【C-1】
非機能要件の整理結果

はじめに

1 概要

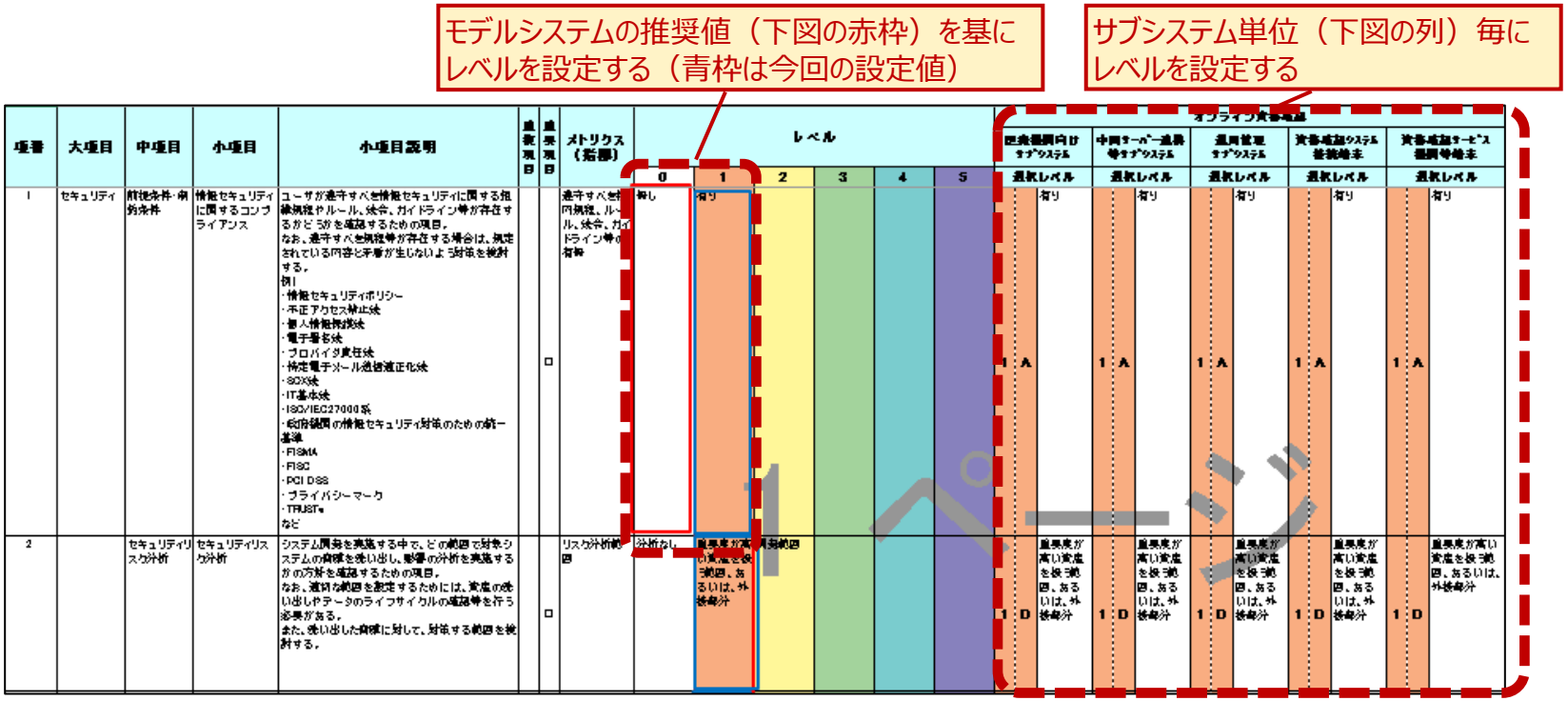
- 本資料は、オンライン資格確認システムの非機能要件を整理するにあたり、前提としたシステム分割案とモデルシステムの選定結果を説明する資料である。
- 非機能要件は、IPA（情報処理推進機構）の非機能要求グレード活用シート*を参考に整理する。
- 非機能要件は、オンライン資格確認を構成する機器と設備の設置場所や役割により異なるため、グレード表を作成するにあたり、オンライン資格確認サービスをサブシステム毎に分割する。
- 記載方法は、中間サーバー等基盤基本設計書を参考にする。

※IPA（情報処理推進機構）非機能要求グレード： https://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html

はじめに

2 サブシステム構成毎に分割した非機能要求グレード

- 非機能要求グレード表の各要求項目は、後述の「サブシステム」(端末も含む)毎に選択レベルを設定する。
  （★後述「非機能要求グレード 前提① サブシステム分割定義」参照）
- 非機能要求グレード表の各要求項目は、「モデルシステム」に応じたIPAのベース値（推奨値）を参考にする。
  （★後述「非機能要求グレード 前提② モデルシステム選定」参照）



非機能要求グレードのイメージ

非機能要求グレード 前提① サブシステム分割定義

非機能要求グレード 前提① サブシステム分割定義

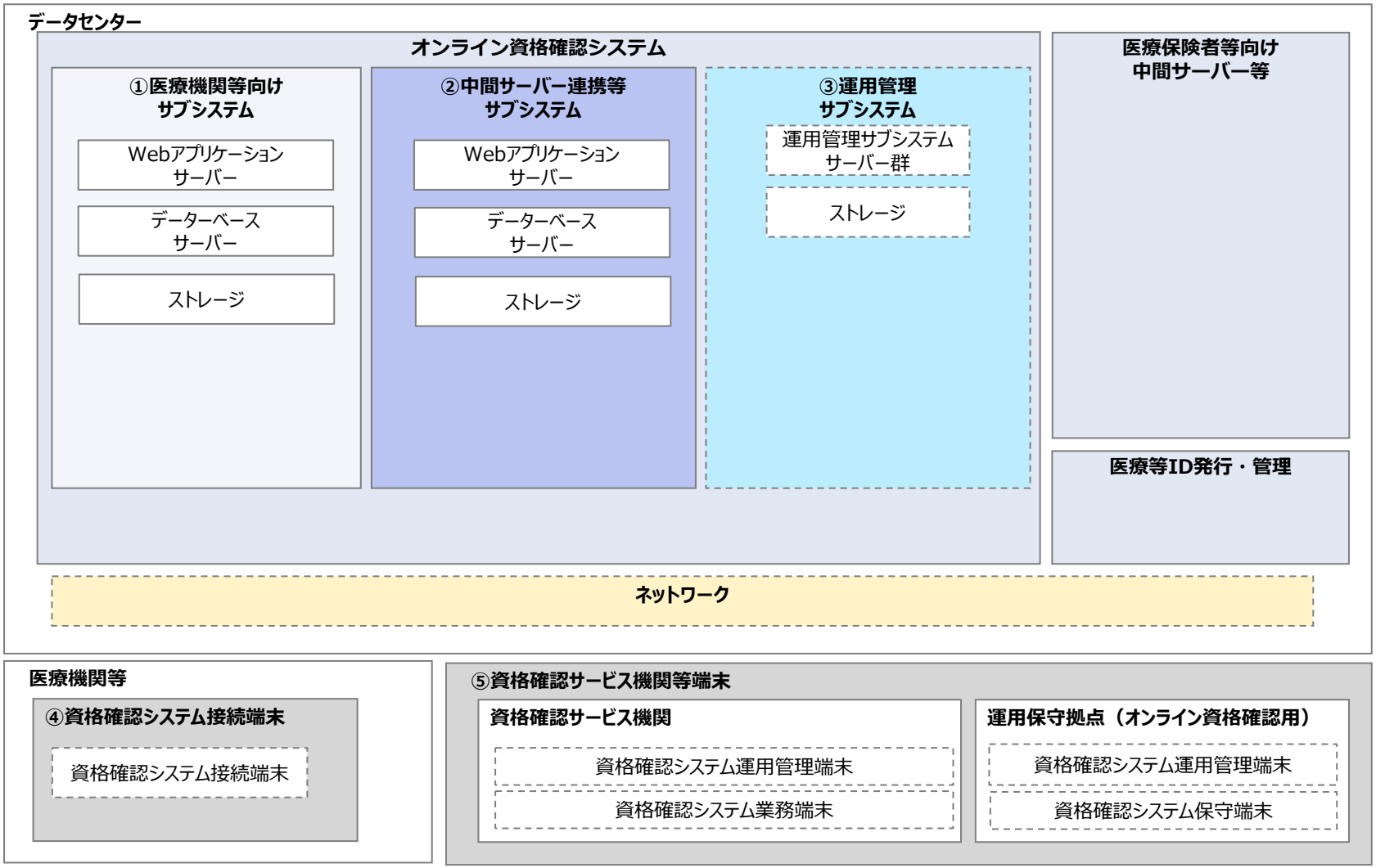
1 サブシステム一覧（案）

- 非機能要求グレードを整理するにあたり、下記の①～⑤に分割し、それぞれに選択レベルを設定する。
- ①から③は、サーバー側システムのサブシステム。④と⑤はクライアント端末である。
  （非機能要件整理では、①～⑤を総称して「サブシステム」と呼ぶ）

項番	名称	説明
①	医療機関等向けサブシステム	医療機関等からの要求を受付け、(PINなし)認証と資格情報の照会・提供を行う。 また、オンライン資格確認が医療等ID発行・管理機関との連携で必要な機能も含む。
②	中間サーバー連携等サブシステム	医療保険者等向け中間サーバー等から資格確認に必要な情報を収集する。 また、オンライン資格確認を運営する上で必要なマスタメンテ、アカウント管理、証跡管理等を行う。
③	運用管理サブシステム	統合監視/バックアップ/バッチ管理等のシステム運用管理や保守を行う。 本番環境のほか、保守環境や検証環境の全てに機能を提供する。
④	資格確認システム接続端末	医療機関等からオンライン資格確認システム（①医療機関向けサブシステム）に接続し、資格確認サービスを利用する端末。
⑤	資格確認サービス機関等端末	資格確認サービス機関等からオンライン資格確認システム（②中間サーバー連携等サブシステム及び③運用管理サブシステム）に接続し、オンライン資格確認を運営する上で必要な業務や運用管理業務、保守作業等を行う端末。

