族構成、状況などを記載した個人票(フェイスシート)の出力、直近の上記支援状況を記載した個人票の出力、要保護児童等進行管理会議対象者一覧の台帳が出力できる。また、会議対象者一覧については担当ごと等出力ができる。	A. 必須の帳票
8	要保護児童等進行管理台帳 保育所・幼稚園等施設別一覧	要保護児童等として登録している児童について、子ども・子育て支援システムに登録のある、保育所等の機関別リストが作成できる。保育園訪問等の際に用いる。	A. 必須の帳票
9	要保護児童等進行管理台帳 学校別一覧	要保護児童等として登録している児童の学校情報ををもとに、学校ごとの児童リストが作成できる。学校との定期的な情報共有や学校訪問の際に用いる。	A. 必須の帳票
10	虐待防止連絡票等	児童相談所と各区こども家庭支援課間でケースを送致する際に使用する様式。また、関係機関からの通告後の報告に使用する様式。	A. 必須の帳票
11	要保護児童等の転居に伴うケース移管について(要保護・要支援児童用・特定妊婦用)	移管時に使用する様式。	A. 必須の帳票
12	ケース移管・情報提供票	移管時に使用する様式。	A. 必須の帳票
13	要保護児童等の転居に伴う情報提供について(依頼)	転入ケースの情報提供依頼時に使用する様式。	A. 必須の帳票
14	要保護児童等の転居に伴う情報提供について(回答)	転出ケースの情報提供依頼に回答する際に使用する様式。	A. 必須の帳票
15	特定妊婦の支援に関する帳票	特定妊婦の支援で活用する様式。「初期調査シート(特定妊婦用)」「赤ちゃんを迎える準備シート」「特定妊婦支援確認シート」「妊娠期アセスメントシート」	B. 必須ではないが、重要
16	宛名(送付票)	児童の保護者等に資料を送付する際に使用する宛名帳票(送付物)。 ※ラベルシールではなく、A4普通紙に印刷して通知書等と同封する想定	D. 現在使用していない。なくても問題はない。
17	こども家庭相談票		A. 必須の帳票
18	こども家庭相談統計	市の独自統計	B. 必須ではないが、重要
19	こども家庭カンファレンス統計	市の独自統計	B. 必須ではないが、重要
20	こども家庭支援協議頭紙	市の独自様式	A. 必須の帳票
21	社会福祉職協議頭紙	市の独自様式	A. 必須の帳票
22	女性福祉相談協議頭紙	市の独自様式	
23	第4-3 児童相談経路別児童受付	福祉行政報告例	A. 必須の帳票
24	第4-4 児童相談種類別児童受付	福祉行政報告例	A. 必須の帳票
25	第4-5 児童相談種類別対応件数	福祉行政報告例	A. 必須の帳票
26	第4-9-2 市町村における養護相談の理由別対応件数	福祉行政報告例	A. 必須の帳票
27	サポートプラン	こども家庭センターにて使用	A. 必須の帳票
28	こどもサポートプラン	セルフプラン(保護者作成)	D. 現在使用していない。なくても問題はない。
29	障害児通所給付費 支給(変更)申請兼利用者負担額減額・免除等(変更)申請書		D. 現在使用していない。なくても問題はない。

No	帳票名	概要・備考	重要度
30	就学児サポート調査票【放課後等デイサービス】	加算の認定に必要な書類(保護者作成)	D. 現在使用していない。なくても問題はない。
31	在宅援助記録票		A. 必須の帳票
32	女性福祉相談票	フェイスシートと罫線記録で構成。罫線記録は「4」と同様で可。	A. 必須の帳票
33	「配偶者からの暴力の被害者の来所相談に関する証明書」の発行について		B. 必須ではないが、重要
34	配偶者からの暴力の被害者の来所相談に関する証明書【健康保険】		B. 必須ではないが、重要
35	配偶者からの暴力の被害者の来所相談に関する証明書【年金】		B. 必須ではないが、重要
36	配偶者からの暴力の被害者の来所相談に関する証明書【就労支援】		B. 必須ではないが、重要
37	配偶者からの暴力の被害者の来所相談に関する証明書【児童手当】		B. 必須ではないが、重要
38	配偶者からの暴力の被害者の来所相談に関する証明書【その他】		B. 必須ではないが、重要
39	相談記録票(第4号様式)	女性相談の各種証明書を作成するのに必要な様式	B. 必須ではないが、重要
40	配偶者からの暴力の被害者の来所相談に関する証明書【給付金】		B. 必須ではないが、重要
41	配偶者からの暴力の被害者の来所相談に関する証明書【雇用保険】		B. 必須ではないが、重要
42	住民基本台帳事務における支援措置申出書に係る確認書		B. 必須ではないが、重要
43	公営住宅への入居等に関する配偶者暴力被害申出受理確認書		B. 必須ではないが、重要
44	索引簿		A. 必須の帳票
45	女性福祉相談受付簿(日報)		A. 必須の帳票
46	女性福祉相談受付簿(月報) (第36表37表福祉行政報告例※横浜市独自も含む)	福祉行政報告例	A. 必須の帳票
47	一時保護依頼書		A. 必須の帳票
48	入所連絡票		A. 必須の帳票
49	支援依頼書(第2号様式)【一時宿泊】		B. 必須ではないが、重要
50	支援依頼連絡票(第3号様式)【一時宿泊】		B. 必須ではないが、重要
51	横浜市DV相談支援センター連絡票		A. 必須の帳票
52	母子生活支援施設入所申込世帯調査票	本市独自の様式。世帯の基礎情報が連携できると良い。	B. 必須ではないが、重要
53	母子生活支援施設緊急一時保護世帯調査票(第2号様式)		B. 必須ではないが、重要
54	母子生活支援施設緊急一時保護依頼書(第3号様式)		B. 必須ではないが、重要
55	母子生活支援施設緊急一時保護開始通知書(第4号様式)		B. 必須ではないが、重要
56	母子生活支援施設緊急一時保護却下通知書(第5号様式)		B. 必須ではないが、重要
57	母子生活支援施設緊急一時保護生活資金支給依頼書(第7号様式)		B. 必須ではないが、重要
58	母子生活支援施設緊急一時保護生活資金支給開始通知書(第8号様式)		B. 必須ではないが、重要
59	母子生活支援施設緊急一時保護入所世帯連絡票(第11号様式)		B. 必須ではないが、重要
60	母子生活支援施設緊急一時保護(妊娠期支援事業)調査票		B. 必須ではないが、重要
61	母体の健康・生活習慣等の情報記録		B. 必須ではないが、重要
62	訪問指導者派遣依頼書(妊娠期・第1号様式)		B. 必須ではないが、重要
63	訪問指導者派遣決定通知書(妊娠期・第2号様式)		B. 必須ではないが、重要
64	訪問指導者派遣依頼通知書(妊娠期・第3号様式)		B. 必須ではないが、重要

No	帳票名	概要・備考	重要度
65	児童家庭センター 帳票		B. 必須ではないが、重要
66	18歳到達予定者名簿	18歳に到達予定の者の一覧	A. 必須の帳票
67	児童記録票 未処理児童名簿	処理が完了していない状態の児童の一覧表	B. 必須ではないが、重要
68	住記異動リスト	住基異動をした対象児童・世帯員をまとめたリスト	A. 必須の帳票
69	要保護児童等に関する各種集計表	<ul style="list-style-type: none"> ○ランク別・年齢別集計表(ランク別年齢別のクロス集計表、全市・区ごと) ○ランク別・区別集計表(ランク別区別集計、全市) ○ランク別・虐待種別別集計表(ランク別虐待種別別のクロス集計表、全市・区ごと) ○ランク別・経路別集計表(ランク別経路別のクロス集計表、全市・区ごと) ○ランク別・把握動機別集計表(ランク別把握動機別のクロス集計表、全市・区ごと) 	A. 必須の帳票

別紙3 帳票要件一覧（児童相談所）

No	帳票名	概要・備考	重要度
1	児童票	措置経過を管理する文書	A. 必須の帳票
2	措置決定通知書（保護者）	措置決定した場合の保護者宛ての通知書	A. 必須の帳票
3	措置決定通知書（施設）	措置決定した場合の施設宛ての通知書	A. 必須の帳票
4	受診券	児童が病院にかかる際に、病院に提示するもの	A. 必須の帳票
5	受診券（控え）	受診券の控え	A. 必須の帳票
6	一時保護通知書（施設／委託先）	一時保護決定した場合の施設または一時保護委託先宛ての通知書	A. 必須の帳票
7	一時保護通知書（保護者）	一時保護決定した場合の保護者宛ての通知書	A. 必須の帳票
8	介護人派遣依頼書	一時保護決定し、介護人をお願いする場合の介護人派遣業者宛ての通知書	A. 必須の帳票
9	一時保護児童記録票	一時保護した児童の諸情報を記載したファイル形式の文書	A. 必須の帳票
10	一時保護解除通知書（施設／委託先）	一時保護の解除決定した場合の施設または一時保護委託先宛ての通知書	A. 必須の帳票
11	一時保護解除通知書（保護者）	一時保護の解除決定した場合の保護者宛ての通知書	A. 必須の帳票
12	介護人派遣終了依頼書	一時保護の解除決定し、介護人をお願いしていた場合の介護人派遣業者宛ての通知書	A. 必須の帳票
13	措置解除通知書（保護者）	措置解除が決定した場合の保護者宛ての通知書	A. 必須の帳票
14	措置解除通知書（施設）	措置解除が決定した場合の施設宛ての通知書	A. 必須の帳票
15	受診券未返却リスト	未返却の受診券の一覧表	C. できれば欲しい帳票
16	受診券発行済リスト	発行した受診券の一覧表	C. できれば欲しい帳票
17	措置延長通知書（保護者）	措置延長が決定した場合の保護者宛ての通知書	A. 必須の帳票

No	帳票名	概要・備考	重要度
18	措置延長通知書（施設）	措置延長が決定した場合の施設宛ての通知書	A. 必須の帳票
19	措置変更通知書（保護者）	措置変更が決定した場合の保護者宛ての通知書	A. 必須の帳票
20	措置停止通知書（保護者）	措置停止が決定した場合の保護者宛ての通知書	A. 必須の帳票
21	措置停止通知書（施設）	措置停止が決定した場合の施設宛ての通知書	A. 必須の帳票
22	措置停止の解除通知書（保護者）	措置停止を解除した場合の保護者宛ての通知書	A. 必須の帳票
23	措置停止の解除通知書（施設）	措置停止を解除した場合の施設宛ての通知書	A. 必須の帳票
24	児相変更通知（施設）	移管が決定した場合の施設宛ての通知書	A. 必須の帳票
25	児相変更通知（保護者）	移管が決定した場合の保護者宛ての通知書	C. できれば欲しい帳票
26	一時保護指令台帳	一時保護を行った児童、保護者等の一覧表	A. 必須の帳票
27	第43：児童相談経路別児童受付	国への報告書（福祉行政報告例）	A. 必須の帳票
28	第44：児童相談種別別児童受付	国への報告書（福祉行政報告例）	A. 必須の帳票
29	第45：児童相談種類別対応件数	国への報告書（福祉行政報告例）	A. 必須の帳票
30	第46：児童相談所における措置停止・措置中等の調査・診断・指導・措置解除	国への報告書（福祉行政報告例）	A. 必須の帳票
31	第47：一時保護児童	国への報告書（福祉行政報告例）	A. 必須の帳票
32	第48：児童相談所における調査・診断及び心理療法・カウンセリング等	国への報告書（福祉行政報告例）	A. 必須の帳票
33	第49：児童相談所における養護相談の理由別対応件数	国への報告書（福祉行政報告例）	A. 必須の帳票
34	第50：児童福祉施設・在所者	国への報告書（福祉行政報告例）	A. 必須の帳票
35	第56：里親及び小規模住居型児童養育事業（ファミリーホーム）	国への報告書（福祉行政報告例）	A. 必須の帳票

No	帳票名	概要・備考	重要度
36	第57：里親及び小規模住居型児童養育事業（ファミリーホーム）に委託されている児童	国への報告書（福祉行政報告例）	A. 必須の帳票
37	施設別在籍児童一覧	指定日当日の施設在籍児童の一覧表	A. 必須の帳票
38	未処理児童名簿	処理していない状態の児童の一覧表	B. 必須ではないが、重要
39	当月翌月1日入所児童名簿	当該月に入所した（予定を含む）、または翌月1日に入所予定の児童の一覧表	A. 必須の帳票
40	当月翌月1日退所児童名簿	当該月に退所した（予定を含む）、または翌月1日に退所予定の児童の一覧表	A. 必須の帳票
41	施設措置 入所指令台帳	措置決定、措置変更により入所した児童、保護者等の一覧表	C. できれば欲しい帳票
42	施設措置 退所指令台帳	措置解除、措置変更により退所した児童、保護者等の一覧表	C. できれば欲しい帳票
43	施設措置 停止・停止の解除・延長指令台帳	措置停止・停止の解除、措置延長を行った児童、保護者等の一覧表	C. できれば欲しい帳票
44	在宅障害児緊急一時保護実施台帳	緊急一時保護対象者の一覧表	C. できれば欲しい帳票
45	被虐待児緊急一時保護実施台帳	介護人を付けた一時保護の月毎の実績報告書	C. できれば欲しい帳票
46	児童入所支度被服請求及び領収報告書	被服の貸与に関する書類	A. 必須の帳票
47	児童票台帳情報	児童票台帳情報データをダウンロードしたもの	B. 必須ではないが、重要
48	一時保護情報	一時保護情報データをダウンロードしたもの	B. 必須ではないが、重要
49	電話相談情報	電話相談情報データをダウンロードしたもの	B. 必須ではないが、重要
50	虐待ホットライン情報	虐待ホットライン情報データをダウンロードしたもの	A. 必須の帳票
51	虐待対応専門員情報	虐待対応専門員情報データをダウンロードしたもの	A. 必須の帳票
52	児童記録票（施設入所用）	児童に関する諸情報が記載されており、施設で保管するもの（施設入所用）	A. 必須の帳票
53	児童記録票（乳児院33条）	児童に関する諸情報が記載されており、施設で保管するもの（乳児院33条）	A. 必須の帳票
54	児童記録票（乳児院以外33条）	児童に関する諸情報が記載されており、施設で保管するもの（乳児院以外33条）	A. 必須の帳票
55	児童記録票（里親委託用）	児童に関する諸情報が記載されており、施設で保管するもの（里親委託用）	A. 必須の帳票
56	障害児童記録票	児童に関する諸情報が記載されており、施設で保管するもの（障害児童用）	A. 必須の帳票
57	重度・重複障害（者）記録票	児童に関する諸情報が記載されており、施設で保管するもの（重度・重複障害（者）用）	A. 必須の帳票

No	帳票名	概要・備考	重要度
58	児童自立生活援助実施承諾書	児童自立生活援助の実施を承認した場合の申込者宛ての通知書	A. 必須の帳票
59	児童自立生活援助実施不承諾通知書	児童自立生活援助の実施を却下した場合の申込者宛ての通知書	A. 必須の帳票
60	児童自立生活援助実施解除通知書	児童自立生活援助の実施を解除した場合の申込者宛ての通知書	A. 必須の帳票
61	電話相談児童票	電話相談情報を画面から入力した内容を印字する	A. 必須の帳票
62	虐待ホットライン通報受付票	虐待ホットライン情報を画面から入力した内容を印字する	A. 必須の帳票
63	措置証明書	児童が施設に入所、又は里親に委託されていることを証明する書類	A. 必須の帳票
64	一時保護委託費請求書データ	一時保護請求書を作成する為のデータ	A. 必須の帳票
65	施設入退所等統計	施設種別毎の在籍、異動児童の集計帳票	A. 必須の帳票
66	在籍児童異動報告	施設毎の在籍、異動児童の集計帳票	A. 必須の帳票
67	電話相談年報	電話相談を年齢男女毎、相談種別毎で集計した統計	A. 必須の帳票
68	里親委託児童の指導について（依頼）	里親委託児童の指導を他の児相に依頼する際の通知書	C. できれば欲しい帳票
69	勘案事項整理票	利用者の状況を整理したもの	A. 必須の帳票
70	措置変更通知書（施設）	措置変更が決定した場合の変更前施設宛ての通知書	A. 必須の帳票
71	虐待対応専門員受付票	虐待対応専門員情報を画面から入力した内容を印字する	A. 必須の帳票
72	児童自立生活援助実施承諾書（施設宛）	児童自立生活援助の実施を承認した場合の施設宛ての通知書	A. 必須の帳票
73	児童自立生活援助実施解除通知書（施設宛）	児童自立生活援助の実施を解除した場合の施設宛ての通知書	A. 必須の帳票