非機能要求グレード 前提① サブシステム分割定義

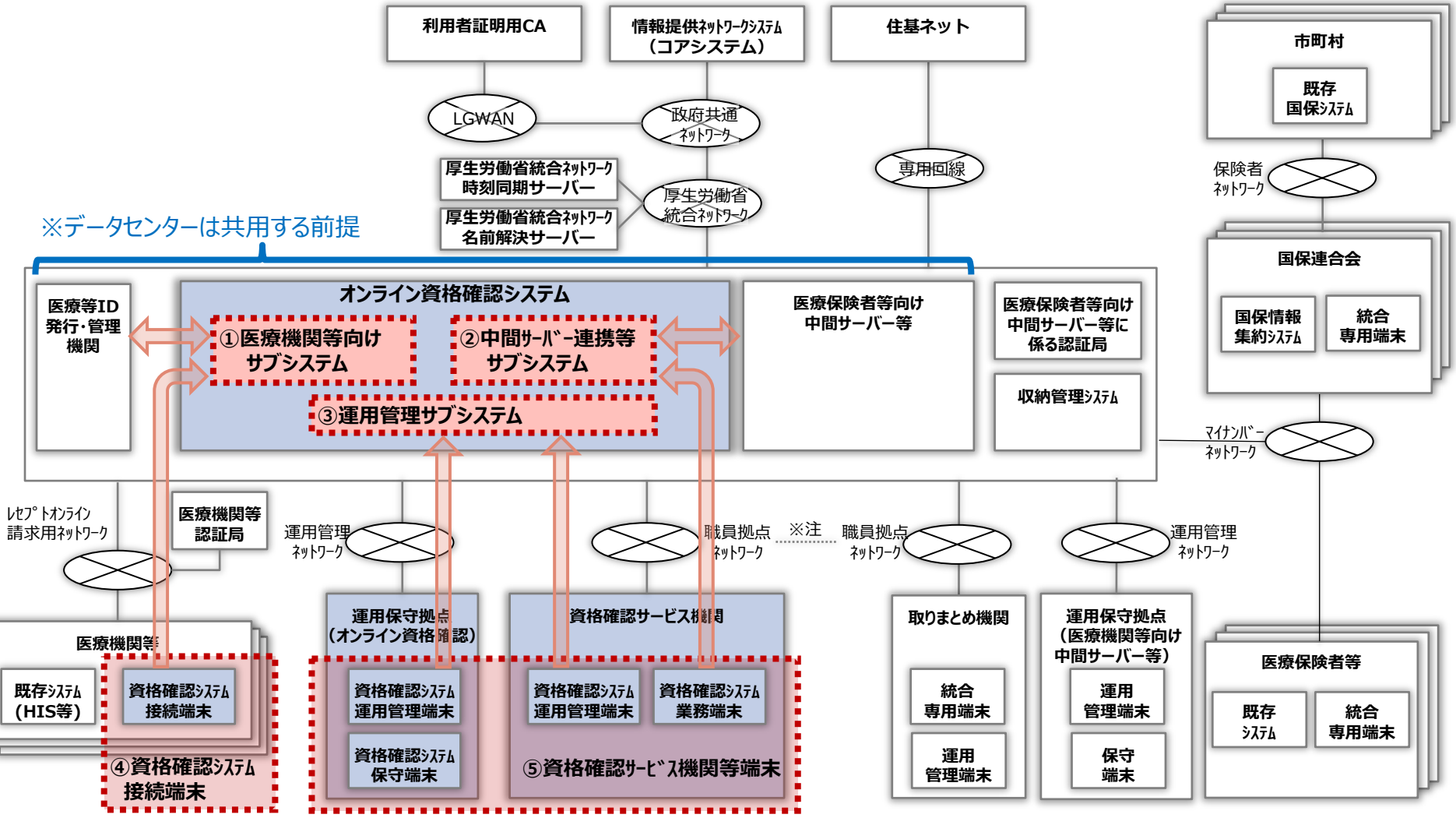
2 構成図（案）



非機能要求グレード 前提① サブシステム分割定義

3 概要図（案）

- 前述のサブシステム分割イメージと、オンライン資格確認を取り巻く全体構成イメージを以下に示す。



※注：「職員拠点ﾈｯﾄﾜｰｸ」は、運営者が同じ支払基金及び中央会であれば共用可能と考えられる。

非機能要求グレード 前提② モデルシステム選定

非機能要求グレード 前提② モデルシステム選定

1 非機能要求グレード　モデルシステム選定（仮定）

- 「非機能要求グレード」には、各要件を決定する上での基準となる3種類の「モデルシステム」（表１　モデルシステムの概要）が定義され、それぞれのモデルシステムに応じて各要件のレベルの推奨値（ベース値）が定められている。
- オンライン資格確認では以下の理由から、「社会的影響が限定されるシステム」であると仮定する。

本システムの機能が低下または利用不可能な状態に陥った場合、医療機関等での診療受付や医事会計業務に影響を及ぼすと共に、患者にも手間や時間をかけてしまう等の混乱を来たす可能性がある。（ただし、それにより国民生活・社会経済活動に多大な影響を与えるものではない。）
また、本システムは不特定多数ではなく、システム利用の手続きを行った保険医療機関等からしか利用できないように認証、制限を行うことを想定している。

表1：モデルシステムの概要

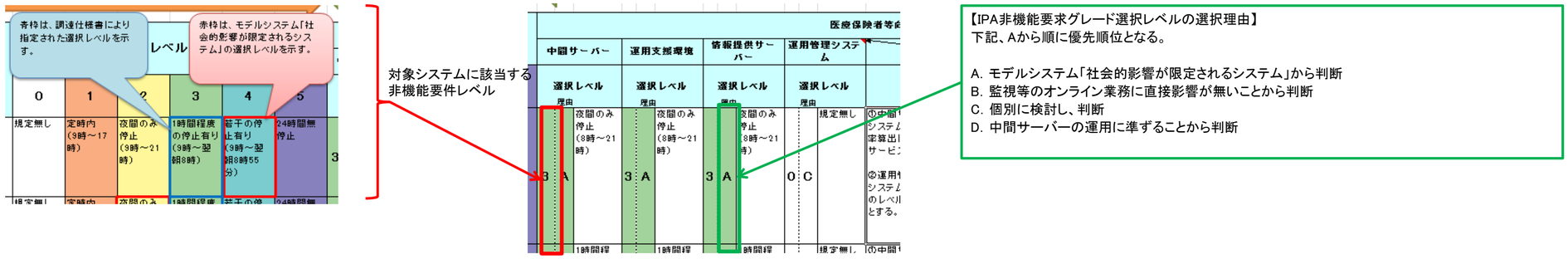
モデルシステム名	社会的影響が殆ど無いシステム	社会的影響が限定されるシステム	社会的影響が極めて大きいシステム
概要	企業の特定部門が比較的限られた範囲で利用しているシステムで、機能が低下または利用不可な状態になった場合、利用部門では大きな影響があるが、その他には影響しないもの。 ここでは、ごく小規模のインターネット公開システムを想定している。	企業活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、当該企業活動に多大の影響を及ぼすと共に取引先や顧客等の外部利用者にも影響を及ぼすもの。 ここでは、企業内のネットワークに限定した基幹システムを想定している。	国民生活・社会経済活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、国民生活・社会経済活動に多大な影響を与えるもの。 ここでは、不特定多数の人が利用するインフラシステムを想定している。

※本システムではモデルとして「社会的影響が限定されるシステム」を採用

- なお、医療保険者等向け中間サーバー等の要件定義でも、モデルシステムとして「社会的影響が限定されるシステム」が採用されている。

（1）選択レベルの表記例

以下に本資料の表記例を示します。



（2）非機能要件及び選択レベル

非機能要求グレード活用シート(原本の範囲)　→　要件定義工程における検討結果

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 運用管理ｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 資格確認ｼｽﾃﾑ接続端末 選択レベル	理由	オンライン資格確認 資格確認ｻｰﾋﾞｽ機関等端末 選択レベル	理由	選択理由
1	可用性	継続性	運用スケジュール	システムの稼動時間や停止運用に関する情報。	○	○	サービス時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	2 C	夜間のみ停止（8時～21時） ※診療開始が8時からの医療機関を考慮し開始時間を変更	3 C	2時間程度の停止有り（21時～翌朝8時の任意の2時間停止） ※中間サーバー等のバックアップ時間を考慮し停止時間を2時間へ変更	0 B	規定無し	2 C	夜間のみ停止（8時～21時） ※診療開始が8時からの医療機関を考慮し開始時間を変更	0 B	規定無し	■医療機関等向けサブシステム、資格確認ｼｽﾃﾑ接続端末 医療機関からの利用時間. ■中間ｻｰﾊﾞｰ連携等サブシステム 資格情報等の同期を行うバッチ実行のため、医療保険者等向け中間サーバー等を利用する. 当該システムのバックアップ時間（04:00～6:00）はサービス停止とする. ■運用管理サブシステム 外部に提供しているサービスを持たないため、レベル0（規定無し）とする。 ■資格確認ｻｰﾋﾞｽ機関等端末 運用保守作業等で利用するため、レベル0（規定無し）とする。
2					○	○	サービス時間（特定日 ）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	0 C	規定無し	0 C	規定無し	0 C	規定無し	0 C	規定無し	0 C	規定無し	全業務特定日なし
3					○	○	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				1 C	計画停止有り（運用スケジュールの変更不可）	1 C	計画停止有り（運用スケジュールの変更不可）	0 B	計画停止有り（運用スケジュールの変更可）	－ －	－	－ －	－	－ －	－	■医療機関等向けサブシステム、中間ｻｰﾊﾞｰ連携等サブシステム 計画停止は有りとするが、医療機関等向けサブシステムのサービス時間「08:00～21:00」を変更しない。 ■運用管理サブシステム 当該サブシステムは、サービス提供しないため運用スケジュールを変更して良いので、レベル0とする。