No	帳票名	概要・備考	重要度
74	措置変更通知書（保護者）	2号指導から3号措置による措置変更が決定した場合の保護者宛ての通知書	A. 必須の帳票
75	フレンドホーム登録書	登録決定した場合のフレンドホーム登録申込者への通知書	A. 必須の帳票
76	フレンドホーム却下通知書	フレンドホーム登録申込を却下した場合の通知書	A. 必須の帳票
77	フレンドホーム登録終了書	フレンドホームの取消決定した場合のフレンドホーム宛ての通知書	A. 必須の帳票
78	フレンドホーム依頼候補児童名簿	次年度実施予定の児童の確認作業で使用する児童の一覧表	C. できれば欲しい帳票
79	依頼書	フレンドホームに対し、依頼する児童を連絡する文書	A. 必須の帳票
80	承諾書	フレンドホームが依頼を受けることを見相に連絡する文書	A. 必須の帳票
81	フレンドホーム・依頼児童について（通知）	決定した組合せを施設に報告するための名簿	A. 必須の帳票
82	フレンドホーム登録更新意向書	3年経過したフレンドホームに更新するかどうかの確認で使用する文書	C. できれば欲しい帳票
83	フレンドホーム登録更新書	登録更新した場合のフレンドホーム更新希望者への通知書	A. 必須の帳票
84	依頼終了書	年度途中で諸事情により依頼を終了する際のフレンドホーム宛の通知書	A. 必須の帳票
85	フレンドホーム台帳	組合せ結果の照会や汎用帳票を作成するためのリスト	A. 必須の帳票
86	フレンドホーム統計報告	児相毎のフレンドホーム数と児童依頼数の集計表	C. できれば欲しい帳票
87	横浜市里親研修施設実習受入依頼書	施設に提出する研修依頼書	A. 必須の帳票
88	施設実習のご案内	里親申請者宛の決定した研修先（施設）の通知書	A. 必須の帳票
89	里親家庭票	家庭状況などを記入する文書	B. 必須ではないが、重要
90	横浜市児童福祉審議会里親部会審議資料	里親部会審議資料作成のための基礎情報	C. できれば欲しい帳票
91	里親部会審議資料	児福審の会議資料	C. できれば欲しい帳票

No	帳票名	概要・備考	重要度
92	横浜市里親認定書	里親認定した場合の通知書	A. 必須の帳票
93	横浜市里親登録決定通知書	里親登録した場合の通知書	A. 必須の帳票
94	横浜市里親申請却下通知書	里親申請の却下決定した場合の里親宛ての通知書	A. 必須の帳票
95	里親更新対象者名簿	里親更新対象者の名簿	A. 必須の帳票
96	里親登録の更新について（通知）	児相に対して更新の可否を通知する文書	A. 必須の帳票
97	横浜市里親登録更新通知書	里親に対して更新の可否を通知する文書	A. 必須の帳票
98	却下通知書（児相宛）	更新に際して却下となった場合の児相宛ての通知書	A. 必須の帳票
99	里親登録更新者名簿	児福審への報告資料（更新者の一覧）	C. できれば欲しい帳票
100	里親認定の取消について（通知）	認定済みの里親の取消決定した場合の児相宛ての通知書	A. 必須の帳票
101	横浜市里親認定取消通知書	認定済みの里親の取消決定した場合の里親宛ての通知書	A. 必須の帳票
102	里親登録の取消について（通知）	登録済みの里親の取消決定した場合の児相宛ての通知書	A. 必須の帳票
103	横浜市里親登録取消通知書	登録済みの里親の取消決定した場合の里親宛ての通知書	A. 必須の帳票
104	委託証明書	里親委託された、または施設入所していることを証明するもの	A. 必須の帳票
105	里親レスパイト・ケア利用決定通知書	里親レスパイト・ケア利用申請に対し、利用可となった場合の通知書	C. できれば欲しい帳票
106	里親レスパイト・ケア依頼書	他の里親や施設に対するレスパイト・ケアによる委託の依頼書	C. できれば欲しい帳票
107	里親・職業指導里親認定台帳	レスパイト・ケアの管理台帳	C. できれば欲しい帳票
108	里親レスパイト・ケア利用却下通知書	里親レスパイト・ケア利用申請に対し、利用不可となった場合の通知書	C. できれば欲しい帳票
109	横浜市里親研修施設実習受入依頼取下書	研修依頼していた施設に対して依頼を取下げた場合の施設宛ての通知書	A. 必須の帳票

No	帳票名	概要・備考	重要度
110	里親更新研修対象者名簿	更新を希望する里親（更新研修を受講すべき里親）のリスト	C. できれば欲しい帳票
111	横浜市里親研修修了証	当該里親研修を修了した場合の証明書	A. 必須の帳票
112	里親研修修了者名簿	当該里親研修を修了した人の一覧（決裁用）	A. 必須の帳票
113	里親名簿	里親とその委託児童の一覧	A. 必須の帳票
114	里親認定について（通知）	児相に対して里親認定者を通知する文書	A. 必須の帳票
115	里親登録について（通知）	児相に対して里親登録者を通知する文書	A. 必須の帳票
116	担当児童相談所の変更について（通知）	里親に対して担当児相変更を通知する文書 ※移管処理時に出力する。	A. 必須の帳票
117	担当児童相談所の変更について（通知）	里親に対して担当児相変更を通知する文書 ※移管処理後、里親管理台帳画面より出力する。（移管先児相用）	A. 必須の帳票
118	里親相談票	里親相談受理情報を出力	A. 必須の帳票
119	里親申請の却下について（通知）	里親申請の却下決定した場合の児相宛ての通知書	A. 必須の帳票
120	児童フェイスシート	虐待ホットラインまたは、受付時に虐待と分かった場合に虐待情報を記載するための個票	C. できれば欲しい帳票
121	受理・判定会議提出票	受理会議、及び判定会議に掛かる児童に関する情報を記載した資料	A. 必須の帳票
122	援助方針・判定会議提出票	援助方針会議、または判定会議に掛かる児童に関する情報を記載した資料	A. 必須の帳票
123	児童虐待防止連絡票	児童相談所と福祉保健センターで児童虐待に関する情報交換を行うための連絡票（児童相談所の様式）	B. 必須ではないが、重要
124	ケース記録	虐待ケースに対して実施した安全確認情報を記載した資料	A. 必須の帳票
125	緊急一時保護申請書	緊急一時保護の利用をするための申込書	A. 必須の帳票
126	緊急一時保護決定通知書	緊急一時保護の利用が決定した対象者に対して、その旨を知らせる通知書（受給者送付用）	A. 必須の帳票
127	緊急一時保護委託決定通知書（施設）	緊急一時保護の利用が決定した対象者の入所施設に対して、その旨を知らせる通知書（施設送付用）	A. 必須の帳票
128	緊急一時保護委託決定通知書（事業者）	緊急一時保護の利用が決定した対象者のサービス事業者に対して、その旨を知らせる通知書（介護人派遣団体送付用）	A. 必須の帳票

No	帳票名	概要・備考	重要度
129	利用者負担額決定内訳表	緊急一時保護の利用が決定した対象者のサービス事業者に対して、利用者負担額の内訳を知らせる書類	A. 必須の帳票
130	利用者負担額決定通知書	決定した利用者負担額について、対象者に知らせる通知書（受給者送付用）	A. 必須の帳票
131	緊急一時保護却下通知書	緊急一時保護の利用が却下となった対象者に対して、その旨を知らせる通知書（受給者送付用）	A. 必須の帳票
132	緊急一時保護取下書	緊急一時保護における申請を取下げの書類	A. 必須の帳票
133	緊急一時保護変更申請書	緊急一時保護の利用の変更をするための申込書	A. 必須の帳票
134	緊急一時保護変更通知書	緊急一時保護の利用の変更が決定した対象者に対して、その旨を知らせる通知書（受給者送付用）	A. 必須の帳票
135	緊急一時保護変更通知書（施設）	緊急一時保護の利用の変更が決定した対象者の入所施設に対して、その旨を知らせる通知書（施設送付用）	A. 必須の帳票
136	緊急一時保護変更通知書（事業者）	緊急一時保護の利用の変更が決定した対象者のサービス事業者に対して、その旨を知らせる通知書（介護人派遣団体送付用）	A. 必須の帳票
137	緊急一時保護辞退届	緊急一時保護の利用の辞退をするための申込書	A. 必須の帳票
138	緊急一時保護決定取消通知書	緊急一時保護の利用の辞退が決定した対象者に対して、その旨を知らせる通知書（受給者送付用）	A. 必須の帳票
139	緊急一時保護決定取消通知書（施設）	緊急一時保護の利用の辞退が決定した対象者の入所施設に対して、その旨を知らせる通知書（施設送付用）	A. 必須の帳票
140	緊急一時保護決定取消通知書（事業者）	緊急一時保護の利用の辞退が決定した対象者のサービス事業者に対して、その旨を知らせる通知書（介護人派遣団体送付用）	A. 必須の帳票
141	対象者一覧	緊急一時保護対象者の一覧	A. 必須の帳票
142	障害児入所受給者証	支給決定により交付	A. 必須の帳票
143	支給決定通知書	支給決定した場合の通知書	A. 必須の帳票
144	支給決定通知書（決議書）	支給決定した場合の通知書	A. 必須の帳票
145	障害児入所医療受給者証	医療型施設の支給決定により交付	A. 必須の帳票
146	却下通知書	各申請に対し却下が決定した場合の通知書	A. 必須の帳票
147	支給決定取消通知書	取消申請に対し決定した場合の通知書	A. 必須の帳票
148	支給決定者一覧表	当該月に支給決定した人の一覧	C. できれば欲しい帳票
149	国基準額（市基準額）適用期間終了予定者一覧表	当該月に適用期間が終了する人の一覧	A. 必須の帳票
150	18歳・20歳年齢到達予定者一覧	当該月に該当年齢に達する人の一覧	B. 必須ではないが、重要
151	在籍統計	在籍統計作成のための基礎データ	A. 必須の帳票
152	年度更新対象者一覧（入所）	入所の年度更新対象者の見相別施設別一覧	A. 必須の帳票
153	支給申請（変更）兼利用者負担額減額・免除等（変更）申請書	年度更新時の20歳未満用の申請書・申告書 印刷業者に一括出力するためのデータ	B. 必須ではないが、重要
154	住記異動リスト	住基異動をした対象児童・世帯員をまとめたリスト	A. 必須の帳票
155	支給決定情報（かながわシステム）	神奈川県国民健康保険団体連合会に送付するための、新規登録分と異動分の支給決定情報データ（かながわシステム用）	A. 必須の帳票
156	支給決定情報（標準システム）	神奈川県国民健康保険団体連合会に送付するための、新規登録分と異動分の支給決定情報データ（標準システム用）	A. 必須の帳票
157	養育支援個人票	現在（印刷出力時）の家族構成、状況などを記載した個人票	A. 必須の帳票

No	帳票名	概要・備考	重要度
158	在宅支援進行管理会議録	現在（印刷出力時）の、区福祉保健センター情報、児童相談所情報、進行管理情報を記載した個人票	A. 必須の帳票
159	在宅支援進行管理会議（養育支援カンファレンス）対象者一覧	カンファレンス対象者を記載するPDF形式で出力する	B. 必須ではないが、重要
160	ランク別・年齢別集計表	ランク別年齢別のクロス集計表（全市・区用）を出力する	A. 必須の帳票
161	ランク別・区別集計表	ランク別区別集計（全市）を出力する	A. 必須の帳票
162	ランク別・虐待種別別集計表	ランク別虐待種別別のクロス集計表（全市・区用）	A. 必須の帳票
163	ランク別・経路別集計表	ランク別経路別のクロス集計表（全市・区用）	A. 必須の帳票
164	ランク別・把握動機別集計表	ランク別把握動機別のクロス集計表（全市・区用）	A. 必須の帳票
165	養育支援台帳（在宅支援進行管理台帳）	在宅支援進行管理台帳に関する情報をEXCEL形式で出力する	A. 必須の帳票
166	養育支援台帳（在宅支援進行管理台帳）	在宅支援進行管理台帳に関する情報をPDF形式で出力する	A. 必須の帳票
167	養育支援台帳（在宅支援進行管理台帳）データ	在宅支援進行管理台帳に関する情報をCSV形式で出力する	A. 必須の帳票
168	要保護児童等進行管理台帳フェイスシート	現在（印刷出力時）の家族構成、状況などを記載した個人票	A. 必須の帳票
169	要保護児童等進行管理台帳（個人票）	現在（印刷出力時）の、区福祉保健センター情報、児童相談所情報、進行管理情報を記載した個人票	A. 必須の帳票
170	個別ケース検討会議提出票／会議録（個人票）	個別ケース検討会議提出票／会議録用に、現在（印刷出力時）の家族構成などを記載した個人票	A. 必須の帳票
171	要保護児童等進行管理会議対象者一覧PDF	要保護児童等進行管理会議対象者をPDF形式で出力する	A. 必須の帳票
172	要保護児童等進行管理会議対象者一覧エクセル（フィルタ）	要保護児童等進行管理会議対象者をEXCEL形式で出力する	A. 必須の帳票
173	要保護児童等進行管理会議対象者（個人票）	現在（印刷出力時）の、区福祉保健センター情報、児童相談所情報を記載した個人票を一括で出力する	A. 必須の帳票
174	要保護児童等進行管理台帳PDF	要保護児童等進行管理台帳の情報をPDF形式で出力する	A. 必須の帳票
175	要保護児童等進行管理台帳（個人票）	現在（印刷出力時）の、区福祉保健センター情報、児童相談所情報、進行管理情報を記載した個人票を一括で出力する	A. 必須の帳票
176	要保護児童等進行管理台帳担当者別一覧	要保護児童等進行管理台帳の情報より、担当者別の一覧表を出力する	A. 必須の帳票
177	要保護児童等進行管理台帳新規登録ケース件数（月次）	把握時ランク別年齢別に、新規登録件数を集計する（全市・区用）	A. 必須の帳票
178	要保護児童等進行管理台帳新規登録ケース一覧	新規登録ケース件数で集計したデータの一覧表を出力する（区用）	A. 必須の帳票
179	要保護児童等進行管理台帳台帳管理終了ケース件数（月次）	台帳管理終了理由別年齢別に、台帳管理終了件数を集計する（全市・区用）	A. 必須の帳票
180	要保護児童等進行管理台帳台帳管理終了ケース一覧	台帳管理終了ケース件数で集計したデータの一覧表を出力する（区用）	A. 必須の帳票

No	帳票名	概要・備考	重要度
181	要保護児童等進行管理台帳 新規登録ケース件数（年次）	把握時ランク別年齢別に、新規登録件数を集計する （全市・区用）	A. 必須の帳票
182	要保護児童等進行管理台帳 台帳管理終了ケース件数（年次）	台帳管理終了理由別年齢別に、台帳管理終了件数を集計する （全市・区用）	A. 必須の帳票
183	要保護児童等進行管理台帳 新規登録ケース件数合計（月次）	把握時ランク別区別に、新規登録件数を集計する （全市用）	A. 必須の帳票
184	要保護児童等進行管理台帳 台帳管理終了ケース件数合計（月次）	台帳管理終了理由別区別に、台帳管理終了件数を集計する （全市用）	B. 必須ではないが、重要
185	要保護児童等進行管理台帳 新規登録ケース件数合計（年次）	把握時ランク別区別に、新規登録件数を集計する （全市用）	B. 必須ではないが、重要
186	要保護児童等進行管理台帳 台帳管理終了ケース件数合計（年次）	台帳管理終了理由別区別に、台帳管理終了件数を集計する （全市用）	B. 必須ではないが、重要
187	要保護児童等進行管理台帳 学校別一覧PDF	要保護児童等進行管理台帳の情報より、学校別の一覧表をPDF形式で出力する	A. 必須の帳票

横浜市情報セキュリティ強化方針

本市では、いまや 160 あまりの情報システムが運用されており、住民記録をはじめとする市民の個人情報や行政運営上重要な情報を多数扱っています。

万一、これらの情報システムが脅威にさらされ個人情報の漏えいなどの事故等が発生すると、市民に多大な影響を及ぼすとともにコンプライアンス上も大きな問題となり、市民の本市への信頼を大きく損なうこととなります。

本市ではこれまで、情報セキュリティ対策として『横浜市情報セキュリティ管理規程』を策定し、この規程に基づき様々な対策を実施してきました。しかし、現状では全庁的なマネジメントの仕組みの確立までには至っておらず、対策が充分であるとはいえません。特に、ソフトウェア資産に関しては、近年、著作権保護を強化する動きや他自治体における不正使用の事例等も起きているにもかかわらず、本市全体として、その管理の仕組みが確立・適用されていません。