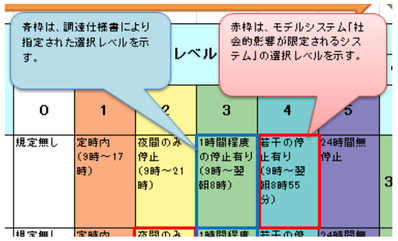
項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル	理由	オンライン資格確認 中間サーバー連携等サブシステム 選択レベル	理由	オンライン資格確認 運用管理サブシステム 選択レベル	理由	オンライン資格確認 資格確認システム接続端末 選択レベル	理由	オンライン資格確認 資格確認サービス機関等端末 選択レベル	理由	選択理由
4			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。		○	対象業務範囲	内部向けバッチ系業務	内部向けオンライン系業務	内部向け全業務	外部向けバッチ系業務	外部向けオンライン系業務	全ての業務	4 C	外部向けオンライン系業務	3 C	外部向けバッチ系業務	2 B	内部向け全業務	– – –	– – –	– – –	– – –	■医療機関等向けサブシステム 外部向けオンライン機能が直接的にユーザーに提供するサービスであるから、レベル4とする。 ■中間サーバー連携等サブシステム 医療機関等向けサブシステムの外部向けオンライン機能が、外部向けバッチ機能が出力するデータに依存しているから、レベル3とする。 ■運用管理サブシステム 業務に対してサービス時間帯に影響のある業務（業務バッチ処理等）について対象の範囲とするため、レベル2とする。
5						○	業務継続の要求度	障害時の業務停止を許容する	単一障害時は業務停止を許容せず、処理を継続させる	二重障害時でもサービス切替時間の規定内で継続する				2 A	二重障害時でもサービス切替時間の規定内で継続する	2 A	二重障害時でもサービス切替時間の規定内で継続する	2 A	二重障害時でもサービス切替時間の規定内で継続する	– – –	– – –	– – –	– – –	医療機関等へ、広くサービスを提供しており、フェーズ2において、全24万医療機関等と接続した場合、システム停止による業務への影響は非常に大きいため、できるだけ業務継続することが要求される。このやめ、選定レベルをレベル2とする。 合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であり、選択したレベルは適切であると考える。 ※ただし、信頼性指標（故障率と平均故障確率）を勘案し、二重障害について対応が不要と判断される場合、レベル1とする。
6						○	サービス切替時間	24時間以上	24時間未満	2時間未満	60分未満	10分未満	60秒未満	3 A	60分未満	3 A	60分未満	3 A	60分未満	– – –	– – –	– – –	– – –	本システムは複数の役割を持つサーバーで構成されることが想定されており、そこで採用する冗長方式も複数方式になることが想定されている。サービス切替時間を60分未満とすることで、柔軟な冗長構成を選択し、費用増大を防止することが可能となる（多重障害の場合を除く）。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは3であり、選択したレベルは適切であると考える。
7			稼動率	明示された利用条件の下で、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動している条件を指す。その稼動時間の中で、サービス中断が発生した時間により稼動率を求める。		○	稼動率	95%以下	95%	99%	99.9%	99.99%	99.999%	4 C	99.99%	3 D	99.9%	0 B	95%以下	– – –	– – –	– – –	– – –	■医療機関等向けサブシステム 医療機関等へ広くサービスを提供するため、24時間365日サービス提供の場合に1時間以下（52.6分）の業務中断（ただし、計画停止時間及び災害発生に伴う停止時間を除く）となる稼働率99.99%を目標とし、レベル4とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と　想定される。この場合、本項目の推奨レベルは4であり、選択したレベルは適切であると考える。 ■中間サーバー連携等サブシステム 連携対象となる医療保険者等向け中間サーバー等の稼働率に合わせ、レベル3とする。 ■運用管理サブシステム 運用管理サブシステムはシステム監視や各サーバーで動作するバッチ処理を制御するサーバー群であり、サービスを提供していないため、稼動率は規定せず、レベル0とする。
8			目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。		○	RPO（目標復旧地点）	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+アーカイブからの復旧）			2 D	1営業日前の時点（日次バックアップからの復旧）	2 D	1営業日前の時点（日次バックアップからの復旧）	2 D	1営業日前の時点（日次バックアップからの復旧）	– – –	– – –	– – –	– – –	■医療機関等向けサブシステム、中間サーバー連携等サブシステム 資格確認に用いる資格情報等の同期を行うバッチ機能では、医療保険者等向け中間サーバー等と連携するため、同システムのRPO（目標復旧地点）に合わせる。 ■運用管理サブシステム 運用統一のため、他サブシステムに合わせる。
9						○	RTO（目標復旧時間）	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		2 A	12時間以内	2 A	12時間以内	2 A	12時間以内	– – –	– – –	– – –	– – –	■医療機関等向けサブシステム、中間サーバー連携等サブシステム 資格確認に用いる資格情報等の同期を行うバッチ機能では、医療保険者等向け中間サーバー等と連携するため、同システムのRTO（目標復旧時間）に合わせる。 ■運用管理サブシステム 運用統一のため、他サブシステムに合わせる。 ※医療保険者等向け中間サーバー等の障害が起因となる場合、連携復旧のためRTO（目標復旧時間）を満たせない可能性がある。業務アプリケーション基本設計で精緻化し、設計結果によっては変更する可能性がある。
10						○	RLO（目標復旧レベル）	システムの復旧	特定業務のみ	全ての業務				2 A	全ての業務	2 A	全ての業務	2 A	全ての業務	– – –	– – –	– – –	– – –	本システムは、多数の業務により構成されており、中には中間サーバー等と連携を行うなど外部システムと関係する業務もある。そのため、業務停止時からの復旧においては全ての業務が復旧することが望ましい。よって、選定レベルをレベル2とする。また、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であるため、選択したレベルは適切であると考える。
11			目標復旧水準（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、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。		○	システム再開目標	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	– –	–	– –	–	– –	–	– –	–	– – –	– – –	– – –	堅牢なデータセンターを採用することにより災害時の倒壊はないとし、大規模災害時にもシステム復旧は不要と想定するため、対象外とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認																選択理由
														医療機関等向けサブシステム			中間サーバー連携等サブシステム			運用管理サブシステム			資格確認システム接続端末			資格確認サービス機関等端末			
								0	1	2	3	4	5	選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		
12		耐障害性	サーバー	サーバーで発生する障害に対して、要求されたサービスを維持するための要求。			冗長化方針（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				1	C	特定のコンポーネントのみ冗長化	1	C	特定のコンポーネントのみ冗長化	1	C	特定のコンポーネントのみ冗長化	–	–	–	–	–	–	原則としてサーバーのコンポーネント（電源・冷却ファン、ハードディスク等）を冗長構成とする。 ただし、マザーボード等、冗長化が不可能または冗長化する場合に費用が大きく増大するコンポーネントについては、機器自体の冗長化により耐障害性を確保するものとするため、レベル1とする。
13							冗長化方針（機器）	非冗長構成	特定のサーバーで冗長化	全てのサーバーで冗長化				2	C	全てのサーバーで冗長化	2	C	全てのサーバーで冗長化	2	C	全てのサーバーで冗長化	–	–	–	–	–	–	単一障害点を極力排除し、耐障害性を確保するため、機器自体を冗長化するため、レベル2とする。 ※ただし、Sorryサーバーについては冗長化不要とする想定。
14			端末	端末で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化方針（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				–	–	– （端末なし）	–	–	– （端末なし）	–	–	– （端末なし）	その他	C	各医療機関等の端末要件による	0	C	資格確認サービス機関等の端末要件による	端末は各機関の管理下にあるため、各機関の端末要件に従う。
15							冗長化方針（機器）	非冗長構成	共用の予備端末を設置	業務や用途毎に予備端末を設置				–	–	– （端末なし）	–	–	– （端末なし）	–	–	– （端末なし）	その他	C	各医療機関等の端末要件による	0	C	資格確認サービス機関等の端末要件による	端末は各機関の管理下にあるため、各機関の端末要件に従う。
16			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化方針（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				1	C	特定のコンポーネントのみ冗長化	1	C	特定のコンポーネントのみ冗長化	1	C	特定のコンポーネントのみ冗長化	–	–	–	–	–	–	原則として、ネットワーク機器のコンポーネント（電源・冷却ファン等）を冗長構成とする。 ただし、冗長化が不可能または冗長化する場合に費用が大きく増大するコンポーネントについては、機器自体の冗長化により耐障害性を確保するものとするため、レベル1とする。
17							冗長化方針（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				2	C	全ての機器を冗長化	2	C	全ての機器を冗長化	2	C	全ての機器を冗長化	–	–	–	–	–	–	単一障害点を極力排除し、耐障害性を確保するため、機器自体を冗長化するため、レベル2とする。
18			ネットワーク	ネットワークの信頼性を向上させるための要求。			冗長化方針（回線）	冗長化しない	一部冗長化	全て冗長化する				2	C	全て冗長化する	2	C	全て冗長化する	2	C	全て冗長化する	–	–	–	–	–	–	単一障害点を極力排除するため、原則としてネットワーク回線を冗長化する。そのため、レベル2とする。
19							冗長化方針（経路）	冗長化しない	一部冗長化	全て冗長化する				2	C	全て冗長化する	2	C	全て冗長化する	2	C	全て冗長化する	–	–	–	–	–	–	単一障害点を極力排除するため、原則としてネットワーク回線を冗長化する。そのため、レベル2とする。
20							セグメント分割	分割しない	サブシステム単位で分割	用途に応じて分割				2	C	用途に応じて分割	2	C	用途に応じて分割	2	C	用途に応じて分割	–	–	–	–	–	–	適切な単位のセグメント分割を実施するため、レベル2とする。
21			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化方針（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				2	C	全てのコンポーネントを冗長化	2	C	全てのコンポーネントを冗長化	2	C	全てのコンポーネントを冗長化	–	–	–	–	–	–	単一障害点を極力排除するため、原則としてストレージのコンポーネント（電源・冷却ファン等）を冗長構成とする。レベル2とする。
22							冗長化方針（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				0	C	非冗長構成	0	C	非冗長構成	0	C	非冗長構成	–	–	–	–	–	–	ストレージ機器は、その他の機器と比較すると一般的に高額であり、高可用な製品を採用することで障害発生により機器が停止する可能性は極小化可能である。そのため、機器自体の冗長構成は必須とせずレベル0とする。
23							冗長化方針（ディスク）	非冗長構成	RAID5による冗長化	RAID1による冗長化				1	C	RAID5による冗長化	1	C	RAID5による冗長化	1	C	RAID5による冗長化	–	–	–	–	–	–	ストレージに格納するデータは、原則としてRAIDによるデータ冗長化を実施する。 なお、採用する具体的なRAIDレベルについては、データ種別毎に性能等の要件を受けて、適切な方式となるよう基本設計工程で検討することとする。
24			データ保護	データの保護に対しての考え方。	○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	「【C-1-3】運用・保守性要件(バックアップ)」に記載する。
25					○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧				–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	「【C-1-3】運用・保守性要件(バックアップ)」に記載する。
26							データインテグリティ	エラー検出無し	エラー検出のみ	エラー検出＆再試行	データの完全性を保障（エラー検出＆訂正）			2	C	エラー検出＆再試行	2	C	エラー検出＆再試行	2	C	エラー検出＆再試行	–	–	–	–	–	–	医療保険者等向け中間サーバー等と連携したデータを用いるため、同システムの設計に合わせ、レベル2とする。
27		災害対策	システム	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための要求。			復旧方針	復旧しない	限定された構成でシステムを再構築	同一の構成でシステムを再構築	限定された構成をDRサイトで構築	同一の構成をDRサイトで構築		0	C	復旧しない	0	C	復旧しない	0	C	復旧しない	–	–	–	–	–	–	堅牢なデータセンターを採用することにより災害時の倒壊はないとし、大規模災害時にもシステム復旧は不要と想定するため、レベル0とする。
28			外部保管データ	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するなどの要求。			保管場所分散度	外部保管しない	1ヵ所	1ヵ所（遠隔地）	2ヵ所（遠隔地）			0	C	外部保管しない	0	C	外部保管しない	0	C	外部保管しない	–	–	–	–	–	–	堅牢なデータセンターを採用することにより災害時の倒壊はないとし、外部保管は行わない.
29							保管方法	媒体による保管	同一サイト内の別ストレージへのバックアップ	DRサイトへのリモートバックアップ				1	C	同一サイト内の別ストレージへのバックアップ	1	C	同一サイト内の別ストレージへのバックアップ	1	C	同一サイト内の別ストレージへのバックアップ	–	–	–	–	–	–	災害時のシステム復旧は不要だが、被害想定を正確に行うことは困難なため、災害対策の一つとして通常運用で取得したバックアップデータを、同サイト内別ストレージに保管する.
30			付帯設備	各種災害に対するシステムの付帯設備での要求。			災害対策範囲	対策を実施しない	特定の対策を実施する	想定する全ての対策を実施する				1	C	特定の対策を実施する	1	C	特定の対策を実施する	1	C	特定の対策を実施する	–	–	–	–	–	–	「別紙_付帯設備要求」に、具体的な要求事項を記す。
31		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧			–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	「【C-1-3】運用・保守性要件(バックアップ)」に記載する。
32			可用性確認	可用性として要求された項目をどこまで確認するかの範囲。		○	確認範囲	実施しない。または単純な障害の範囲	業務を継続できる障害の範囲	業務停止となる障害のうち一部の範囲	業務停止となる障害の全ての範囲			2	A	業務停止となる障害のうち一部の範囲	2	A	業務停止となる障害のうち一部の範囲	2	A	業務停止となる障害のうち一部の範囲	–	–	–	–	–	–	想定する障害ケースに対する処理・動作についてのテストを実施する方針とする。ただし、全ての障害ケースを再現することは困難であるため障害発生時のサービス切替処理・動作に応じたテスト行う方針とする。また、復旧作業を定義した中で発生リスクが高く業務への影響が大きい障害について計画・実施する方針とする。 したがってレベル2とする。