これらの現状と課題を踏まえ、次の 3 つの対策に早急に取り組んでいきます。

- 1 情報システムの導入、開発及び運用にあたっては、横浜市個人情報の保護に関する条例、横浜市職員の公正な職務の執行及び適正な行政運営の確保に関する規則、横浜市情報セキュリティ管理規程等を遵守するとともに、手続の明確化と透明性を確保し、安全かつ効率的で満足度の高いシステム構築を行います。
- 2 情報セキュリティ対策とりわけソフトウェアなどの情報資産を適切に管理するために、新たに役割と責任を明確にした管理体制を構築するとともに、全庁的な PDCA のマネジメントサイクルを確立・適用し、必要な啓発・研修を定期的に行います。
- 3 情報システムの運営状況や情報セキュリティ対策の実施状況について、定期的・継続的に監査等を行い、対策の有効性を検討し、改善に努めます。

平成 22 年 6 月 25 日

横浜市長 林 文子

横浜市サイバーセキュリティ強化方針

今日、インターネットその他の高度情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、これらの整備及び情報通信技術の活用の進展に伴って世界的規模でサイバーセキュリティに対する脅威が生じている。

不正アクセスや新たな攻撃手法といった、これら脅威から、個人情報への漏えいや情報資産の破壊・改ざんの被害を発生させず、情報資産の機密性、完全性及び可用性の維持を確保することが、本市の喫緊の課題となっている。

本市は、市民の個人情報や行政運営上重要な情報などの重要な情報を多数取り扱っている。また、多くの業務が情報システムやネットワークに依存している。

したがって、本市が保有する情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠であるため、次のことについて積極的に取り組むことを宣言する。

- 1 市民からの信頼に応えられるよう、本市の情報資産を、全力を挙げて適正に保護及び管理するための安全対策を推進する。
- 2 サイバーセキュリティ基本法の基本理念にのっとり、サイバーセキュリティに関する施策を実施する。
- 3 サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱な体制を構築する。
- 4 全ての職員は、サイバーセキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守する。
- 5 サイバーセキュリティ対策を適切に実施するため、全ての職員に対して必要な教育を実施する。

平成 30 年 3 月 15 日

横浜市最高情報セキュリティ責任者 渡辺 巧教

●横浜市情報セキュリティ管理規程

令和5年3月24日
達第1号
庁中一般

横浜市情報セキュリティ管理規程を次のように定める。

横浜市情報セキュリティ管理規程

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）の全部を改正する。

（目的）

第1条 この規程は、横浜市の保有する情報資産の取扱いに関し措置すべき事項を定めることにより、当該情報資産に対して機密性、完全性及び可用性の維持を図ること並びに当該情報資産の適正な運用による行政の信頼性の確保を図ることを目的とする。

（基本理念）

第2条 本市は、保有する情報資産が、市民の安全と福祉の向上に資することを目的として市民から管理を負託されたものであることを基本認識とし、この市民の信頼に応えられるよう全力を挙げて適正に保護及び管理することを基本理念とする。

（定義）

第3条 この規程において、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) 区局 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、横浜市会計室規則（平成19年3月横浜市規則第36号）第1条に規定する会計室、横浜市区役所事務分掌条例（平成28年2月横浜市条例第2号）第1条に規定する区役所をいう。
- (2) 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築する電子計算機処理の環境をいう。
- (3) 行政文書 横浜市行政文書管理規則（平成12年3月横浜市規則第25号）第2条第1項に規定する行政文書をいう。
- (4) システム関連文書 情報システムの開発及び運用に用いる行政文書をいう。
- (5) 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。
- (6) 記録媒体 データを記録した磁気ディスク、磁気テープその他の媒体をいう。
- (7) 個人情報 個人情報の保護に関する法律（平成15年法律第57号）第2条第1項に規定する個人情報をいう。
- (8) 特定個人情報 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）第2条第8項に規定する特定個人情報をいう。
- (9) 情報資産 区局が保有し、又は外部委託する情報システム、システム関連文書、情報システム利用時の認証に関する情報、データ及び記録媒体並びに個人情報及び特定個人情報を含む行政文書を

いう。

- (10) 機密性 情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。
- (11) 完全性 情報が破壊、改ざん又は消去されていない状態を確保することをいう。
- (12) 可用性 情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。
- (13) 情報セキュリティ 情報資産の機密性、完全性及び可用性を維持することをいう。
- (14) 情報セキュリティ対策 情報セキュリティの実現を目的として実施する対策をいう。
- (15) 職員 地方公務員法（昭和 25 年法律第 261 号）第 3 条に規定する一般職及び特別職の職員のうち、情報資産を使用する職員をいう。
- (16) 課等 横浜市事務分掌条例第 2 条の規定により設置された部、室、課及び係をいう。
- (17) 横浜市情報セキュリティポリシー 横浜市情報セキュリティ強化方針、横浜市サイバーセキュリティ強化方針、横浜市情報セキュリティ管理規程、横浜市情報セキュリティ管理要綱及び横浜市情報セキュリティ対策共通実施手順からなる、情報セキュリティに関する規程類の総称をいう。
- (18) 情報セキュリティ事故 情報資産の盗難、漏えい、改ざん、破壊等の機密性、完全性及び可用性が脅かされる事象をいう。

（対象とする脅威）

第 4 条 情報資産に対する脅威として、次に掲げる脅威を想定した、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに部外者の侵入、内部不正等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害による情報資産の損壊・滅失並びにサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等、インフラの障害からの波及等

（職員の責務）

第 5 条 職員は、第 2 条に定める基本理念及び情報セキュリティの重要性について認識し、情報資産を適切に取り扱わなければならない。

2 職員は、情報資産の取扱いに当たっては、次に掲げる法令等を遵守しなければならない。

- (1) 著作権法（昭和 45 年法律第 48 号）
- (2) 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
- (3) 個人情報の保護に関する法律
- (4) 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
- (5) サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- (6) 横浜市個人情報の保護に関する条例（令和 4 年 12 月横浜市条例第 38 号）

- (7) 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）

（組織体制）

- 第 6 条 第 4 条の脅威から情報資産を保護するため、次のとおり情報セキュリティ総括管理者、情報セキュリティ運用管理者、区局情報セキュリティ総括責任者、区局情報セキュリティ運用責任者、情報セキュリティ担当者及び情報資産管理者を置き、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
- 2 情報セキュリティ総括管理者は、横浜市最高情報統括責任者等設置規則（平成 27 年 3 月横浜市規則第 36 号）第 5 条に規定する最高情報セキュリティ責任者（以下「CISO」という。）をもって充て、情報セキュリティ運用管理者及び区局情報セキュリティ総括責任者を総括し、これらの者に対し情報セキュリティに関する事項について指示及び指導を行い、CISO が設置する横浜市情報セキュリティ委員会において決定した事項について、区局の情報セキュリティ対策を決定する。
 - 3 情報セキュリティ運用管理者は、デジタル統括本部長をもって充て、情報セキュリティ総括管理者を補佐するとともに、職員への情報セキュリティ対策実施の徹底を図るため、区局情報セキュリティ総括責任者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。
 - 4 区局情報セキュリティ総括責任者は、当該区局の長をもって充て、区局情報セキュリティ運用責任者及び情報セキュリティ担当者を総括し、これらの者に対し情報セキュリティに関する事項について指示及び指導を行う。
 - 5 区局情報セキュリティ運用責任者は、当該区局の総務担当課長をもって充て、区局情報セキュリティ総括責任者を補佐するとともに、当該区局の職員への情報セキュリティ対策の実施の徹底を図るため、情報セキュリティ担当者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。
 - 6 情報セキュリティ担当者は、当該区局の課等の長をもって充て、取り扱う情報資産の情報資産管理者と密に連携して、課等内の情報セキュリティ対策を実施するとともに、情報資産を利用する課等の職員に対して指導及び監督を行う。
 - 7 情報資産管理者は、別に定める情報資産の分類に応じた情報資産を主管する課等の長又は担当課長をもって充て、当該情報資産を利用する職員が所属する課等の情報セキュリティ担当者と密に連携して、当該情報資産の適正な維持管理を実施するとともに、当該情報資産を利用する職員に対して指導及び監督を行う。

（情報セキュリティ対策）

第 7 条 情報セキュリティ運用管理者は、以下の各号に掲げる情報セキュリティ対策を実施する。

- (1) 情報資産の機密性、完全性及び可用性に応じた分類並びに当該分類に基づく管理
- (2) 情報システム全体の強靱性向上
- (3) 物理的・人的・技術的における情報セキュリティ対策
- (4) 横浜市情報セキュリティポリシーの運用
- (5) 情報セキュリティ事故発生時の対応
- (6) 業務委託及び外部サービス利用時における情報セキュリティの確保

(情報セキュリティ監査及び自己点検の実施)

第8条 情報セキュリティ総括管理者は、前条の情報セキュリティ対策の実施状況を年1回及び必要に応じ監査及び自己点検し、問題がある場合には、速やかに是正しなければならない。

2 情報セキュリティ運用管理者は、区局の情報セキュリティ対策の実施状況を必要に応じ監査及び自己点検し、問題がある場合には、是正を命じることができる。

3 前2項に規定する監査は、客観性を確保するために、外部の専門的知識・見識を有する者の協力を得て実施することができる。

(横浜市情報セキュリティポリシーの見直し)

第9条 情報セキュリティ総括管理者は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、横浜市情報セキュリティポリシーを年1回及び必要に応じ見直ししなければならない。

(例外措置)

第10条 情報セキュリティ担当者は、この規程を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ総括管理者と協議の上、例外措置をとることができる。

2 情報セキュリティ担当者は、行政事務の遂行に緊急を要する等の場合であって、前項に定める例外措置をとることが不可避の時は、事後速やかに情報セキュリティ総括管理者に報告しなければならない。

(施行細則)

第11条 この規程に定めるもののほか、この規程の施行に関し必要な事項は、情報セキュリティ運用管理者が定める。

附 則

この達は、令和5年4月1日から施行する。

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(5.0) 2022年10月21日

横浜市デジタル統括本部 住民情報基盤課

目次

1 はじめに	5
(1) 本書の目的	5
(2) 対象読者	5
2 情報共有基盤の概要	6
(1) 情報共有基盤構築の経緯	6
(2) 情報共有基盤の目的	6
ア 業務の効率化の実現	6
イ 情報化関連経費の縮減	6
ウ 業務所管部門部署の管理負担の軽減	6
エ ベンダロックインの排除	6
(3) AIST 包括フレームワーク	7
(4) 情報共有基盤が提供するサービス	7
ア 基盤ネットワーク	7
イ 端末統制基盤 (情報共有基盤ドメイン)	7
ウ 仮想基盤	7
エ 基盤システム	8
(5) 情報共有基盤の機器構成	9
3 業務システムによる情報共有基盤の利用	10
4 情報共有基盤ネットワーク	11
(1) 情報共有基盤ネットワークの概要	11
.....	12
(2) ネットワークサービスの概要	12
ア 情報共有基盤ドメイン	12
イ DHCP	12
ウ DNS	13
エ NTP	13
(3) ネットワークセキュリティ	13
ア 機器接続制御	13

イ 基盤ファイアウォール.....	14
ウ 認証局.....	14
(4) LGWAN 接続.....	15
5 基盤端末.....	16
(1) 情報共有基盤端末の概要.....	16
(2) 端末・ユーザー管理.....	16
ア Active Directory の運用.....	16
イ ライセンス認証 (KMS).....	17
ウ 端末の導入.....	17
(3) 資源配布.....	18
ア 外字の配信.....	18
イ 任意のスクリプトの配信.....	18
(4) セキュリティ対策.....	19
ア ウイルス対策.....	19
イ データ書き出し制限.....	19
(5) 共有フォルダ.....	19
6 仮想基盤.....	21
(1) 仮想基盤の概要.....	21
(2) HCI アプライアンス (Nutanix).....	22
(3) 仮想化プラットフォーム (VMware vSphere).....	22
(4) 仮想基盤向けネットワークサービス.....	22
ア ロードバランサ.....	23
(5) 運用管理 (Hinemos).....	23
(6) バックアップ機能 (NetBackup).....	24
7 SSO システム.....	25
8 基盤ポータル.....	26
9 基盤連絡受付データベース.....	27
10 帳票基盤.....	28
11 データ連携基盤.....	29

(1) 文字コード変換	29
12 用語集	31

1 はじめに

(1) 本書の目的

本書の目的は、情報共有基盤の利用者に対して情報共有基盤の利用方法の概要を示すことである。

なお、本書は情報システムの標準化・共通化前のシステムをスコープとしており、本書では標準化後のシステムについては取り扱わない。

(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読者とする。

2 情報共有基盤の概要

(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である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。

令和 4 年度に、仮想基盤の更新に伴い、基盤システムの OS 及びミドルウェア等について更新を行った。

(2) 情報共有基盤の目的

情報共有基盤の目的は、行政運営の効率化である。具体的には、下記に示す 4 つを掲げている。

ア 業務の効率化の実現

複数の業務システムが共通して利用できるデータ連携の仕組みを整備することで、システム間の情報伝達を円滑にし、業務を効率化する。

イ 情報化関連経費の縮減

複数の業務システムがハードウェアなどのシステムインフラを共用することにより、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。

ウ 業務所管部門部署の管理負担の軽減

業務システムが利用するシステムインフラの管理を基盤システム所管部門が一括して引き受けることで、業務システム所管部門の管理負担の軽減を図る。

エ ベンダロックインの排除

特定の事業者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。

(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。

(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。

ア 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。

イ 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。

ウ 仮想基盤

業務システム用の仮想サーバ及び仮想基盤向けネットワークサービス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。

エ 基盤システム

シングルサインオン (SSO)、ポータル、データ連携等、業務システムが共通して必要とする機能を提供している。

本書の 7SSO システム ～ 11 データ連携基盤で説明している。

(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 2-1 情報共有基盤機器構成図に示す。

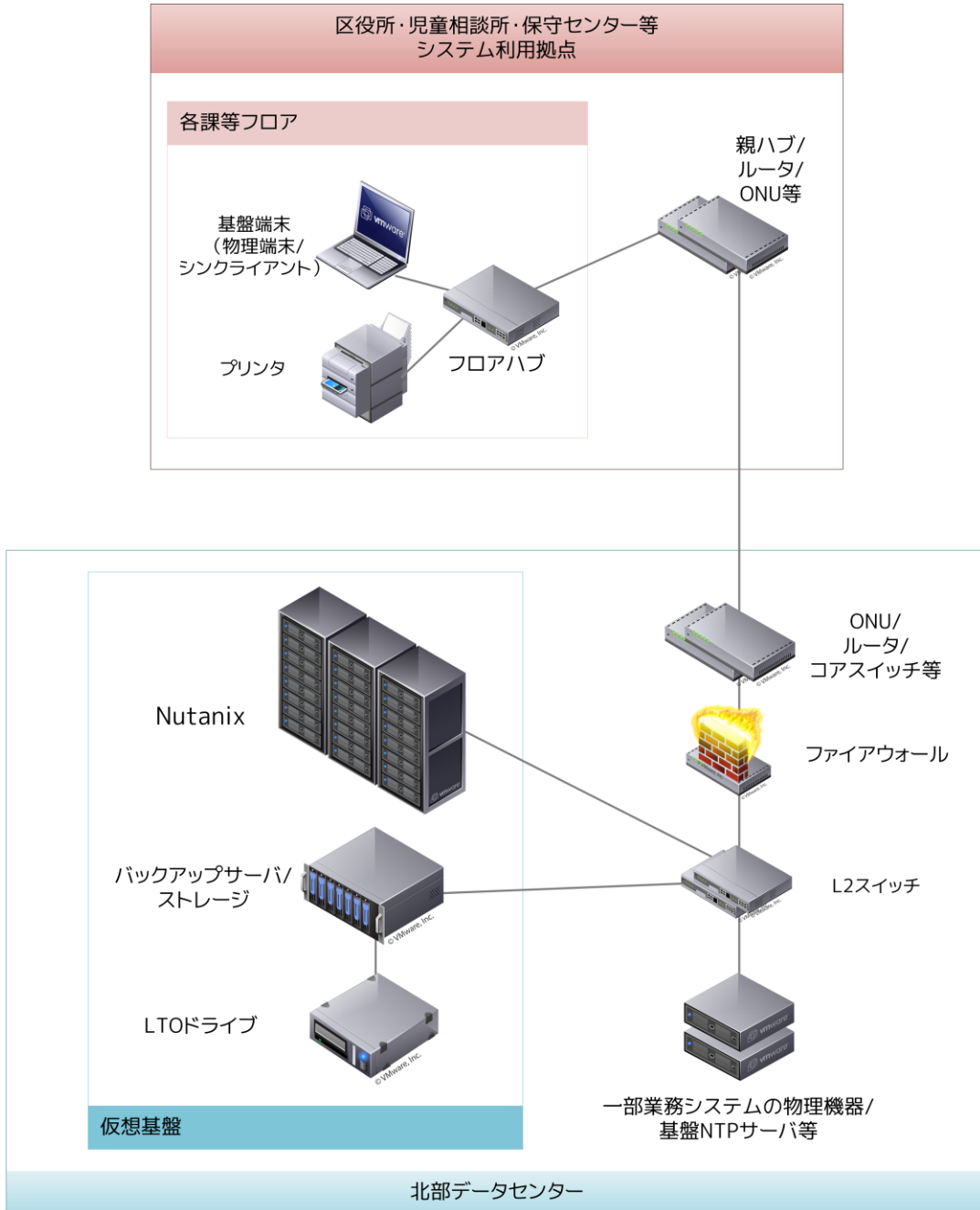


図 2-1 情報共有基盤機器構成図

3 業務システムによる情報共有基盤の利用

業務システムは、その用途に応じて情報共有基盤が提供するシステムインフラや機能の一部、又は全部を利用することができる。

4 情報共有基盤ネットワーク

(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一部である。

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（事前に申請し、許可された通信のみ）。

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到示す。

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 ※
市庁舎サーバールーム	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	システム開発・運用拠点
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