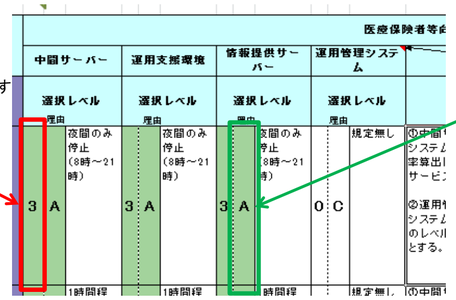
項番	要求内容
①	震度6強の災害に耐えることができる、堅牢なデータセンターであること。
②	機器をマシンルームのラックへ固定して設置できることが可能であり、将来的にラックの増設が必要となった場合にも拡張余地があること。
③	本システムはラック当りの重量を制限して分散構成を採るため、床荷重800Kg/㎡の条件を満たすこと。
④	電源工事を行わなくても、必要とする電力が供給可能であること。
⑤	UPSによる瞬電対策が行われていること。
⑥	自家発電による100%の給電を2日維持できる停電対策が行われていること。
⑦	電圧変動が±10%以下、周波数変動が±2%以下であること。
⑧	個別に接地工事の必要がないこと。
⑨	漏電ブレーカー設置等の漏電対策がとられていること。
⑩	温度が18℃～27℃、湿度が45%～55%であること。
⑪	システム機器が稼動するために十分な冷却能力があり、ホットスポットが発生しないよう熱を効率よく放出するための空調性能を備えていること。また、空調設備に関する制約がないこと。
⑫	上水道が断水していても、空調設備が継続利用可能であること。
⑬	センサーや消火設備設置等の火災対策がとられていること。
⑭	避雷針などの雷害対策がとられていること。
⑮	床や配管へのセンサー設置等の漏水対策がとられていること。
⑯	水害に影響しない立地であること。
⑰	予め取り決めた運用手順を実行できるオペレータが常駐するデータセンターであること。

（1）選択レベルの表記例

以下に本資料の表記例を示します。



対象システムに該当する非機能要件レベル



【IPA非機能要求グレード選択レベルの選択理由】
下記、Aから順に優先順位となる。

A. モデルシステム「社会的影響が限定されるシステム」から判断
B. 監視等のオンライン業務に直接影響が無いことから判断
C. 個別に検討し、判断
D. 中間サーバーの運用に準ずることから判断

（2）非機能要件及び選択レベル

非機能要求グレード活用シート(原本の範囲)　／　要件定義工程における検討結果

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル 理由	医療機関等向けサブシステム 理由	オンライン資格確認 中間サーバー連携等サブシステム 選択レベル 理由	中間サーバー連携等サブシステム 理由	オンライン資格確認 運用管理サブシステム 選択レベル 理由	運用管理サブシステム 理由	資格確認システム接続端末 選択レベル 理由	資格確認システム接続端末 理由	資格確認サービス機関等端末 選択レベル 理由	資格確認サービス機関等端末 理由	選択理由
1	性能・拡張性	業務処理量	通常時/ピーク時の業務量	性能・拡張性に影響を与える業務量。 該当システムの稼動時を想定し、合意する。 それぞれのメトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	○	○	ユーザ数	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				1 C	上限が決まっている	1 C	上限が決まっている	1 C	上限が決まっている	– – –		– – –		■医療機関等向けサブシステム 医療機関等の事務担当者のみなので、上限が決まっている。 ■中間ｻｰﾊﾞｰ連携等サブシステム、運用管理サブシステム 資格確認サービス機関と運用保守事業者の担当者のみなので、上限が決まっている。
2						○	同時アクセス数	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				1 C	同時アクセスの上限が決まっている。	1 C	同時アクセスの上限が決まっている。	1 C	同時アクセスの上限が決まっている。	– – –		– – –		■医療機関等向けサブシステム 組織認証用電子証明書をインストールした医療機関等内の端末のみ接続可能となっており、上限が決まっている。 ■中間ｻｰﾊﾞｰ連携等サブシステム、運用管理サブシステム 資格確認サービス機関と運用保守拠点に配置されている端末のみなので、上限が決まっている。
3						○	データ量	全てのデータ量が明確である	主要なデータ量のみが明確である					業務アプリケーションの基本設計で定義する										業務アプリケーションの基本設計で定義する。
4						○	オンラインリクエスト件数	処理毎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					1 C	主な処理のリクエスト件数のみが明確である	業務アプリケーションの基本設計で定義する	– B	対象外	– – –		– – –		■医療機関等向けサブシステム 対象業務：医療機関等からの資格確認業務（医_01-10～医_01-70） 通常時：約500万件/日、ピーク時：約1000件/秒 ■中間ｻｰﾊﾞｰ連携等サブシステム 対象業務：資格確認サービスで取り扱う資格情報に対する照会（資_01-03） 関係要求事項で精査中 ■運用管理サブシステム 運用管理サブシステムはサービス提供しないため、対象外とする。
5						○	バッチ処理件数	処理単位毎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					業務アプリケーションの基本設計で定義する										

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認												選択理由
								0	1	2	3	4	5	医療機関等向けサブシステム 選択レベル			中間サーバー連携等サブシステム 選択レベル			運用管理サブシステム 選択レベル			資格確認システム接続端末 選択レベル			資格確認サービス機関等端末 選択レベル			
														理由			理由			理由			理由			理由			
6			ピーク特性	ピーク特性は、各処理のピーク時の特性を表わす情報であり、具体的には処理サイクル、ピーク時間(オンライン処理)、開始条件、終了目標時刻、処理サイクル(バッチ処理)等がある。			ピーク特性（オンライン）	標準の非機能要求グレードに項目で不足していたため、「医療保険者向け中間サーバー等」の開発で新規項目を定義した						その他	C	診療時間開始1時間	その他	C	月曜日、土曜日又は祝日明け	その他	C	ピークなし	–	–	–	–	–	–	■医療機関等向けサブシステム 対象業務：医療機関等からの資格確認業務（医_01-10～医_01-70） ■中間ｻｰﾊﾞｰ連携等サブシステム、運用管理サブシステム 対象業務：資格確認サービスで取り扱う資格情報に対する照会（資_01-03）
7							ピーク特性（バッチ）	標準の非機能要求グレードに項目で不足していたため、「医療保険者向け中間サーバー等」の開発で新規項目を定義した						業務アプリケーションの基本設計で定義する												
8			業務量増大度	システム稼動開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率。 必要に応じ、開始日の平均値や、開始後の定常状態との比較を行う場合もある。		○	ユーザ数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	1	C	1.2倍	1	C	1.2倍	1	C	1.2倍	–	–	–	–	–	–	■医療機関等向けサブシステム フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、ユーザー数は医療機関等の機関数に依存する。機関数が大きく増加することはないので、レベル1（1.2倍）とする。 ■中間ｻｰﾊﾞｰ連携等サブシステム、運用管理サブシステム ユーザーは資格確認サービス機関と運用保守事業者の担当者のみである。フェーズ2運用後、担当が大きく増加することはないので、レベル1（1.2倍）とする。
9						○	同時アクセス数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	1	C	1.2倍	1	C	1.2倍	1	C	1.2倍	–	–	–	–	–	–	■医療機関等向けサブシステム フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、同時アクセス数は医療機関等の機関数に依存する。機関数が大きく増加することはないので、レベル1（1.2倍）とする。 ■中間ｻｰﾊﾞｰ連携等サブシステム、運用管理サブシステム 当時アクセス数の最大値は資格確認サービス機関と運用保守事業者の端末数である。。フェーズ2運用後、端末数が大きく増加することはないので、レベル1（1.2倍）とする。
10						○	データ量増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	2	C	1.5倍	1	C	1.2倍	1	C	1.2倍	–	–	–	–	–	–	■医療機関等向けサブシステム フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、データ量はオンラインリクエストログ（処理履歴）が多くを占める。オンラインリクエスト件数と合わせて、レベル2（1.5倍）とする。 ■中間ｻｰﾊﾞｰ連携等サブシステム データ量の多くは資格情報と紐付情報であり、どちらも国民数に比例する。国民数が大きく増加することはないので、レベル1（1.2倍）とする。 ※ただし、資格履歴の持ち方によっては、選択レベルを変更する可能性がある。 ■運用管理サブシステム データ量はシステム規模に依存する。フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、システム規模拡大は計画されていないので、レベル1（1.2倍）とする。
11						○	オンラインリクエスト件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	2	C	1.5倍	2	C	1.5倍	1	C	1.2倍	–	–	–	–	–	–	■医療機関等向けサブシステム フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、オンラインリクエスト件数はレセプト請求件数に依存する。レセプト請求はゆるやかに増加するので、レベル2（1.5倍）とする。 ■中間ｻｰﾊﾞｰ連携等サブシステム フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、主なオンライン業務である対象業務：資格確認サービスで取り扱う資格情報に対する照会（資_01-03）のオンラインリクエスト件数はレセプト請求件数に依存する。レセプト請求はゆるやかに増加するので、レベル2（1.5倍）とする ■運用管理サブシステム オンラインリクエスト件数はシステム規模に依存する。フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、システム規模拡大は計画されていないので、レベル1（1.2倍）とする。
12						○	バッチ処理件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	–	–	–	1	C	1.2倍	1	C	1.2倍	–	–	–	–	–	–	■中間ｻｰﾊﾞｰ連携等サブシステム データ量の多くは資格情報と紐付情報であり、どちらも国民数に比例する。国民数が大きく増加することはないので、レベル1（1.2倍）とする。 ■運用管理サブシステム バッチ処理件数はシステム規模に依存する。フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後、システム規模拡大は計画されていないので、レベル1（1.2倍）とする。