※ 北部データセンターとの関係では、市庁舎サーバールームは「利用拠点」扱いとなる。

(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。

ア 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)ア Active Directory で説明する。

イ 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。

基盤システム所管部門に対し利用申請をした機器は、同部門が管理し全体に共有している「端末台帳」に、MAC アドレスと IP アドレス等の情報を記録される。DHCP サーバは、この端末台帳に記載された機器の MAC アドレスと IP アドレスに基づいて設定される。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。

原則として固定 IP アドレスの使用は認めておらず、DHCP から払い出しを受けていない機器の通信は遮断される

ウ 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。

エ 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。端末・サーバからは、Stratum3 である Active Directory サーバ (正/副) を参照すること。

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)

(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。

ア 機器接続制御

(2)イ 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。

イ 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。

ウ 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、業務システムの環境名と FQDN 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 (crt 形式) と秘密鍵 (key 形式) のペアで各業務システムに受け渡す。仮想基盤のロードバランサを利用している環境の場合、利用方法については 6(4)ア □

ードバランサを参照すること。

(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。

利用にあたっては、事前に、住民情報系ネットワーク統括責任者 (当課管理担当) に、「住民情報系ネットワーク接続協議依頼書」を提出して協議を依頼し、接続の許可を得なければならない。

また、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

(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。

(2) 端末・ユーザー管理

ア 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 Microsoft Edge 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。

イ 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。

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。

認証が可能な OS/Office 製品のバージョンについては、Redmine の Wiki に掲載する。

ウ 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、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（仕様の下限を定めたもの）及びそれぞれの業務システムの要求を満たす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。これにより端末が端末台帳に登録され、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、新規プリンタの導入についても同様の運用を行っている。

(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립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、PalletControl を用いている。

ア 外字の配信

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基幹システム外字の表示・入力ができるようにしている。

イ 任意のスク립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립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립トのサンプルを配布している。配布されているスク립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립トにはバージョン 6.3 用のスク립トとバージョン 7 以降用のスク립トの 2 種類が存在するが、基盤端末ではバージョン 6.3 用のスク립トのみ利用できる。

(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。

ア 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 Endpoint Security、Linux サーバ用に McAfee Endpoint Security for Linux を採用している。

イ 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 (SD カード等) に直接書き出し可能な内蔵カードリーダー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読み書きを制限している。

(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、希望に応じて、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、事前に指定されたユーザ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、(2)ア 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

(1) 仮想基盤の概要

仮想基盤は、業務システム用の仮想サーバ及び仮想基盤向けネットワークサービス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・仮想基盤向けネットワークサービス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 仮想基盤サービス仕様書」(旧名称:「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。

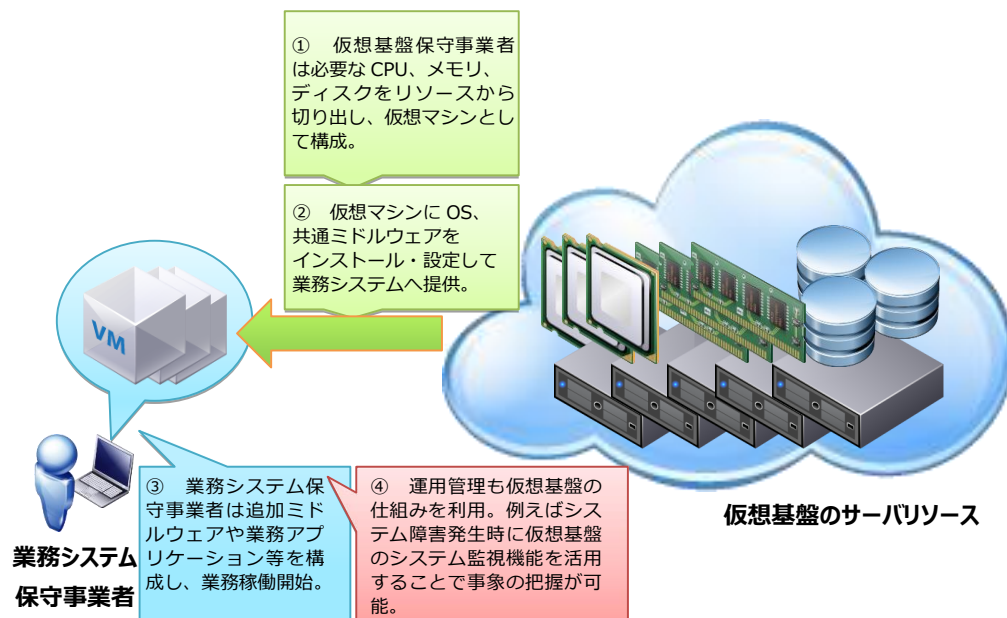


図 6-1 仮想基盤の利用イメージ

(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。

(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。

(4) 仮想基盤向けネットワークサービス

仮想基盤上の仮想マシン間のネットワークは、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。

ア 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、ロードバランサ（物理）を共同利用できる。

仮想基盤を利用する業務システムは、端末から見てサーバの手前側に設置されたロードバランサと端末間で HTTPS 通信を行う。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通信についてはサーバ側へのサーバ証明書の導入は不要である。

(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) 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。

また、Wiki により、各種情報及び申請様式が共有されている。

基盤連絡受付データベースの画面イメージを図 9-1 基盤連絡受付データベースに示す。

#	ステータス	トラッカー	カテゴリ	題名	更新日	期日	作成者	担当者	起票元
55342	新規	連絡票	03 依頼	レセプト端末への顔認証の配備について	2018/05/21 10:08		横浜 文子	港北一 基盤システム	
55278	新規	連絡票	04 インシデント	増えているプリンタより出力できない (東土ヶ谷区 tepc-161014-003)	2018/05/21 10:00		関内 二郎	NEC 基盤システム 保守者	
55288	新規	連絡票	03 依頼	[20180518] 【生保】SSOアカウント再発行依頼 (健康福祉局)	2018/05/21 09:55		横浜市 生活保護システム運用部署	SHNet 生活保護システム 運用者	
55335	新規	連絡票	03 依頼	【依頼：SSO申請】福祉保健システム連携申請 (国球職員、アルバイト) <20180521>	2018/05/21 09:52	2018/05/24	横浜 文子	SHNet 福祉保健システム 運用者	
55231	対応済	連絡票	03 依頼	プリンタ出力先変更依頼(朝谷区 Y91PC217)	2018/05/21 09:36	2018/05/23	日ノ出 三郎	NEC 基盤システム 保守者	

図 9-1 基盤連絡受付データベース

10 帳票基盤

情報共有基盤は各業務システム向けに帳票出力機能を提供するため、共通の帳票基盤を運用している。各業務システムはこの帳票基盤を利用して帳票を作成及び出力することができる。

帳票ソフトウェアはウイングアーク 1st 社の SVF を導入している。導入している製品パッケージは下記の通り。

- SVF Connect SUITE Standard (旧名「Universal Connect/X」)
- SVF for PDF
- SVF for Java Print
- SVF for Web/Client

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。

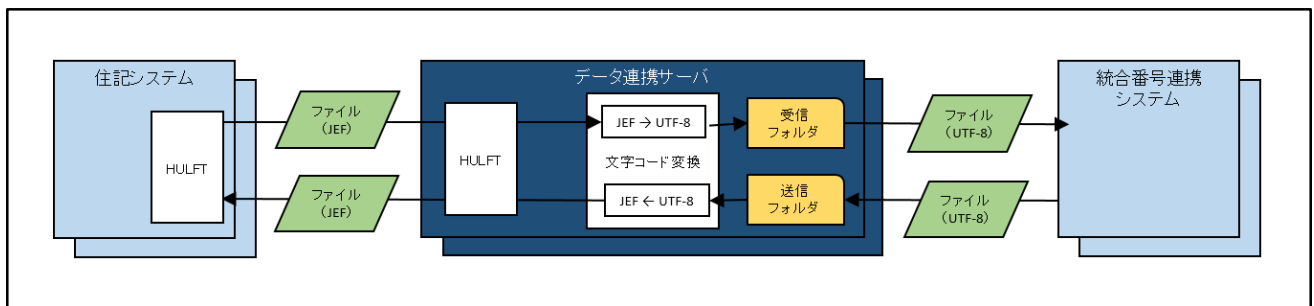


図 11-1 データ連携基盤利用の例

(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		<ul style="list-style-type: none"> ・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。 	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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。 		<ul style="list-style-type: none"> ・外字の変換は不可。
Shift-JIS から	<ul style="list-style-type: none"> ・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) 	<ul style="list-style-type: none"> ・外字の変換は不可。 	

12 用語集

初出 ページ	用語	意味
8	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。
11	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。
11	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。
15	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管理するサーバ。各機関間の連携における中継点となる。
19	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。
21	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。
22	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。
29	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。
30	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。

横浜市 仮想基盤サービス仕様書

第 1.0 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	2022/03/23	日立	新規作成

内容

1.	はじめに.....	5
1.1.	本書の位置付け.....	5
1.2.	対象読者.....	5
1.3.	関連ドキュメント.....	5
2.	仮想基盤の概要.....	6
2.1.	サービス提供範囲.....	7
2.2.	仮想基盤の仕組み.....	8
2.2.1.	仮想基盤のシステム構成.....	9
2.2.2.	仮想基盤で用意する3つの基盤.....	10
2.3.	仮想基盤の可用性.....	11
2.3.1.	仮想マシンの冗長化構成.....	11
2.3.2.	ハードウェアの冗長化構成.....	12
2.3.3.	仮想基盤の可用性に関する留意事項.....	12
3.	サービス内容.....	13
3.1.	サービスメニュー.....	13
3.2.	サービス提供時間.....	13
3.3.	サービスメニューのリードタイム.....	15
4.	サービスの詳細内容.....	16
4.1.	仮想マシン提供サービス.....	16
4.2.	ライセンス提供サービス.....	19
4.3.	ネットワーク提供サービス.....	20
4.3.1.	仮想基盤の内部ネットワーク構成.....	20
4.3.2.	仮想基盤ネットワークと基幹ネットワークの間の通信について.....	21
4.3.3.	既存環境・外部ネットワークとの接続.....	23
4.3.4.	ロードバランサーの標準設定値について.....	24
4.4.	運用管理機能提供サービス.....	25
4.4.1.	ジョブ機能.....	26
4.4.2.	監視機能.....	27
4.5.	バックアップ設定サービス.....	30
4.6.	バックアップ・リストア機能提供サービス.....	33
4.6.1.	システムバックアップ.....	33
4.6.2.	ファイルバックアップ.....	34
4.6.3.	データバックアップ（オプションサービス）.....	35

4.7.	システムリストア支援サービス.....	36
5.	サービス利用にあたって.....	37
5.1.	セキュリティ.....	37
5.1.1.	分散ファイアウォール.....	37
5.1.2.	仮想マシンに導入するウイルス対策.....	37
5.1.3.	セキュリティパッチの適用.....	37
5.1.4.	OS のローカル管理者パスワード.....	38
5.2.	仮想基盤のリソース管理.....	39
5.3.	仮想マシンへの接続方式と使用アカウント.....	40
6.	その他制限事項・注意事項.....	42

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の仮想基盤（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。

1.3. 関連ドキュメント

本書に記載の内容に関連するドキュメントを以下に示します。

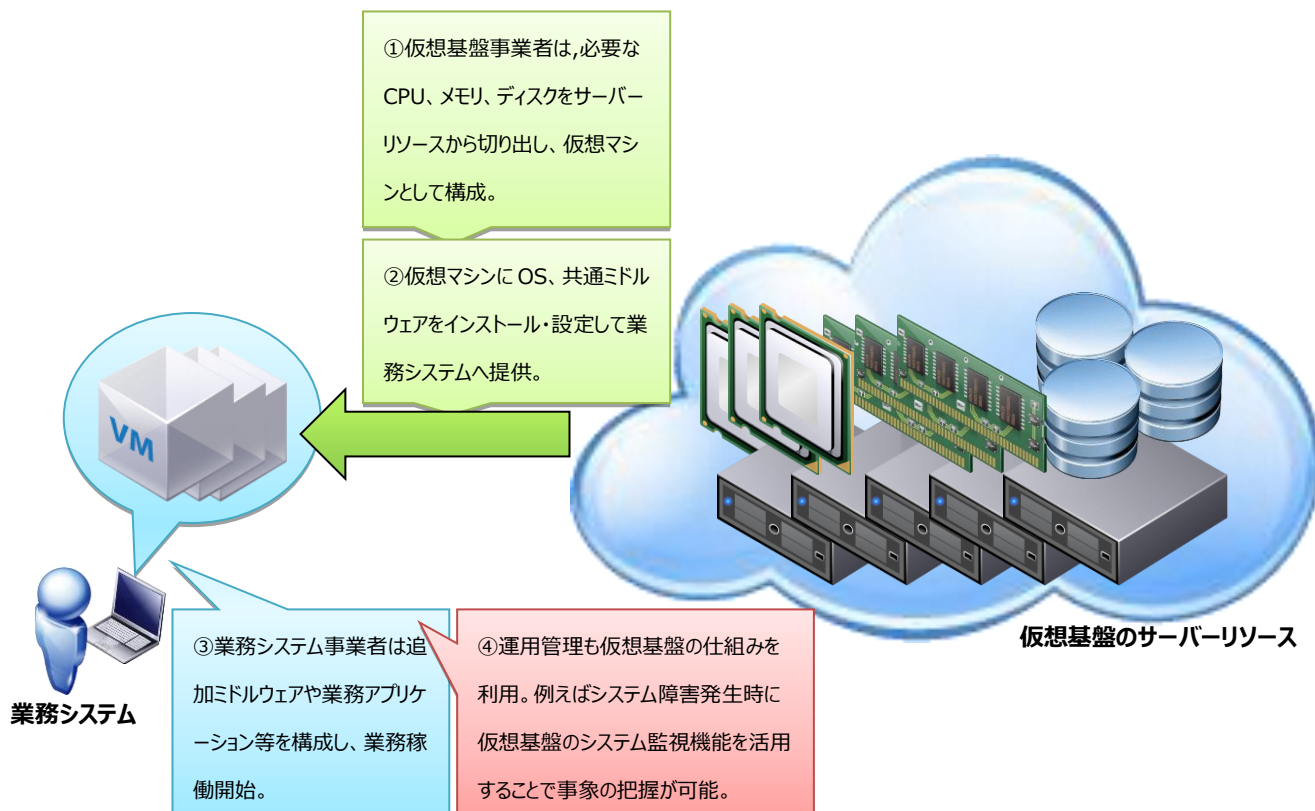
2. 仮想基盤の概要

本書に記載する仮想基盤とは、情報共有基盤所管部門が提供する、情報共有基盤のサービスの一部である仮想基盤機能を示します。仮想基盤は、情報共有基盤所管部門が監督し、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ー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ー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ーや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、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。