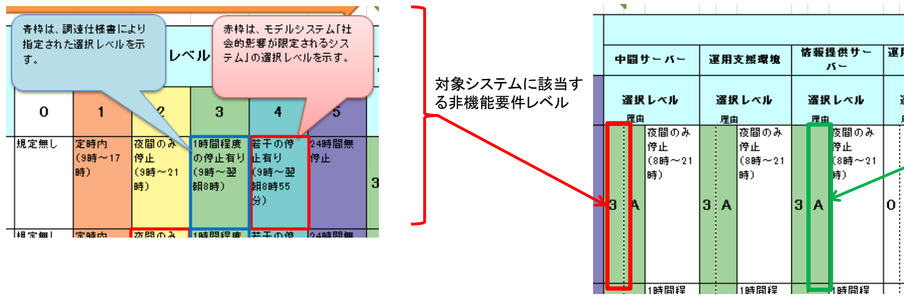
項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル / 理由	オンライン資格確認 中間サーバー連携等サブシステム 選択レベル / 理由	オンライン資格確認 運用管理サブシステム 選択レベル / 理由	オンライン資格確認 資格確認システム接続端末 選択レベル / 理由	オンライン資格確認 資格確認サービス機関等端末 選択レベル / 理由	選択理由
13			保管期間	システムが参照するデータのうち、OSやミドルウェアのログなどのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。		○	保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管	運用設計の結果をもとに定義する					運用設計の結果をもとに定義する
14							対象範囲	オンラインで参照できる範囲	アーカイブまで含める					運用設計の結果をもとに定義する					運用設計の結果をもとに定義する
15		性能目標値	オンラインレスポンス	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ふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に遵守率を決める。具体的な数値は特定の機能またはシステム分類毎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）		○	通常時レスポンス遵守率	遵守率を定めない	60%	80%	90%	95%	99%以上	3 A 90%		3 A 90%		0 B	遵守率を定めない	– – –	– – –	■医療機関等向けサブシステム、中間サーバー連携等サブシステム 2回続けてレスポンスが低下することが1%ならば、ユーザに安定したシステムと感じてもらえると仮定し、レベル3（90%）とする（※1）。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは3であり、選択したレベルは適切であると考える。 ※1：レスポンス低下率＝100% － レスポンス遵守率。レスポンス低下率（10%）のとき、2回続けてレスポンス低下する確率は、0.1×0.1=0.01(1%)となる。この場合のレスポンス遵守率が90%となる。 ■運用管理サブシステム サービスを提供しないサブシステムなので、レベル0（規定無し）とした。
16						○	ピーク時レスポンス遵守率	遵守率を定めない	60%	80%	90%	95%	99%以上	2 A 80%		2 A 80%		0 B	遵守率を定めない	– – –	– – –	■医療機関等向けサブシステム、中間サーバー連携等サブシステム ピーク時でも2回続けてレスポンスが低下することが5%以下ならば、ユーザに安定したシステムと感じてもらえると仮定し、レベル2（80%）とする（※1）。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であり、選択したレベルは適切であると考える。 ※1：レスポンス低下率＝100% － レスポンス遵守率。レスポンス低下率（20%）のとき、2回続けてレスポンス低下する確率は、0.2×0.2=0.04(4%)となる。この場合のレスポンス遵守率が80%となる。 ■運用管理サブシステム サービスを提供しないサブシステムなので、レベル0（規定無し）とした。
17							縮退時レスポンス遵守率	縮退をしない	60%	80%	90%	95%	99%以上	2 C 80%		1 C 60%		0 B	遵守率を定めない	– – –	– – –	■医療機関等向けサブシステム 外部向けオンライン機能でサービスを提供していることから、縮退時もピーク時と同様を要求とする。 ■中間サーバー連携等サブシステム 縮退時なので、ピーク時より低いレベル1（60%）とした。 ■運用管理サブシステム サービスを提供しないサブシステムなので、レベル0（規定無し）とした。
18			バッチレスポンス（ターンアラウンドタイム）	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ふまえ、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、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に遵守率を決める、具体的な数値は特定の機能またはシステム分類毎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）		○	通常時レスポンス遵守度合い	遵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				– –	–	2 A	再実行の余裕が確保できる	2 A	再実行の余裕が確保できる	– – –	– – –	主要なバッチ処理として資格確認用情報や紐付情報の連携等が想定されている。連携等のレスポンスが予定よりも遅れた場合にタイムラグが広がってしまうなどの影響があるので、予定した処理を確実に実行できる環境を整備する必要がある。そのため、余裕のあるレベル2とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であり、選択したレベルは適切であると考える。
19						○	ピーク時レスポンス遵守度合い	遵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				– –	–	2 A	再実行の余裕が確保できる	2 A	再実行の余裕が確保できる	– – –	– – –	主要なバッチ処理として資格確認用情報や紐付情報の連携等が想定されている。連携等のレスポンスが予定よりも遅れた場合にタイムラグが広がってしまうなどの影響があるので、予定した処理を確実に実行できる環境を整備する必要がある。そのため、余裕のあるレベル2とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であり、選択したレベルは適切であると考える。
20							縮退時レスポンス遵守度合い	縮退をしない	所定の時間内に収まる	再実行の余裕が確保できる				– –	–	1 C	所定の時間内に収まる	1 C	所定の時間内に収まる	– – –	– – –	縮退時も業務影響を与えないようにするため、レベル1とする。
21		リソース拡張性	CPU拡張性	CPUの拡張性を確認するための項目。 システム運用開始時のCPU利用率とCPUスロットの空き具合から確認する。 CPU利用率が少ないほど拡張性はあるが、CPUのコストは高く、無駄が生じていることになる。 CPU搭載余裕有無は空きスロットの有無と空きスロット数を確認することで、拡張余力があるかどうかを示す。		○	CPU利用率	80%以上	50%以上80%未満	20%以上50%未満	20%未満			1 A 60%		1 A 60%		1 A	60%	– – –	– – –	一般的なシステムで健全に動作している状態としてCPU利用率80%以下を指標とする場合が多いため、レベル1とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは1であり、選択したレベルは適切であると考える。
22						○	CPU搭載余裕有無	余裕無し	1スロットの空き有り	2スロットの空き有り	3スロットの空き有り	4スロット以上の空き有り		0 C 余裕無し。		1 C 1スロットの空き有り		1 C	1スロットの空き有り	– – –	– – –	■医療機関等向けサブシステム フェーズ1からフェーズ2へのインフラ拡張時に、スケールアウトで対応できるようにする。当該サブシステムでは、CPU拡張を必要とする場合、スケールアウトで対応するため、レベル0（余裕無し）とする。 ■中間サーバー連携等サブシステム、運用管理サブシステム 項番30「スケールアップ」で対象となるサーバーについて、サーバー入れ替えなしで比較的コストの安い処理能力強化策であるCPU追加ができるようにレベル1を選択する。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは1であるたり、選択したレベルは適切であると考える。 ※ただし、中間サーバー連携等サブシステムのWEB/APサーバーについては、医療機関等向けサブシステム同様にスケールアウトで対応する想定をしており、スケールアウトできるサーバーについては、レベル0とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル	理由		オンライン資格確認 中間サーバー連携等サブシステム 選択レベル	理由		オンライン資格確認 運用管理サブシステム 選択レベル	理由		オンライン資格確認 資格確認システム接続端末 選択レベル	理由		オンライン資格確認 資格確認サービス機関等端末 選択レベル	理由		選択理由
23			メモリ拡張性	メモリの拡張性を確認するための項目。 システム運用開始時のメモリ利用率とメモリスロットの空き具合から確認する。 メモリ利用率が少ないほど拡張性はあるが、メモリのコストは高く、無駄が生じていることになる。		○	メモリ利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			1	A	50%以上 80%未満	1	A	50%以上 80%未満	1	A	50%以上 80%未満	–	–	–	–	–	–	一般的なシステムで健全に動作している状態としてメモリ利用率80%以下を指標とする場合が多いため、レベル1とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは1であり、選択したレベルは適切であると考える。
24				メモリ搭載余裕有無は空きスロットの有無と空きスロット数を確認することで、拡張余力があるかどうかを示す。		○	メモリ搭載余裕有無	余裕無し	1スロットの空き有り	2スロットの空き有り	3スロットの空き有り	4スロット以上の空き有り		1	C	1スロットの空き有り	1	C	1スロットの空き有り	1	C	1スロットの空き有り	–	–	–	–	–	–	メモリ増設は、CPU増設よりはコストが低く、処理性能安定化等に寄与する。そのため、メモリ拡張性を保持することとし、レベル1とする。合わせて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは1であり、選択したレベルは適切であると考える。 ※ただし、DBサーバーのように大きなメモリサイズを必要とする場合は、コストを勘案しメモリ搭載余裕有無を判断することとする。