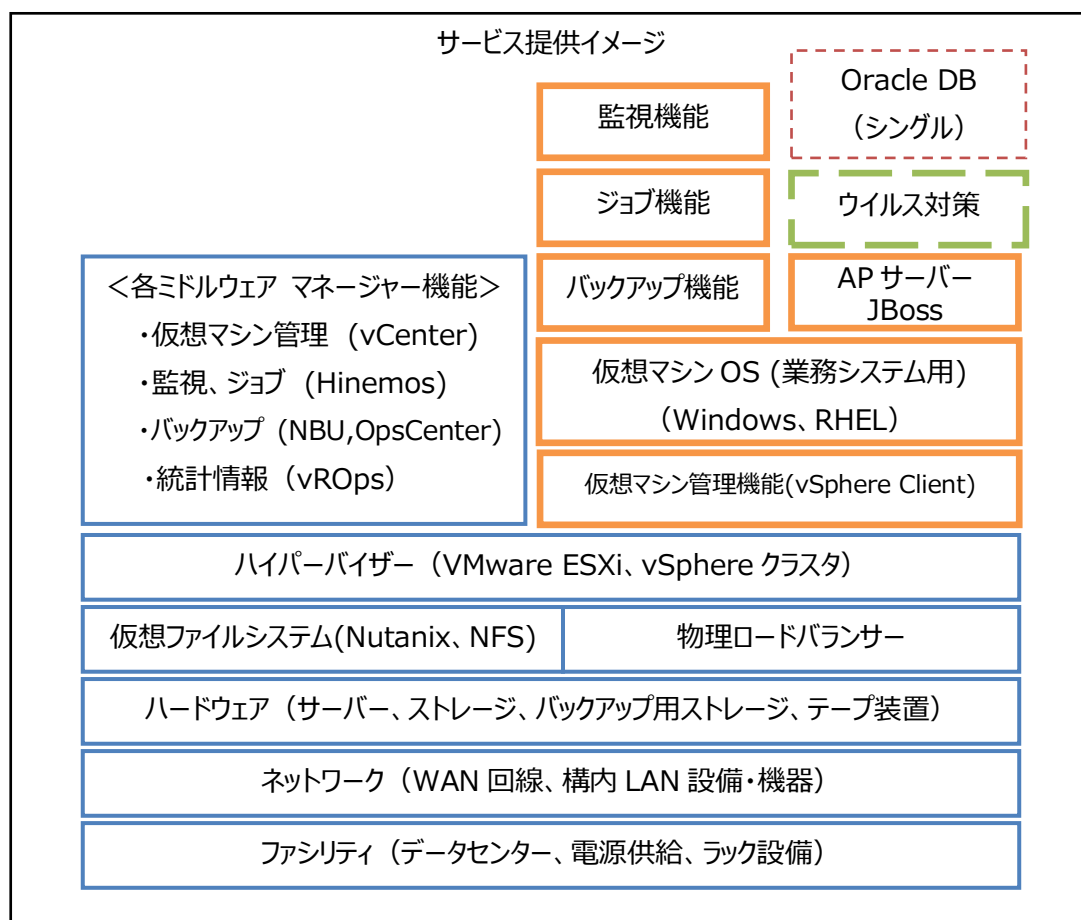
2.1. サービス提供範囲

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、業務システム事業者にて「導入する・しない」の選択が可能です。

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・Oracle Database の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。



凡例：



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。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となる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。そのため、仮想基盤は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。

なお、業務システムのインフラとして仮想基盤を採用するかどうか判断するにあたっては、以下を考慮する必要があります。

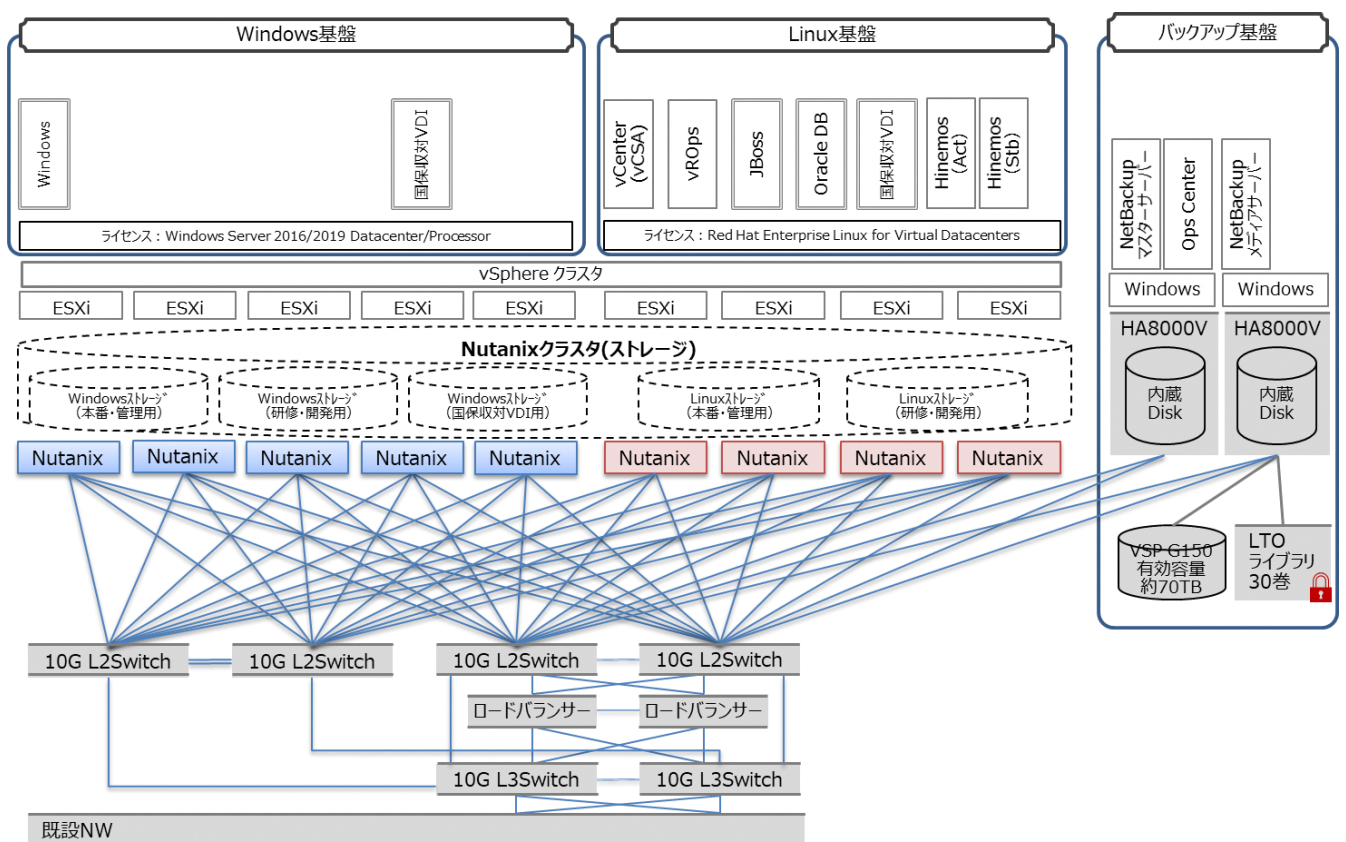
- ・共通の仕組みを業務システムが共用することで全体の労力と費用を低減するものであるため、業務システム個別の要件に対応して構成を変更したり、機能を追加したりすることはできません。
- また、仮想基盤のサービス停止を伴うメンテナンス作業等の運用スケジュール決定にあたって、業務システムの都合を考慮することはできません。
- ・業務システムのアプリケーションとインフラを別に開発、運用することになるため、責任分界点が生じます。このため、業務システムのアプリケーションとインフラを一括で開発、運用する場合と比較して、障害発生時の復旧等に時間を要する場合があります。

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。図を見て分かる通り、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3つの基盤とNW環境に分けて考えることができます。3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3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、1 つの VMware vSphere クラスタで2つのグループを構成しています。その 2 つのグループは用途に応じてそれぞれ、「Windows 基盤」、「Linux 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、物理サーバー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3つの基盤について示します。

No	基盤名	説明
1	Windows 基盤	<p><提供機能></p> <ul style="list-style-type: none"> ・仮想マシン管理機能 (PowerCLI※) <p>※CLI で仮想マシンのパワーオンや状態確認を実施する際に使用</p> <p><仮想マシン (業務システム用) 配置の考え方></p> <ul style="list-style-type: none"> ・Windows Server 2016/2019 を使用する仮想マシン ・Linux 基盤に所属しない仮想マシン
2	Linux 基盤	<p><提供機能></p> <ul style="list-style-type: none"> ・仮想マシン管理機能 (vCenter) ・運用管理サーバー (Hinemos による監視機能、ジョブ機能) ・Oracle ライセンス提供 (機能提供無し、インストールは各業務システム事業者にて実施。Linux 版のみ資材を用意) <p><仮想マシン (業務システム用) 配置の考え方></p> <ul style="list-style-type: none"> ・RHEL7.9/8.4 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	バックアップ基盤	<p><提供機能></p> <ul style="list-style-type: none"> ・バックアップ/リストア機能 (NetBackup) ・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。Windows 基盤、Linux 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 サーバー（シングルインスタンス構成）のように、1 台構成の仮想マシンに対して適用する。
- ホストアフィニティ
現用系/待機系といったサーバー構成時の各仮想マシンを別の 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。

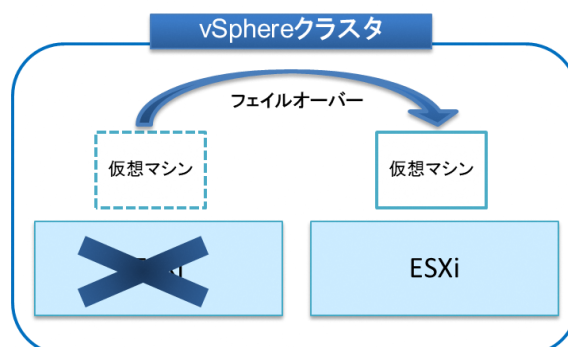
また、仮想マシン管理機能を提供しているサーバーについてはホットスタンバイ構成とはなっていないため、障害時には一時的にサービスダウンすることになります。

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。

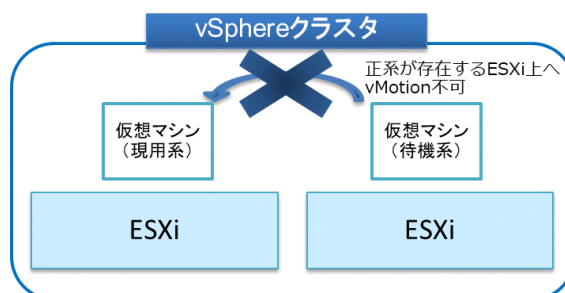
2.3.1. 仮想マシンの冗長化構成

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ー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)



また業務システムに提供する仮想マシンで、現用系/待機系といったサーバー構成の場合、ホストアフィニティを設定し、各仮想マシンを別の ESXi 上で起動させることが可能です。そのため、ESXi 障害時に現用系/待機系の仮想マシンが同時に利用停止となることを防ぐことができます。



2.3.2. 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 9 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。

2.3.3. 仮想基盤の可用性に関する留意事項

仮想マシンが稼働している ESXi（物理サーバー）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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・Windows Server、RHEL、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	<ul style="list-style-type: none"> ・利用申請書および受入申請書に基づいたネットワーク環境の提供 (仮想基盤用 L3SW、物理ロードバランサーの設定)
4	バックアップ設定サービス	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・システムリストアの場合は、申請書に基づいた作業支援（必須） ・システムリストアに該当しない（ファイルリストア等）場合は、本サービスの適用外となりますので各業務システム事業者にて実施してください。

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、基幹ネットワークが停止する場合、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	<ul style="list-style-type: none"> ・対象に応じて、四半期から年次のサイクルで実施します。 ・具体的な実施日（年間スケジュール）は、毎年 4 月頃に情報共有基盤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	<ul style="list-style-type: none"> ・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。 <ul style="list-style-type: none"> 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ー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、情報共有基盤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、サービス提供開始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。

No	サービスメニュー	リードタイム	
		新規業務システム受入の場合 (仮想マシン 8 台あたり)	既存業務システムの場合 (仮想マシン 1 台あたり)
1	仮想マシン提供サービス	11 開庁日以内	2 開庁日以内
2	ライセンス提供サービス	(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)	
3	ネットワーク提供サービス		個別調整
4	バックアップ設定サービス	2 開庁日以内	1 開庁日以内
5	バックアップ・リストア機能提供サービス	(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)	
6	運用管理機能提供サービス	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)	1 開庁日以内
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)	

「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。

なお利用申請時の要件によっては、仮想マシンを、“テンプレートから作成”ではなく“新規作成”とする場合があります。“新規作成”の場合、上記のリードタイムよりさらに時間がかかることを見込んでください。

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	Windows2016 テンプレート	Windows Server 2016 Standard	2 コア	8GB	100GB
2	Windows2019 テンプレート	Windows Server 2019 Standard	2 コア	8GB	100GB
3	RHEL7.9 テンプレート	Red Hat Enterprise Linux 7.9	2 コア	8GB	100GB
4	RHEL8.4 テンプレート	Red Hat Enterprise Linux 8.4	2 コア	8GB	100GB
5	RHEL7.9 + JBoss テンプレート	・Red Hat Enterprise Linux 7.9 ・JBoss EAP 7.3	2 コア	8GB	100GB
6	RHEL8.4 + JBoss テンプレート	・Red Hat Enterprise Linux 8.4 ・JBoss EAP 7.3	2 コア	8GB	100GB

※ システム領域のみ。100GB 未満にする場合はテンプレートから払い出しできません。

◆ 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。

◆ 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。

また上記の 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。

- 仮想マシンテンプレートの OS モジュール構成

- ・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。またテンプレート作成時点においてリリースされている更新プログラムを適用しています。適用されている更新プログラムについても、OS テンプレートの定数設計書を確認してください。

- ・RHEL テンプレート、および RHEL+JBoss テンプレートについては、テンプレート作成時点に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。

- 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された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、ウイルス対策ソフト
- ・RHEL+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 + JBoss7.3

なお、Oracle DB サーバー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、ウイルス対策ソフトを予めインストールした状態で提供いたします。Oracle Database 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 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。払い出し後の 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。

● 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。

No	ミドルウェア	バージョン
1	VMware ESXi	7.0 u1d
2	VMware vCenter Server Appliance	7.0 u1d

● 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情報共有基盤所管部門に報告し承諾を得てください。情報共有基盤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は行っておりません。）
- ・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となります。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者にて対応してください。

4.2. ライセンス提供サービス

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ならびにミドルウェアのバージョンは、以下のとおりです。

- Windows Server 2016 Standard
- Windows Server 2019 Standard
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.4
- Oracle Database 19c[19.11.0.0 DBRU:210420] (Oracle Database Standard Edition 2)
- Oracle Java SE 8u291
- Red Hat JBoss Enterprise Application Platform 7.3
- Hinemos 6.2.2
- NetBackup 8.3

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			
		Windows2016	Windows2019	RHEL7.9	RHEL8.4
ミドルウェア	Oracle DB 19c	○※	○※	○	○
	JBoss EAP 7.3	×	×	○	○

※Windows系のサーバーにOracle Databaseをインストールする場合、資材準備を含め、各業務システム事業者にて実施してください。

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。セグメント内の全ての仮想マシンは相互に通信が可能です。

また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。

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	仮想基盤管理用サーバー群を設置し利用 (ESXi、vCenter 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ー群を設置し利用 (バッチサーバ等)
4	バランシングセグメント	ロードバランサーで負荷分散されるサーバー群を設置し利用 (Web サーバー等)
5	AP セグメント	AP サーバー設置セグメント、WEB サーバー～AP サーバー間で利用
6	DB セグメント	DB サーバー設置セグメント、AP サーバー～DB サーバー間で利用
7	RMAN セグメント	データバックアップで利用 (データバックアップ (4.6.3 章) を必要とするシステムのみ)
8	番号用 LGWAN セグメント	LGWAN 接続経路で利用
9	FW セグメント	LGWAN 接続 FW の FW 間で利用
10	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、HA8000V 等)
11	モニタリングセグメント	仮想基盤監視用のセグメント 各サーバーを収容し、監視及び NBU バックアップの通信で利用

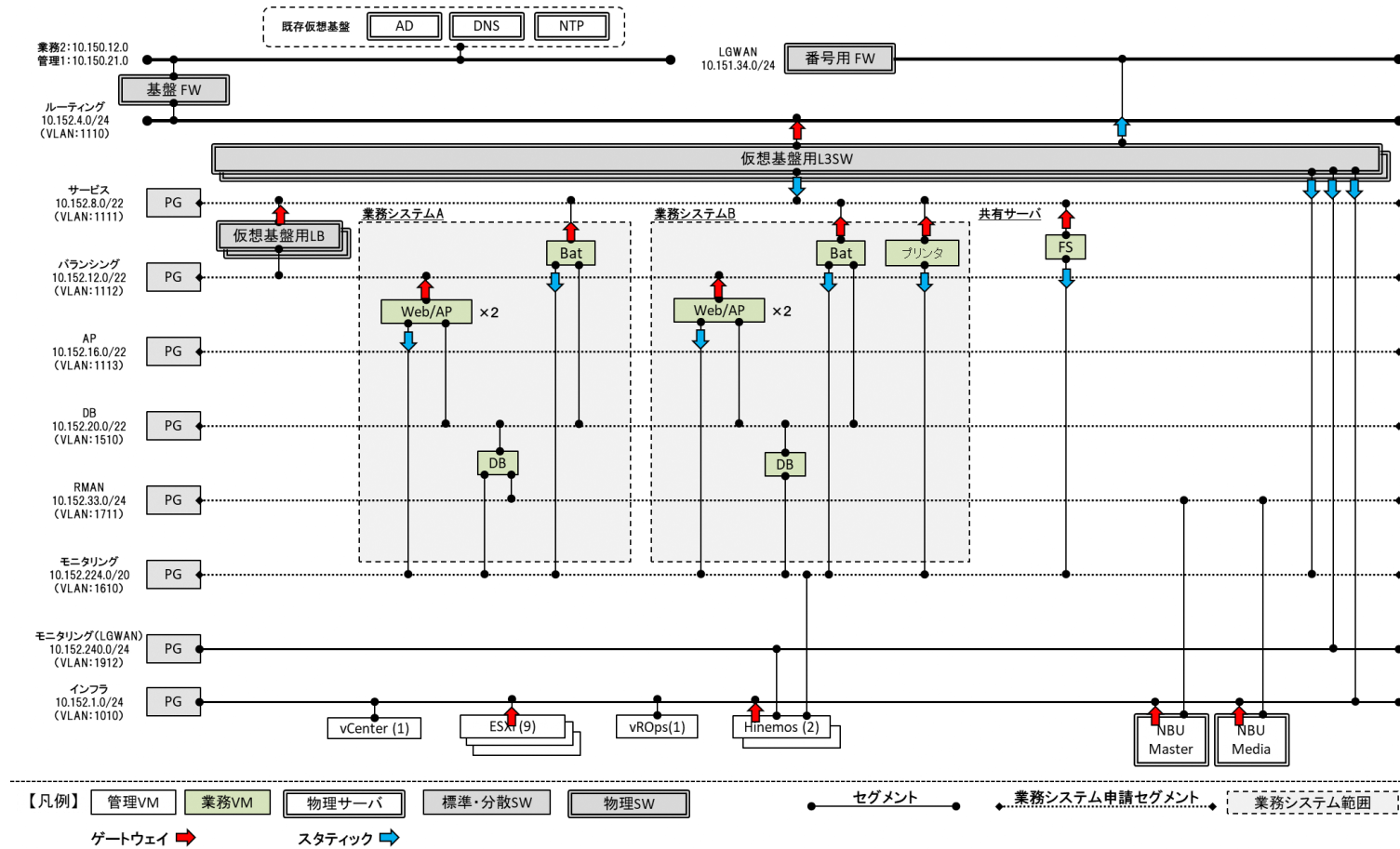
次項では、仮想基盤の本番環境における論理ネットワークの標準構成、および構成例を示します。

4.3.2. 仮想基盤ネットワークと基幹ネットワークの間の通信について

仮想基盤のサービスセグメントは、既存の基幹ネットワークとの通信が可能な構成となっています。モニタリングセグメント経由でも通信は可能ですが、その場合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幹ネットワークに所属するサーバー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。

● 論理ネットワーク構成の構成例

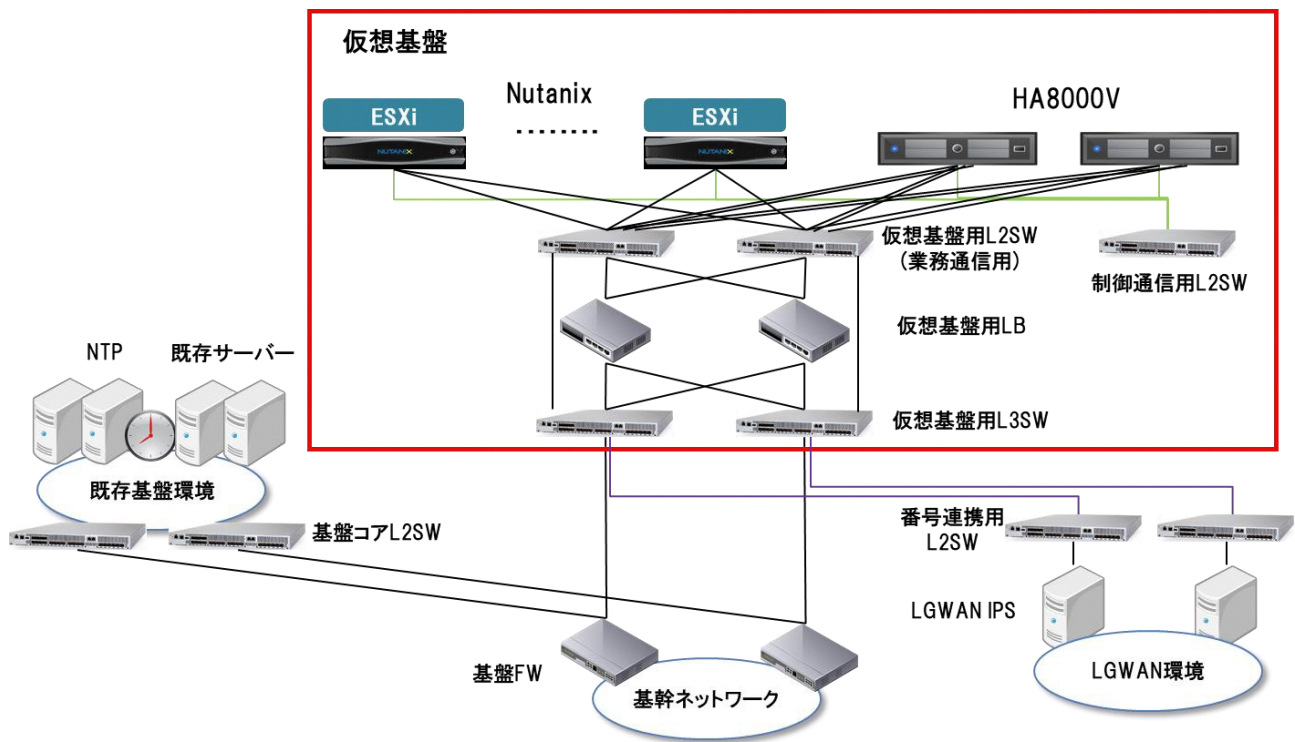


4.3.3. 既存環境・外部ネットワークとの接続

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（NTPサーバー等、基盤システムの物理サーバー）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. ロードバランサー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物理ロードバランサー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	300 秒	同一のクライアントからのリクエストを常に同じサーバーに転送する時間。 申請により変更することが可能（最大 3600 秒）
4	セッションタイムアウト間隔	3600 秒	端末からの TCP セッションのタイムアウト値。
5	サービス監視間隔	5 秒	
6	サービス監視タイムアウト	16 秒	
7	X-Forwarded-For-HTTP ヘッダ	有効	
8	IP アドレス透過有無	非透過	<ul style="list-style-type: none"> ・物理 LB 配下のサーバーは接続元 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、サーバー側で 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。

また本サービスを提供している運用管理サーバーについては、予め待機系のサーバーを配置しています（ミッションクリティカル構成）。したがって、運用管理サーバーにて障害が発生した際は、待機系に切り替わり、サービスを継続して提供します。

- 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ーを提供します。
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。
同時接続数が上限に達した場合は、運用管理サーバーを再起動して解消するため、やむを得ず Hinemos マネージャへの接続を強制切断します。
- 運用管理サーバーの定期メンテナンス実施について
Hinemos の安定稼働を目的とした運用管理サーバーの定期メンテナンス作業を、年に複数回実施します。
日時については、年度当初に情報共有基盤所管部門より周知します。

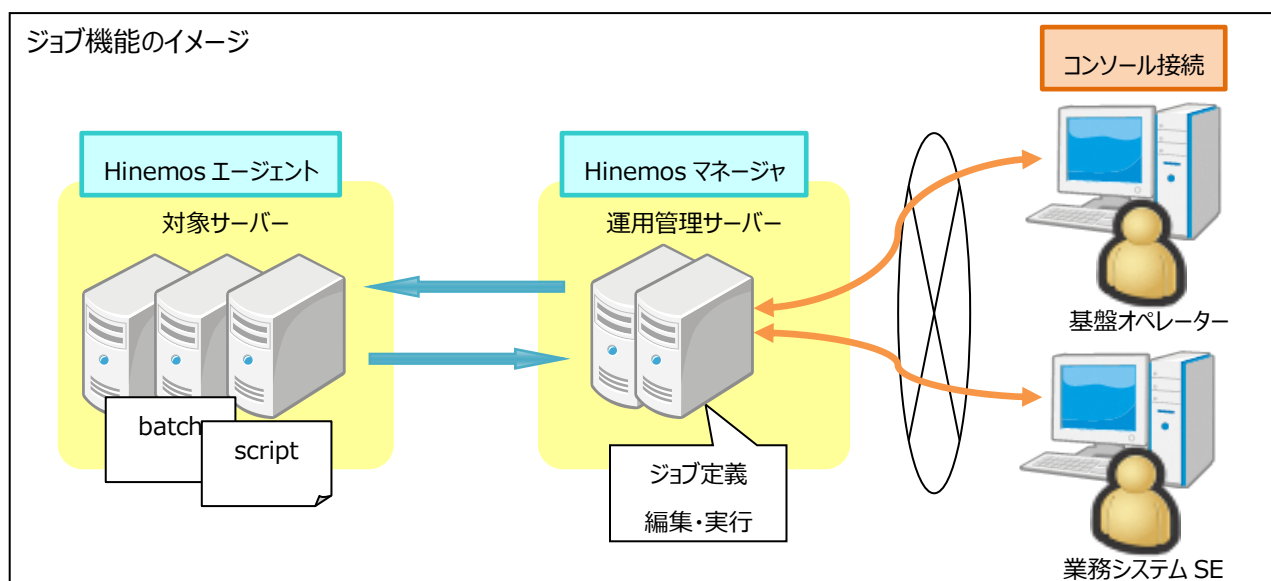
4.4.1. ジョブ機能

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。運用管理機能はマルチテナント利用のため、業務システム事業者がジョブユニットを作成することを禁止しています。必ず、払い出されたジョブユニットを使用してください。

また、ジョブの実行を基盤オペレーターに依頼する場合、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（内容は情報共有基盤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、基盤オペレーターに引継いでください。

なお前述のとおり、運用管理サーバーは冗長化構成となっていますが、万が一正副両系で障害が発生した際は、サービス利用ができません。そのため、運用管理機能の障害に備え、ジョブの手動実行やリカバリを想定したジョブの構築をお願いします。

ジョブ機能の概要について、以下の図に示します。



- Hinemos からジョブを実行する際に対象サーバーで利用されるアカウント
 ジョブの実行ユーザーとして、仮想マシンに払い出した OS 管理者ユーザーを割り当てています。詳細は、仮想マシン払い出し時に提供される「仮想マシン作成報告書」のアカウント一覧情報を確認してください。
 上記ユーザー以外をジョブ実行ユーザーとして設定したい場合、情報共有基盤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ーの監視設計を行い、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、運用管理サーバー（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]

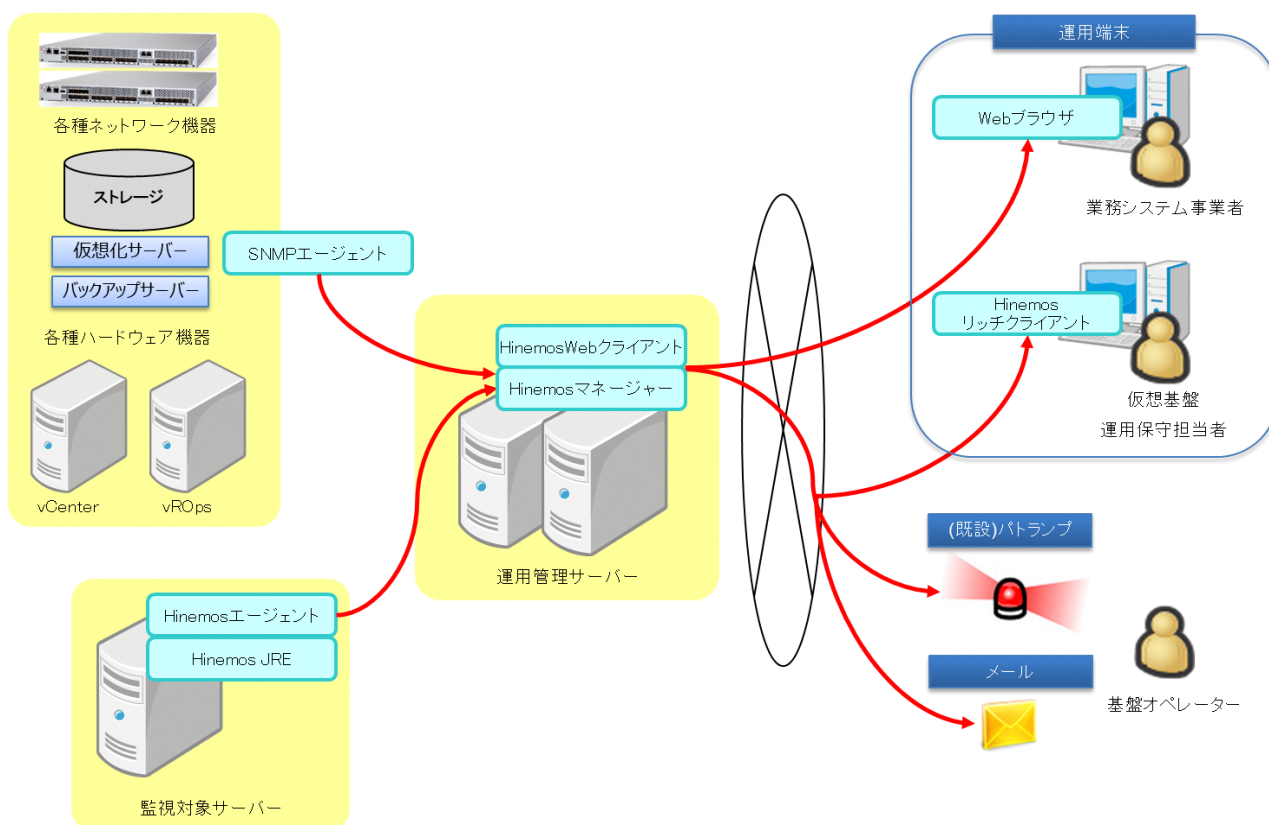
No	監視種別	概要
1	PING 監視	ICMP (Ping) を用いて監視対象の IP アドレス死活を監視する。
2	システムログ監視	RHEL のシステムログに出力されたメッセージを監視する。
3	イベントログ監視	Windows イベントログに出力されたメッセージを監視する。
4	ログ監視	特定のログファイルに出力されたメッセージを監視する。
5	リソース監視	対象機器や OS のリソース状況を監視する。
6	プロセス監視	監視対象サーバーのシステム (OS) およびアプリケーションのプロセスを監視する。
7	Windows サービス監視	Windows サービスの状態を監視する。
8	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 サーバー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。
13	HTTP 監視	Web サーバーの応答有無や応答時間、HTTP レスポンスの内容を監視する。

なお、監視結果及びジョブの実行結果を通知する機能として、「ステータス通知」「イベント通知」「メール通知」「コマンド通知」の 4 つの機能を使用します。通知の詳細については、別途提供している「運用管理基盤 詳細設計書 Hinemos（システム監視 + ジョブ管理）編」を参照してください。

本番稼働中に障害を検知した場合は、基盤オペレーター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ー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ーに対する監視内容
- ・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
（基盤オペレーター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、不要なエラー通知を発生させることは、基盤オペレーターの業務や運用管理基盤に無用な負荷をかけることになるため、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が必要な場合は、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”に変更することを禁じます。