25			ディスク拡張性	ディスクの拡張性を確認するための項目。 システム運用開始時のディスク利用率とディスク増設スロットの空き具合から確認する。 ディスク利用率が少ないほど拡張性はあるが、ディスクのコストは高く、無駄が生じていることになる。 ディスク搭載余裕有無は空きスロットの有無と空きスロット数を確認することで、拡張余力があるかどうかを示す。ディスクは内蔵ディスクが不足しても外部増設が可能であり、CPUやメモリより拡張性は高い。			ディスク（システム領域）利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			0	C	80%	0	C	80%	0	C	80%	–	–	–	–	–	–	システム領域には、主にOS・ミドルウェア・業務アプリケーション・各種ログ等を格納する。OS・ミドルウェア・業務アプリケーションは、単調増加するデータではないのでサイジング可能であるが、各種ログはアクセス等により想定外の増加が発生する可能性がある。 はじめに、"ディスク利用率をα%と定義する"とは、システムライフサイクル終了時のディスク利用率をα%と想定するということである。 次に、ディスク利用率は、CPUやメモリの利用率と異なり、100%に達した時点でシステムダウンやアプリケーションの異常終了が発生する可能性が非常に高い。従って、上述したシステムライフサイクル終了時点の想定利用率は100%ではなく、ある程度余裕を持たせた値に設定する必要がある。 上記の理由より、既存システムのリプレース等、データ量(項番3)とその増大率(項番11)がある程度予測可能なシステムでは、ディスク利用率を非機能要求グレードのレベル0(80%以上)に合わせて、80%とする場合が多い。 システム領域データ使用量は、ある程度の予測が可能なため、ディスクの利用率を80%とする。
26							ディスク（システム領域）増設余裕有無	余裕無し	1スロットの空き有り	2スロットの空き有り	3スロットの空き有り	4スロット以上の空き有り		0	C	余裕無し	0	C	余裕無し	0	C	余裕無し	–	–	–	–	–	–	前項に記載の通り、システム領域データ使用量は、ある程度予測が可能なため。このためスロット単位の拡張性は不要であり、レベル0とする。
27							ディスク（データ領域）利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			1	C	50%以上 80%未満	1	C	50%以上 80%未満	1	C	50%以上 80%未満	–	–	–	–	–	–	要件整理の段階では、データ量予測が可能か判明していない。次項28番と組合せレベル1を適用し、想定外のデータ増加に対応できるようにする。
28							ディスク（データ領域）増設余裕有無	余裕無し	1スロットの空き有り	2スロットの空き有り	3スロットの空き有り	4スロット以上の空き有り		4	C	4スロット以上の空き有り	4	C	4スロット以上の空き有り	4	C	4スロット以上の空き有り	–	–	–	–	–	–	業務データの入出力時に求められる性能や本システムで取り扱うデータの規模を考慮すると、外部ストレージに格納することが望ましい。 外部ストレージの拡張性はスロットで定義されるものではないが、レベル4（4スロット以上）の拡張性があるので、レベル4とする。
29			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目。 既存のネットワーク機器を活用する場合は既存ネットワークの要件を確認するために利用する。 ネットワークの帯域については、項番34で確認する。			ネットワーク拡張性	標準の非機能要求グレードに項目で不足していたため、「医療保険者向け中間サーバー等」の開発で新規項目を定義した						レベル無し	C	余裕有り	レベル無し	C	余裕有り	レベル無し	C	余裕有り	–	–	–	–	–	–	スケールアウトによるサーバー数の増加を考慮し、スタック接続等によりネットワークの拡張が柔軟に実施可能にするため。
30			サーバー処理能力増強	サーバー処理能力増強方法に関する項目。 将来の業務量増大に備える方法（スケールアップ/スケールアウト）をあらかじめ考慮しておくこと。どちらの方法を選択するかはシステムの特徴によって使い分けることが必要。 スケールアップは、より処理能力の大きなサーバーとの入れ替えを行うことで処理能力の増強を行う。 スケールアウトは同等のサーバーを複数台用意し、サーバー台数を増やすことで処理能力の増強を行う。			スケールアップ	スケールアップを行わない	一部のサーバーのみを対象	複数のサーバーを対象				0	C	スケールアップを行わない	1	C	WEB/アプリケーションサーバー(バッチ処理用)を対象とする	2	C	WEB/アプリケーションサーバー(バッチ処理用)を対象とする	–	–	–	–	–	–	■医療機関等向けサブシステム WEB/アプリケーションサーバー(オンライン処理用）は、スケールアウトとすることが一般的であり、レベル0とする。 ■中間サーバー連携等サブシステム どうしてもスケールアウトできないWEB/アプリケーションサーバー（バッチ処理用）は、スケールアップとするため、レベル1とする。 ■運用管理サブシステム 運用管理はパッケージソフトウェア中心のため、サーバー能力向上ではWEB/アプリケーションサーバー（バッチ処理用）を、スケールアップとする。
31							スケールアウト	スケールアウトを行わない	一部のサーバーのみを対象	複数のサーバーを対象				2	C	WEB/アプリケーションサーバー(オンライン処理用)、データベースサーバーを対象とする	2	C	WEB/アプリケーションサーバー(オンライン処理用)、データベースサーバーを対象とする	2	C	WEB/アプリケーションサーバー(オンライン処理用)、データベースサーバーを対象とする	–	–	–	–	–	–	■医療機関等向けサブシステム WEB/アプリケーションサーバー(オンライン処理用）は、スケールアウトとすることが一般的であり、レベル2とする。 ■中間サーバー連携等サブシステム WEB/アプリケーションサーバー(オンライン処理用）は、スケールアウトとすることが一般的であり、レベル2とする。アプリケーションサーバー（バッチ処理用）も可能であればスケールアウトでればスケールアウトで処理能力向上できるようにする。 ■運用管理サブシステム WEB/アプリケーションサーバー(オンライン処理用）は、スケールアウトとすることが一般的であり、レベル2とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル	理由	オンライン資格確認 中間サーバー連携等サブシステム 選択レベル	理由	オンライン資格確認 運用管理サブシステム 選択レベル	理由	オンライン資格確認 資格確認システム接続端末 選択レベル	理由	オンライン資格確認 資格確認サービス機関等端末 選択レベル	理由	選択理由
32		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度。 伝送遅延時間、パケット損失率、帯域幅をなんらかの仕組みで決めているかを示す。回線の帯域が保証されていない場合性能悪化につながることが多い。			帯域保証の設定	無し	プロトコル単位で設定	各サーバー毎に設定	アプリケーションのエンドツーエンドで検証・保証			0 C 無し		0 C 無し		0 C 無し		– – –		– – –		帯域保証回線を導入するため（※）、ネットワークのサービス品質を保証する機能は導入しない。レベル0とする。 ※フェーズ1で流用する、レセプトオンライン請求用ネットワークでの医療機関等から接続拠点（東日本、西日本）は対象外とする。フェーズ2では医療機関等とのNWは未定のため本項目を前提とするが、フェーズ2NW検討結果によっては変更する可能性がある。
33			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲。			測定頻度	測定しない	構築当初に測定	運用中、必要時に測定可能	運用中、定常的に測定			2 C 構築当初の他、フェーズ1（パイロット運用）での性能測定、及び、フェーズ2（本格運用）でのシステム改修時に維持保守環境（フェーズ1環境）での性能測定		2 C 構築当初の他、フェーズ1（パイロット運用）での性能測定、及び、フェーズ2（本格運用）でのシステム改修時に維持保守環境（フェーズ1環境）での性能測定		2 C 構築当初の他、フェーズ1（パイロット運用）での性能測定、及び、フェーズ2（本格運用）でのシステム改修時に維持保守環境（フェーズ1環境）での性能測定		– – –		– – –		構築当初の他、下記性能計測を実施 ・フェーズ1（パイロット運用）での性能計測を実施しフェーズ2（本格運用）環境向けのサイジングを行う ・フェーズ2（本格運用）でのシステム改修時に、保守環境（フェーズ1環境）で性能計測を行う。
34							確認範囲	確認しない	一部の機能について、目標値を満たしていることを確認	全ての機能について、目標値を満たしていることを確認				1 C 業務シナリオを定義する		1 C 業務シナリオを定義する		1 C 業務シナリオを定義する		– – –		– – –		ピーク時及び通常時を想定した業務シナリオを定義のうえで性能テストを実施するため、レベル1とする。
35			リソース利用率の制限	性能目標値の確保にあたり、リソース利用率の制限を行うかを検討する。この項目はサイジングのINPUTとしても利用する。			CPU利用率	標準の非機能要求グレードに項目で不足していたため、「医療保険者向け中間サーバー等」の開発で新規項目を定義した						レベル無し C	60%	レベル無し C	60%	レベル無し C	60%					サーバーが高負荷状態で稼動すると待ち行列が発生する。システムの特性にもよるがCPU利用率が70～80%を超過する付近で顕在化し、負荷が高くなるほどにレスポンスは低下していく傾向にある。このためレスポンス遵守率を達成するためには、待ち行列を考慮してレスポンスを予測するべきだが、システムは複数のコンポーネントにより複雑に構成されているため予測の手法が確立されておらず非常に困難である。よってCPU利用率については一定の制限を設ける。 なお、ここでいうCPU利用率とは、瞬間的な利用率ではなく特定時間帯あたりの利用率の平均値を指す。本プロジェクトにおいては基盤先行によりサイジングの見積精度が低くなるリスクを考慮して決定するべきである。以上より、CPU利用率の上限を「60%」と定義する。
36							メモリ利用率	標準の非機能要求グレードに項目で不足していたため、「医療保険者向け中間サーバー等」の開発で新規項目を定義した						レベル無し C	80%	レベル無し C	80%	レベル無し C	80%					メモリ利用率については、容量が不足しスワッピングが発生した際の性能劣化が著しいため、想定外の状況を考慮した設定値に制限する。なお、ここでいうメモリ利用率とは、瞬間的な利用率ではなく特定時間帯あたりの利用率の平均値を指す。基盤基本設計の結果、メモリの利用率が意図せず上昇してしまうリスクが少ないと考えられるため利用率を80%とする。 （Active-Active構成で冗長化を実現するサーバーは縮退時に新たなインスタンスなどが立ち上がる事はない、事前に割り当てられたメモリの範囲内でのみ処理が行われる方式を採用、など）
37			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。 特にB2Cシステムなどクライアント数を制限できないシステムで発生する。システムの処理上限を超えることが多いため、Sorry動作を実装し対策する場合が多い。			トランザクション保護	トランザクション保護は不要である	同時トランザクション数の制限機能	同時トランザクション数の制限機能に加え、Sorry動作	独立したSorry動作を行うサーバーの設置			2 C 同時トランザクション数の制限機能に加え、Sorry動作		0 C トランザクション保護は不要である		0 C トランザクション保護は不要である		– – –		– – –		■医療機関等向けサブシステム 医療機関等窓口の混雑時の 耐久性維持が重要なため、レベル2とする。 ■中間サーバー連携等サブシステム、運用管理サブシステム 資格確認サービス機関と運用保守事業者の担当者がユーザーで限られた人数であり、また業務量も多くないことから、レベル0とする。