- 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。

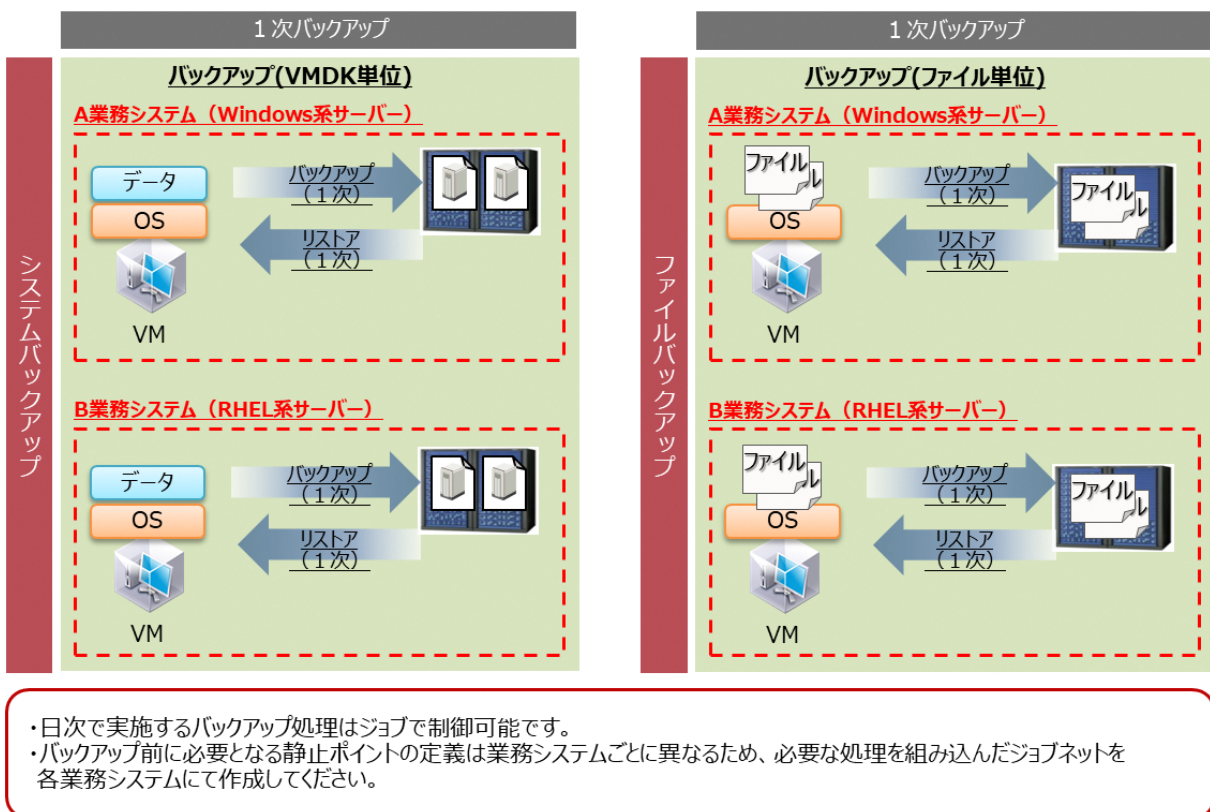
csv ダウンロードの詳細については、別途提供している「運用管理基盤利用手順書(Hinemos)」を参照してください。

(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ファイルバックアップについて示します。



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。
- ・2022年4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ーが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レーブの低下」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。

(※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。

- ・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"パラメータを指定した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"パラメー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"パラメー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7日間となります。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。）
- ・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"パラメータを指定した1次バックアップに限ります。
- ・"full_week"パラメー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情報共有基盤所管部門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 サーバーにおいて、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情報共有基盤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、情報共有基盤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ご連絡します。

4.6. バックアップ・リストア機能提供サービス

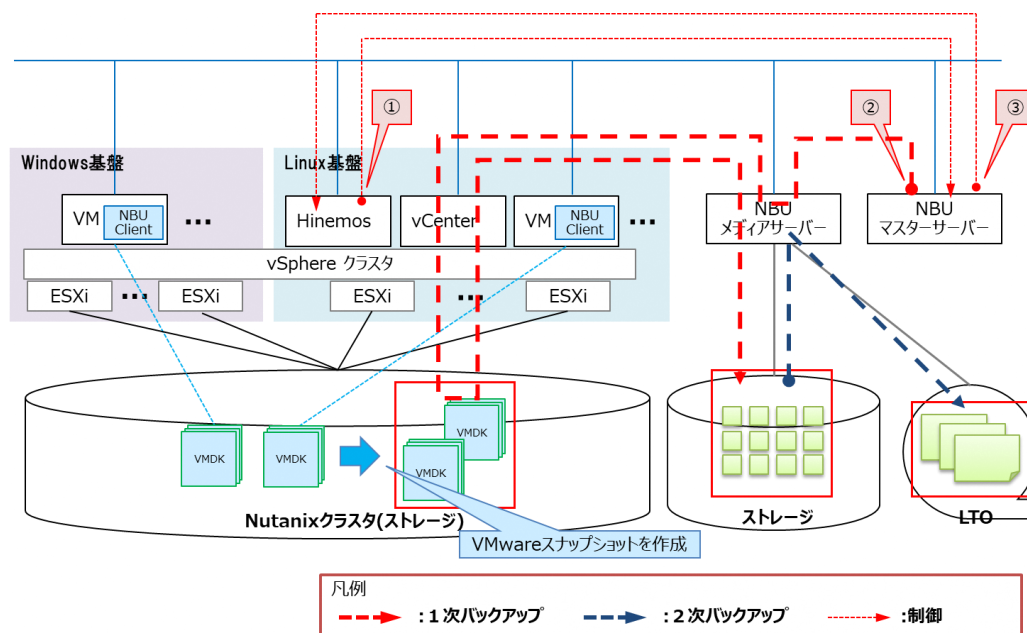
4.6.1. システムバックアップ

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。

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のパラメー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。）



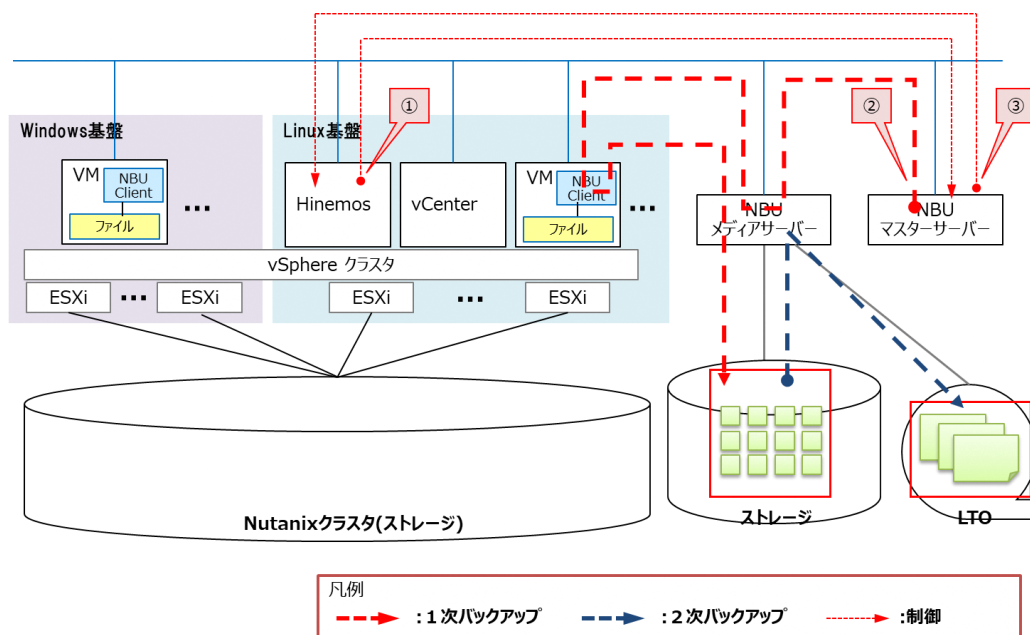
No	処理項目	処理内容
①	ジョブ開始	運用管理サーバー（Hinemos）より、バックアップジョブを開始する。 ・NBU マスターサーバーへバックアップポリシー実行を指示。
②	バックアップ処理	NBU マスターサーバーでバックアップポリシーが開始する。 ・NBU メディアサーバーが対象サーバー（仮想マシン）をストレージ（VSP G150）へバックアップ。
③	ジョブ完了	NBU マスターサーバーでのバックアップポリシー完了後、運用管理サーバーよりバックアップジョブを完了する。 ・NBU マスターサーバーがバックアップポリシー完了後にリターンコードを発行。

4.6.2. 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。

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。）



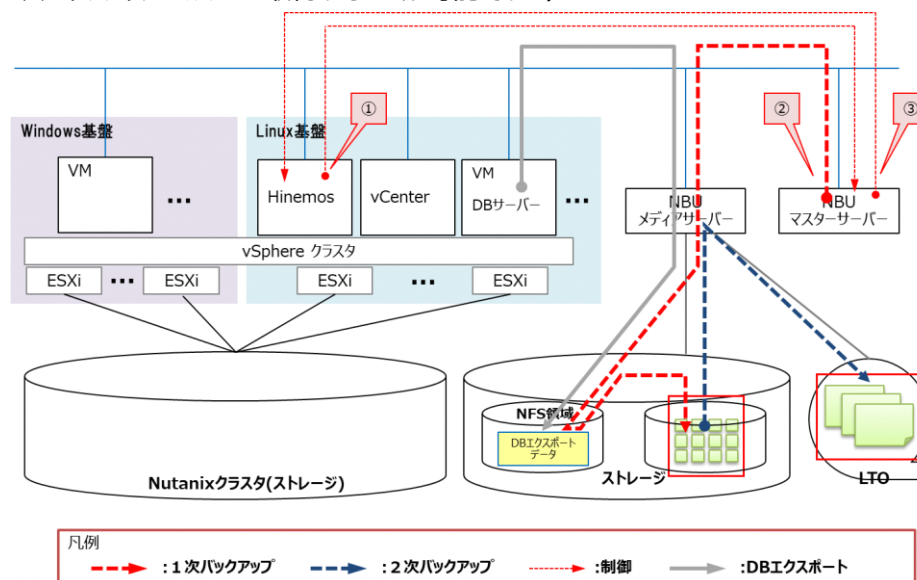
No	処理項目	処理内容
①	ジョブ開始	運用管理サーバー（Hinemos）より、バックアップジョブを開始する。 ・NBU マスターサーバーへバックアップポリシー実行の指示。
②	バックアップ処理	NBU マスターサーバーでバックアップポリシーが開始する。 ・NBU メディアサーバーへバックアップ実行の指示。 ・NBUClient 経由で対象サーバーのデータをストレージ（VSP G150）へバックアップ。
③	ジョブ完了	NBU マスターサーバーでバックアップポリシー完了後、運用管理サーバーよりバックアップ用ジョブを完了する。 ・NBU マスターサーバーのバックアップポリシー完了を確認。

4.6.3. データバックアップ（オプションサービス）

NBU の機能によって NBU メディアサーバーの 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 DB サーバーにおけるデータエクスポート等のバックアップ実行結果（バックアップデータ）を格納する NFS 領域を NBU メディアサーバーに作成し、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、バックアップ実行後に結果（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。）

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	運用管理サーバー(Hinemos)より、バックアップジョブを開始する。 ・NBU マスターサーバーへバックアップポリシー実行の指示。 （DB サーバーからストレージ（VSP G150）の NFS 領域へのデータエクスポートは事前に実施済）
②	バックアップ処理	NBU マスターサーバーでバックアップポリシーが開始する。 ・NBU メディアサーバーがバックアップデータを、ストレージ（VSP G150）へバックアップ。
③	ジョブ完了	NBU マスターサーバーでバックアップポリシー完了後、運用管理サーバーよりバックアップジョブを完了する。 ・NBU マスターサーバー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。

4.7. 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、情報共有基盤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

分散ファイアウォールは廃止しました。必要に応じて、業務システム事業者にて Windows ファイアウォール等の設定を実施してください。

5.1.2. 仮想マシンに導入するウイルス対策

仮想マシン OS には、ウイルス対策ソフト(McAfee エージェント)がインストールされています。このウイルス対策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、情報共有基盤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、情報共有基盤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、情報共有基盤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、情報共有基盤所管部門の指示に従ってください。

- ¥¥kbmvm-fs01sv¥仮想基盤連絡用¥100_参考情報¥01_OS パッチ情報¥仮想基盤 2022

[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のアカウント・パスワードが定義されています。詳細は、仮想マシン払い出し時に提供される「仮想マシン作成報告書」のアカウント一覧情報を確認してください。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、サーバー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。

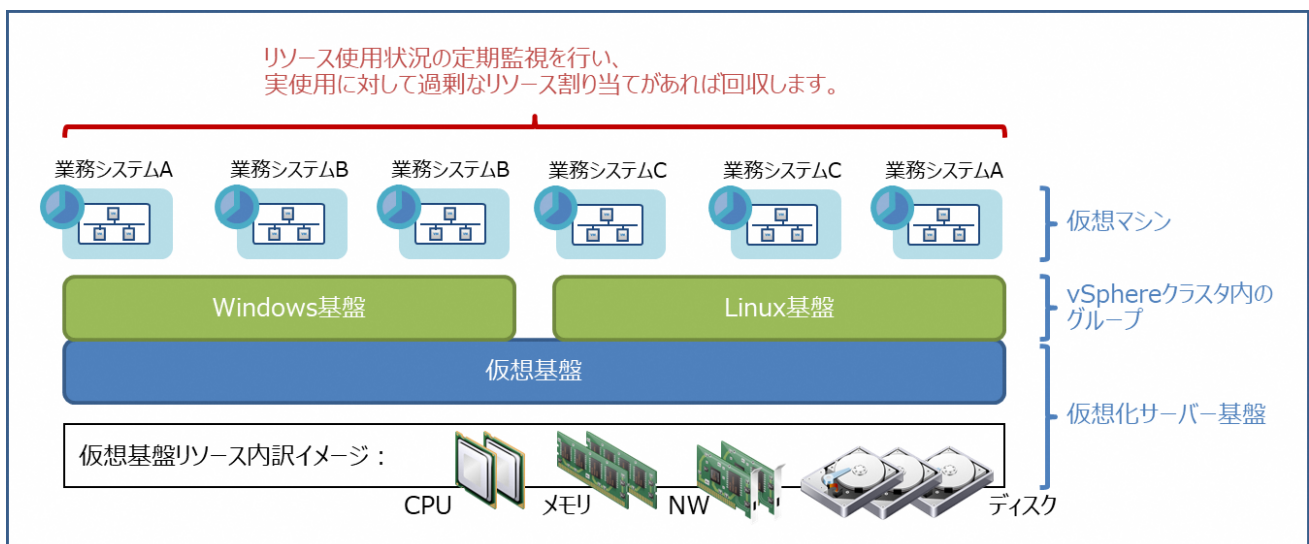
回収とは、例えば仮想マシンに CPU を 4 コア割り当てているが実際の使用状況が常に 2 コアを下回っている場合、仮想マシン設定を 4 コアから 2 コアにダウンサイジングさせていただくことになります。

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。

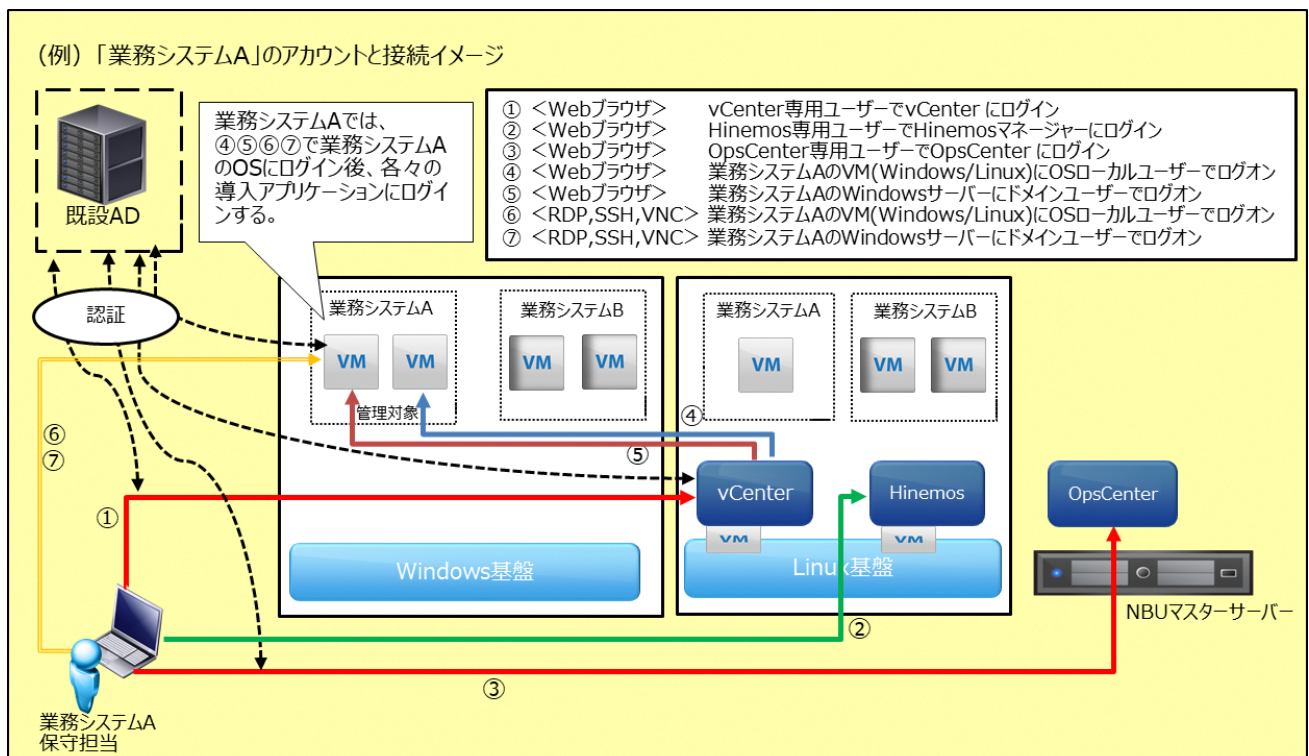


● …CPU、メモリ、ディスク領域などの割り当てリソースのイメージ
 リソースの使用状況に応じて、割り当てを小さく ⇒ したり、大きく ⇒ します。

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。



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。サーバー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、情報共有基盤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	一般ユーザー	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	ドメインユーザー	一般ユーザー	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	vCenter	製品個別	一般ユーザー	仮想基盤事業者	① (※1)	電源 OFF/ON、端末コンソール操作
6	OpsCenter	製品個別	一般ユーザー	仮想基盤事業者	③ (※2)	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
7	Hinemos	製品個別	一般ユーザー	仮想基盤事業者	② (※1)	ジョブ定義の設定、監視の有効・無効化

(※1) vCenter および Hinemos 接続に使用する Web ブラウザについては、「Google Chrome バージョン 92.0」以上を使用してください。

(※2) 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 95.0」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	ドメインユーザー	業務システム事業者
5	vCenter	製品個別	業務システム事業者
6	OpsCenter	製品個別	業務システム事業者
7	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。
- ハイパーバイザー（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、基盤システムにて提供している McAfee（ウイルス対策ソフト）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以前のバージョンにおいて報告されています。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物理 LB についてはセッションタイムアウト間隔:3600 秒、パーシステンスタイムアウトが 300 秒（業務要件に応じ、3,600 秒への変更可能）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 等の情報は情報共有基盤所管部門に確認してください。

以上

電子計算機処理等の契約に関する情報取扱特記事項

(情報を取り扱う際の基本的事項)

第1条 この特記事項(以下「特記事項」という。)は、委託契約約款(以下「約款」という。)の特記条項として、電子計算機処理等の委託契約に関する横浜市(以下「委託者」という。)が保有する情報の取扱いについて、必要な事項を定めるものである。

2 情報を電子計算機処理等により取り扱う者(以下「受託者」という。)は、情報の保護の重要性を認識し、この契約による業務(以下「本件業務」という。)を遂行するための情報の取扱いに当たっては、委託者の業務に支障が生じることのないよう、適正に取り扱わなければならない。

(定義)

第2条 特記事項において、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) 電子計算機処理等 電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。ただし、専ら文章を作成するための処理、専ら文書図画の内容を記録するための処理、製販その他の専ら印刷物を制作するための処理及び専ら文書図画の内容の伝達を電気通信の方法により行うための処理を除く。

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

(3) 不開示資料等 不開示情報が記録された、文書、図画、写真、フィルム及び電磁的記録をいう。

(適正な管理)

第3条 受託者は、本件業務に係る情報の漏えい、滅失、毀損及び改ざん等(以下「漏えい等」という。)の防止その他の情報の適正な管理のために必要な措置を講じなければならない。

2 受託者は、情報の取扱いに関する規程類を整備するとともに、情報の適正な管理を実施する者として本件業務に係る情報の管理責任者を選任しなければならない。

3 受託者は、電子計算機を設置する場所、情報を保管する場所その他の情報を取り扱う場所(以下「作業場所」という。)を定めるとともに、作業場所に係る入退室の規制、防災・防犯対策その他の安全対策を講じなければならない。

4 受託者は、本件業務に着手する前に前3項に定める管理責任体制及び安全対策その他の安全管理措置について、委託者に報告しなければならない。

5 受託者は、前項の規定により報告した事項に関し、委託者が理由を示して異議を申し出た場合には、当該異議に関する事項を変更しなければならない。この場合において、当該変更を経費を要するときは、その費用負担は委託者と受託者とが協議して決定する。

(従事者の監督)

第4条 受託者は、本件業務に従事している者が、本件業務に関して知り得た不開示情報をみだりに他人に知らせ、又は不当な目的に使用しないよう、必要かつ適切な監督を行わなければならない。この契約が終了し、又は解除された後においても同様とする。

(収集の制限)

第5条 受託者は、本件業務を遂行するために必要な範囲内で、適正かつ公正な手段により情報を収集しなければならない。

(禁止事項)

第6条 受託者は、あらかじめ委託者の指示又は承諾があった場合を除き、本件業務に係る情報に関し、次に掲げる行為をしてはならない。

(1) 本件業務を処理する目的以外での利用

(2) 複写又は複製(作業場所内において効率的に作業を進めるためにやむを得ないものを除く)

(3) 作業場所の外への持ち出し

(再委託の禁止等)

第7条 受託者は、本件業務を遂行するための不開示情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、あらかじめ、委託者の書面による承諾を得た場合は、この限りでない。

2 受託者は、前項ただし書の承諾を得て、本件業務に係る情報を第三者に取り扱わせる場合には、情報の保護に関し、特記事項と同等の内容及び委託者が指示する事項について、当該第三者(会社法(平成17年法律第86号)第2条第1項第3号の子会社を含む。以下「再受託者」という。)との間で約定しなければならない。2以上の段階にわたる委託(以下「再々委託等」という。)を行う場合も、この例によるべきことを再受託者又はこれに類する者に求めなければならない。

3 再受託者が本件業務に係る情報を第三者に取り扱わせる場合にあっては、受託者は、当該第三者(会社法第2条第1項第3号の子会社を含む。)における情報の取扱いに係る管理体制をあらかじめ確認し、当該確認内容を委託者に報告し、委託者の書面による承諾を受けた上でなければ、第1項ただし書の承諾に相当する承諾をしてはならない。再々委託等を行う場合も、同様とする。

4 業務内容が定型的であり、かつ、情報の漏えい等の危険性が低いものとして委託者が別に定める業務の委託(再委託及び再々委託等(以下「再委託等」と総称する。))を含む。)については、委託者が別に定める事項をあらかじめ

め委託者に報告した場合には、第1項ただし書の承諾及び前項に規定する受託者による承諾を要しない。

5 第3条第5項の規定は、前項に規定する報告について準用する。

(不開示資料等の返還等)

第8条 受託者は、本件業務を遂行するために委託者から貸与され、又は受託者が収集し、複製し、若しくは作成した不開示資料等を、業務の遂行上使用しないこととなったとき又はこの契約が終了したとき若しくは解除されたときは、委託者の指示に従い、直ちに委託者に返還し、若しくは引き渡し、若しくは消去し、又はその他の方法により処理(以下「返還等」という。)するものとする。

2 前項の場合において、委託者が当該不開示資料等の消去又はその他の方法による処理を指示した場合は、復元困難な消去、焼却、シュレッダー等による裁断等当該情報が第三者の利用に供されることのない方法によらなければならない。

3 第1項の場合において、受託者が正当な理由なく指定された期限内に不開示資料等の返還等をしないときは、委託者は、受託者に代わって当該不開示資料等を回収し、又は廃棄することができる。この場合において、受託者は、委託者の回収又は廃棄について異議を申し出ることができず、委託者の回収又は廃棄に要した費用を負担しなければならない。

(報告及び検査)

第9条 委託者は、情報を保護するために必要な限度において、委託契約期間中、受託者に対して、情報の管理の状況及び委託業務の履行状況について、報告を求めることができる。

2 委託者は、委託契約期間中必要と認められた場合は、情報の管理の状況及び委託業務の履行状況について、作業場所において検査することができる。

3 前2項の場合において、報告又は検査に直接必要な費用は、受託者の負担とする。ただし、委託者の事情により、過分の費用を要した分については、委託者が負担する。

(事故発生時等における報告)

第10条 受託者は、委託者の提供した情報並びに受託者及び再受託者が本件業務のために収集した情報について、火災その他の災害、盗難、漏えい、改ざん、破壊、コンピュータウイルスによる被害、不正な利用、不正アクセス等の事故が生じたとき、又は生ずるおそれがあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

(引渡し)

第11条 受託者は、約款第28条第2項の規定による検査(以下「検査」という。)に合格したときは、直ちに、契約の履行の目的物を納品書を添えて委託者の指定する場所に納入するものとし、納入が完了した時をもって契約の履行の目的物の引渡しを完了したものとする。

(契約の解除及び損害の賠償)

第12条 委託者は、次のいずれかに該当するときは、この契約を解除し、又は受託者に対して損害賠償を請求することができる。

(1) 本件業務を遂行するために受託者が取り扱う不開示情報について、受託者の責に帰すべき理由による漏えい等があったとき。

(2) 前号に掲げる場合のほか、特記事項に違反し、本件業務の目的を達成することができないと認められるとき。

2 前項第1号の不開示情報の漏えい等に伴う損害賠償その他の一切の責任は、不開示情報の漏えい等が、受託者が再委託等をし、当該再委託等先において発生した場合であっても、当該受託者が負うものとする。

3 委託者は、受託者が検査に不合格となったときは、この契約を解除することができる。

(著作権等の取扱い)

第13条 この契約により作成される成果物の著作権等の取扱いについては、約款第5条の規定にかかわらず、次の各号に定めるところによる。

(1) 受託者は、著作権法(昭和45年法律第48号)第21条(複製権)、第26条の3(貸与権)、第27条(翻訳権、翻案権等)及び第28条(二次的著作物の利用に関する原著者の権利)に規定する権利を、目的物の引渡し時に委託者に無償で譲渡するものとする。

(2) 委託者は、著作権法第20条(同一性保持権)第2項第3号又は第4号に該当しない場合においても、その使用のために、この契約により作成される目的物を改変し、任意の著作者名で任意に公表できるものとする。

(3) 受託者は、委託者の書面による事前の同意を得なければ、著作権法第18条(公表権)及び第19条(氏名表示権)を行使することができないものとする。

(4) 受託者がこの契約の締結前から権利を有している著作物の著作権は、受託者に留保されるものとする。この場合において、受託者は、委託者に対し、当該著作物について、委託者が契約の履行の目的物を使用するために必要な範囲で、著作権法に基づく利用を無償で許諾するものとする。

2 前項の規定にかかわらず、著作物の利用について設計図書で別段の定めをした場合には、その図書の定めに従うものとする。

3 受託者は、この契約によるすべての成果物が、第三者の著作権、特許権その他の権利を侵害していないことを保証するものとする。ただし、委託者の責に帰すべき事由に起因する権利侵害となる場合は、この限りではない。

(最近改正：令和5年4月1日)

個人情報取扱特記事項

(令和5年4月)

(個人情報を取り扱う際の基本的事項)

第1条 横浜市（以下「委託者」という。）がこの特記事項が付帯する契約（以下「この契約」という。）において個人情報を取り扱わせる者（以下「受託者」という。）は、個人情報の重要性を認識し、この契約による事務（以下「本件事務」という。）を処理するに当たっては、個人情報の保護に関する法律、横浜市個人情報の保護に関する条例その他の関係法令等を遵守し、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

(適正な管理)

第2条 受託者は、本件事務に係る個人情報の漏えい、滅失、毀損及び改ざん等（以下「漏えい等」という。）の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

2 受託者は、個人情報の取扱いに関する規程類を整備するとともに、本件事務に係る個人情報の管理責任者を選任しなければならない。

3 受託者は、個人情報を取り扱う場所及び保管する場所（以下「作業場所」という。）を定めるとともに、作業場所に係る入退室の規制、防災・防犯対策その他の安全対策を講じなければならない。

4 受託者は、本件事務に係る個人情報の取扱いに着手する前に前3項に定める管理責任体制、安全対策その他の安全管理措置について、安全管理措置報告書（第1号様式）により委託者に報告しなければならない。

5 受託者は、前項の規定により報告した事項に関し、委託者が理由を示して異議を申し出た場合には、当該異議に関する事項を変更しなければならない。この場合において、当該変更を経費を要するときは、その費用負担は委託者と受託者とが協議して決定する。

(従事者の監督)

第3条 受託者は、本件事務の処理に従事している者が本件事務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用しないよう必要かつ適切な監督を行わなければならない。この契約が終了し、又は解除された後においても同様とする。

(収集の制限)

第4条 受託者は、本件事務を処理するために必要な範囲内で、適正かつ公正な手段により個人情報を収集しなければならない。

(禁止事項)

第5条 受託者は、あらかじめ委託者の指示又は承諾があった場合を除き、本件事務に係る個人情報に関し、次に掲げる行為をしてはならない。

- (1) 本件事務を処理する目的以外での利用
- (2) 複写又は複製（作業場所内において効率的に作業を進めるためにやむを得ないものを

除く。)

(3) 作業場所の外への持ち出し

(再委託の禁止等)

第6条 受託者は、本件事務を処理するための個人情報を自ら取り扱うものとし、第三者に取り扱わせてはならない。ただし、あらかじめ、委託者の書面による承諾を得た場合はこの限りでない。

2 受託者は、前項ただし書の承諾を得て、本件事務に係る個人情報を第三者に取り扱わせる場合には、個人情報の保護に関し、本特記事項と同等の内容及び委託者が指示する事項について、当該第三者（会社法（平成17年法律第86号）第2条第1項第3号の子会社を含む。以下「再受託者」という。）との間で約定しなければならない。2以上の段階にわたる委託（以下「再々委託等」という。）を行う場合も、この例によるべきことを再受託者又はこれに類する者に求めなければならない。

3 再受託者が本件事務に係る個人情報を第三者に取り扱わせる場合にあっては、受託者は、当該第三者（会社法第2条第1項第3号の子会社を含む。以下「再々受託者」という。）における個人情報の取扱いに係る管理体制をあらかじめ確認し、当該確認内容を委託者に報告し、委託者の書面による承諾を受けた上でなければ、第1項ただし書の承諾に相当する承諾をしてはならない。再々委託等を行う場合も、同様とする。

4 業務内容が定型的であり、かつ、個人情報の漏えい等の危険性が低いものとして委託者が別に定める業務の委託（再委託及び再々委託等（以下「再委託等」と総称する。）を含む。）については、委託者が別に定める事項をあらかじめ委託者に報告した場合には、第1項ただし書の承諾及び前項に規定する受託者による承諾を要しない。

5 第2条第5項の規定は、前項に規定する報告について準用する。

(個人情報記録された資料等の返還等)

第7条 受託者は、本件事務を処理するために委託者から貸与され、又は受託者が収集し、複製し、若しくは作成した個人情報が記録された資料等を、業務の遂行上使用しないこととなったとき又はこの契約が終了したとき若しくは解除されたときは、委託者の指示に従い、直ちに委託者に返還し、若しくは引き渡し、若しくは消去し、又はその他の方法により処理するものとする。

(報告及び検査)

第8条 委託者は、個人情報を保護するために必要な限度において、委託契約期間中、受託者に対し、個人情報の管理状況及び委託業務の履行状況について報告を求めることができる。

2 委託者は、個人情報を保護するために必要な限度において、委託契約期間中少なくとも1年に一度、情報の管理の状況及び委託業務の履行状況について、原則として作業場所において検査するものとする。

3 前2項の場合において、報告、資料の提出又は検査に直接必要な費用は、受託者の負担とする。ただし、委託者の事情により過分の費用を要した分については、委託者が負担する。

(事故発生時等における報告)

第9条 受託者は、個人情報の漏えい等の事故が生じ、又は生ずるおそれがあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

(研修実施報告書の提出)

第10条 受託者は、従事者に対し、個人情報を取り扱う場合に従事者が遵守すべき事項、個人情報の保護に関する法令等に基づく罰則の内容及び個人情報の漏えい等が生じた際に負う民事上の責任についての研修を実施し、研修実施報告書(第2号様式)を委託者に提出しなければならない。

2 受託者は、個人情報を取り扱う事務を再受託者に委託する場合には、再受託者に対し、前項の研修を実施させ、同項の研修実施報告書を受託者に提出させなければならない。

3 前項の場合において、受託者は、再受託者から提出された研修実施報告書を委託者に提出しなければならない。

(契約の解除及び損害の賠償)

第11条 委託者は、次のいずれかに該当するときは、この契約を解除し、又は受託者に対して損害賠償の請求をすることができる。

(1) 本件事務を処理するために受託者が取り扱う個人情報について、受託者の責に帰すべき理由による個人情報の漏えい等があったとき。

(2) 前号に掲げる場合のほか、この特記事項に違反し、本件事務の目的を達成することができないと認められるとき。

2 前項第1号の個人情報の漏えい等に伴う損害賠償その他の一切の責任は、個人情報の漏えい等が、受託者が再委託等をし当該再委託等先において発生した場合であっても、当該受託者が負うものとする。

年 月 日

(提出先)

(提出者)

団体名

責任者職氏名

研修実施報告書・誓約書

個人情報保護に関する法律第66条第2項の規定により準用される同条第1項に定める措置の一環として、横浜市の個人情報を取り扱う事務に従事する者に対し、個人情報を取り扱う場合に遵守すべき事項並びに個人情報保護に関する法令等に基づく罰則の内容及び漏えい等の事故が発生した場合の民事上の責任についての研修を実施しましたので、別紙(全枚)のとおり報告いたします。

個人情報保護に関する法令等及び個人情報取扱特記事項を遵守し、並びに従事者にも遵守させ、個人情報を適切に取り扱うことを誓約いたします。