（1）選択レベルの表記例

以下に本資料の表記例を示します。



対象システムに該当する非機能要件レベル

【IPA非機能要求グレード選択レベルの選択理由】
下記、Aから順に優先順位となる。

A. モデルシステム「社会的影響が限定されるシステム」から判断
B. 監視等のオンライン業務に直接影響が無いことから判断
C. 個別に検討し、判断
D. 中間サーバーの運用に順ずることから判断

（2）非機能要件及び選択レベル

非機能要求グレード活用シート(原本の範囲)　／　要件定義工程における検討結果

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル 理由	医療機関等向けサブシステム 24時間無停止	中間サーバー連携等サブシステム 選択レベル 理由	中間サーバー連携等サブシステム 24時間無停止	運用管理サブシステム 選択レベル 理由	運用管理サブシステム 24時間無停止	資格確認システム接続端末 選択レベル 理由	資格確認システム接続端末 規定無し	資格確認サービス機関等端末 選択レベル 理由	資格確認サービス機関等端末 規定無し	選択理由
1	運用・保守性	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。	○	○	運用時間（通常）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	5 C	24時間無停止	5 C	24時間無停止	5 C	24時間無停止	0 C	規定無し	0 C	規定無し	サービスを提供する時間帯を含め、システムを構成するサーバー等が電源ONで稼動している時間帯と解釈し、以下の整理とする。 ■医療機関等向けサブシステム、中間サーバー連携等サブシステム、運用管理サブシステム サービス時間帯以外でも電源は落とさず、常時電源ONで運用する。 ■資格確認システム接続端末、資格確認サービス機関等端末 担当者が業務を行うときに起動していれば良いので、レベル0とする。
2					○	○	運用時間（特定日）	規定無し	定時内（9時～17時）	夜間のみ停止（9時～21時）	1時間程度の停止有り（9時～翌朝8時）	若干の停止有り（9時～翌朝8時55分）	24時間無停止	0 C	規定無し	0 C	規定無し	0 C	規定無し	0 C	規定無し	0 C	規定無し	全業務で特定日無し
3			バックアップ	システムが利用するデータのバックアップに関する項目。	○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧				2 C	システム内の全データを復旧	2 C	システム内の全データを復旧	2 C	システム内の全データを復旧	–	–	–	–	IPA非機能要求グレードでレベル1は、業務継続性の要求を満たすために必要なデータを復旧すると記載があり、業務再開に必要なデータと解釈できる。業務再開に必要なデータ以外にも監査、法令及び規則等への対応に必要な証跡となるログ等も復旧する必要があることを考慮し、レベル2とする。ただし、復旧時間の短縮のため、業務再開に必要なデータ以外を非同期での復旧または対象外とすることを検討する。なお、業務再開に必要なデータおよびシステム復旧方法については基本設計工程での留意点とする。
4						○	バックアップ利用範囲	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	ユーザエラーからの回復	データの長期保存（アーカイブ）			1 C	障害発生時のデータ損失防止	1 C	障害発生時のデータ損失防止	1 C	障害発生時のデータ損失防止	–	–	–	–	原則として、バックアップの利用範囲は決めたられたRPO(目標復旧地点)「1営業日前の時点」へのデータ回復が可能なレベル1を選択する。ただし、規則・法令等の規定により証跡として保存する必要のあるログ等についてはレベル3を選択する。保存対象のアーカイブデータについては基本設計工程での留意点とする。
5						○	外部データ利用可否	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				2 C	外部データは利用できない	2 C	外部データは利用できない	2 C	外部データは利用できない	–	–	–	–	復旧において外部データを利用する際、データの取得先環境の影響をうける場合がありRTO(目標復旧時間)内での復旧が難しくなる。そのため、外部データを使用しないレベル2とする。
6					○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			1 C	オフラインバックアップ	1 C	オフラインバックアップ	1 C	オフラインバックアップ	–	–	–	–	業務データを安定かつ整合性を保った状態でバックアップ取得するためにミドルウェア(データベース製品等)の停止を推奨する。このため、バックアップ取得のための停止時間を2時間程度と想定し、原則としてレベル1を選択する。ただし、業務を含めた運用スケジュールが精査される中で停止時間が確保できない場合、基本設計工程にてレベル2またはレベル3での対応をバックアップ対象毎に検討する。
–							バックアップ保管先	「医療保険者向け中間サーバー等」の開発において、標準の非機能要求グレードに項目が存在していないため、新規項目を定義した						– C	ストレージ	– C	ストレージ	– C	ストレージ	–	–	–	–	バックアップ処理がサービス提供時間に与える影響を低減するため、外部媒体と比較し入出力速度が高速なストレージをバックアップ保管先とする。
7						○	バックアップ取得間隔	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	4 C	日次で取得	4 C	日次で取得	4 C	日次で取得	–	–	–	–	可用性要件：目標復旧水準（業務停止時）のRPO(目標復旧地点)「1営業日前の時点」を満たすためにレベル4とする。
8						○	バックアップ保存期間	バックアップを保存しない	1年未満	3年	5年	10年以上有限	永久保存	1 C	1年未満	1 C	1年未満	1 C	1年未満	–	–	–	–	原則として障害発生時のデータ損失防止のためのバックアップ保存期間はRPO(目標復旧地点)「1営業日前の時点」を満たすレベル1とする。ただし、監査・法令及び規約等への対応に長期間の保存が必要なデータについてはセキュリティ要件に準じた保存期間を定める。メンテナンス等にて不定期に更新されるデータ(システム系データ等)については、次回システム変更作業までは最新のバックアップを保管する等を基本設計工程で定めることとする。
9						○	バックアップ自動化の範囲	全ステップを手動で行う	数ステップを手動で行う（テープ交換とバックアップ開始コマンドの入	1ステップのみ手動で行う（テープ交換のみ）	全ステップを自動で行う			3 C	全ステップを自動で行う	3 C	全ステップを自動で行う	3 C	全ステップを自動で行う	–	–	–	–	原則として運用者の作業工数が削減できるレベル3とする。ただし、システム構成変更作業前後のバックアップ等、任意のタイミングで手動で実行が想定されるバックアップも存在するため、自動化の範囲については基本設計工程での留意点とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 運用管理ｻﾌﾞｼｽﾃﾑ 選択レベル	理由	オンライン資格確認 資格確認ｼｽﾃﾑ接続端末 選択レベル	理由	オンライン資格確認 資格確認ｻｰﾋﾞｽ機関等端末 選択レベル	理由	選択理由
10			運用監視	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。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。		○	監視情報	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	4 C リソース監視を行う		4 C リソース監視を行う		4 C リソース監視を行う		– – –		– – –		CPU利用率やメモリ利用率、ﾃﾞｨｽｸ利用率等の基本的なリソース監視は、健全なシステム運用には必要なため、レベル4とする。
11						○	監視間隔	監視を行わない	不定期監視（手動監視）	定期監視（1日間隔）	定期監視（数時間間隔）	リアルタイム監視（分間隔）	リアルタイム監視（秒間隔）	4 C リアルタイム監視（分間隔）		4 C リアルタイム監視（分間隔）		4 C リアルタイム監視（分間隔）		– – –		– – –		医療機関等向けのオンライン業務は、随時要求を受付実行される。この業務に対し、数時間間隔の監視では障害等の検知が遅くなるため、レベル4とする。加えて、IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定されている。この場合、本項目の推奨レベルは4であるため、選択が適切であると判断する。
12							システムレベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		IPA非機能要求グレードにて、システムレベル監視はバックアップの監視及びジョブの監視等が該当すると定義されている。バックアップ及びジョブはどちらも監視する必要があるため、レベル2を採用する。
13							プロセスレベルの監視	監視を行わない	一部監視を行う	全て監視を行う				1 C 一部監視を行う		1 C 一部監視を行う		1 C 一部監視を行う		– – –		– – –		サービス提供に影響があるプロセスを選定して監視は、健全なシステム運用に必要なため、レベル1とする。対象とするプロセスは基本設計工程の留意点とする。
14							データベースレベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		すべてのデータベースを監視するため、レベル2とする。なお、ミドルウェア組込のデータベースは対象外とする。
15							ストレージレベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		すべてのストレージを監視するため、レベル2とする。
16							サーバー（ノード）レベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		すべてのサーバー（ノード）を監視するため、レベル2とする。
17							端末レベルの監視	監視を行わない	一部監視を行う	全て監視を行う				– – –		– – –		– – –		その他 C 各医療機関等の端末要件による		0 C 監視を行わない		■資格確認ｼｽﾃﾑ接続端末 端末は各機関の管理下にあるため、各医療機関の端末要件に従う。 ■資格確認ｻｰﾋﾞｽ機関等端末 端末は使用前後に電源ON/OFFするため、監視を行わない。
							ネットワーク機器レベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		ネットワーク機器は全て監視対象とし死活監視やログ監視を行うため、レベル2とする。
18							ネットワーク・パケットレベルの監視	監視を行わない	一部監視を行う	全て監視を行う				2 C 全て監視を行う		2 C 全て監視を行う		2 C 全て監視を行う		– – –		– – –		ネットワーク・パケットレベルの監視では、ネットワーク帯域の使用率の監視を行う。すべてのネットワーク機器を対象とするため、レベル2とする。
19			時刻同期	システムを構成する機器の時刻同期に関する項目。			時刻同期設定の範囲	時刻同期を行わない	サーバー機器のみ時刻同期を行う	サーバーおよびクライアント機器について時刻同期を行う	ネットワーク機器も含めシステム全体で時刻同期を行う	システム全体を外部の標準時間と同期する		4 C システム全体を外部の標準時間と同期する		4 C システム全体を外部の標準時間と同期する		4 C システム全体を外部の標準時間と同期する		4 C システム全体を外部の標準時間と同期する		4 C システム全体を外部の標準時間と同期する		本システムは外部システムとの接続が存在するため、厚生労働省殿または取りまとめ機関のネットワーク内に存在する時刻同期サーバーとの接続が望ましい。よって、外部の標準時間との整合性を担保するレベル4を採用する。 医療機関等に設置されるオンライン資格確認接続端末も、時刻同期については、サーバーと同様に時刻同期を行う必要があるのでレベル4を採用する。
20		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスタデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目。	○	○	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				【C-1-1】可用性要件　継続性（計画停止の有無）で定義済み										※【C-1-1】可用性要件　項番3（継続性（計画停止の有無））で定義済み。
21							計画停止の事前アナウンス	計画停止が存在しない	計画停止は年間計画によって確定する	1ヶ月前に通知	1週間前に通知	前日に通知		1 C 計画停止は年間計画によって確定する		1 C 計画停止は年間計画によって確定する		1 C 計画停止は年間計画によって確定する		– – –		– – –		フェーズ2が想定している医療機関等全般へのオンライン資格確認普及後は、医療機関等にとって重要なサービスとなることから、月単位のスケジュールで本システムなしの業務運用変更はインパクトが大きい。もし計画停止（運用スケジュールを変更しない）を行うならば年間計画で通知することが望ましいことから、レベル1とする。 ※参考 ・フェーズ1で医療機関等と接続するレセプトオンライン請求用NWは、年末年始(12/29～1/3)は停止する。 ・レセプトオンライン請求NWでは、あらゆる理由のシステム停止を予告なく行う旨を利用規約に記載している（第5条1項）。ただし、停止している場合の運用も利用規約に規程している（同第2、3項）。
22			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。		○	保守作業自動化の範囲	保守作業は全て手動で実施する	一部の保守作業を自動で実行する	全ての保守作業を自動で実行する				1 C 一部の保守作業を自動で実行する		1 C 一部の保守作業を自動で実行する		1 C 一部の保守作業を自動で実行する		– – –		– – –		何らかの判断を必要とする作業（稼動状況や監視情報の分析等）はリスクがあるため、自動化しない。一方、判断が不要な作業はリスクが低いため自動化対象とする。よって、レベル1とする。なお、本資料における自動化とはすべての作業を全自動で行うことではないと定義する。よって自動化した場合であっても一部手動で実施する作業は存在することとなる。
23							サーバーソフトウェア更新作業の自動化	サーバーへの更新ファイル配布機能を実装しない	サーバーへの更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	サーバーへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	サーバーへの更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			2 C サーバーへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する		2 C サーバーへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する		2 C サーバーへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する		– – –		– – –		OS、ミドルウェア、業務アプリケーションの更新作業は、サーバーの設置数が多く、手動実行では保守作業が長時間に及ぶ可能性がある。そのため自動化が可能な処理は自動化してシステム停止時間の短縮を図る。よって、レベル2とする。ただし、ミドルウェアの製品仕様上、自動化が困難な場合は対象外とする。
							ストレージ等のファームウェア更新作業の自動化	非機能要求グレードでは「サーバーソフトウェア更新作業の自動化」に含めて定義されているが、分割して記載する						– C 自動化しない		– C 自動化しない		– C 自動化しない		– – –		– – –		自動化が困難と想定されるためストレージ等のファームウェアは自動化の対象外とする。
24							端末ソフトウェア更新作業の自動化	端末への更新ファイル配布機能を実装しない	端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	端末への更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			– – –		– – –		– – –		1 C 端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する		1 C 端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する		端末にオンライン資格確認用クライアントアプリケーションを配置する場合の選択レベル。もし、ブラウザのみで必要な機能が動作し、クライアントアプリケーションの配布がない場合は、本項目は対象外とする。
							ネットワーク機器のファームウェア更新作業の自動	非機能要求グレードでは「端末ソフトウェア更新作業の自動化」に含めて定義されているが、分割して記載する						– C 自動化しない		– C 自動化しない		– C 自動化しない		– – –		– – –		自動化が困難と想定されるためネットワーク機器のファームウェアは自動化の対象外とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認												選択理由
														医療機関等向けサブシステム			中間サーバー連携等サブシステム			運用管理サブシステム			資格確認システム接続端末			資格確認サービス機関等端末			
								0	1	2	3	4	5	選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		
25			パッチ適用ポリシー	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。			パッチリリース情報の提供	ユーザの要求に応じてベンダが受動的にパッチリリース情報を提供する	ベンダが定期的にユーザへパッチリリース情報を提供する	ベンダがリアルタイムに（パッチリリースと同時に）ユーザへパッチリリース情報を提供する				1	C	ベンダが定期的にユーザへパッチリリース情報を提供する	1	C	ベンダが定期的にユーザへパッチリリース情報を提供する	1	C	ベンダが定期的にユーザへパッチリリース情報を提供する	－	－	－	1	C	ベンダが定期的にユーザへパッチリリース情報を提供する	全てのパッチに対してリアルタイムにリリース情報を提供する場合はコストが膨大となることから、定期的なリリース情報の提供を行うレベル1とする。ただし、システム脆弱性に直結する等の緊急度の高いパッチがリリースされた際は、ハードウェア保守ベンダーから速やかに情報提供を受け、運用保守ベンダーから資格確認サービス機関に対し適用判断を仰ぐこととする。
26							パッチ適用方針	パッチを適用しない	推奨されるパッチのみを適用する	全てのパッチを適用する				1	C	推奨されるパッチのみを適用する	1	C	推奨されるパッチのみを適用する	1	C	推奨されるパッチのみを適用する	－	－	－	1	C	推奨されるパッチのみを適用する	障害パッチは推奨されるパッチのみを適用し、システムの構成上 対象外と判断できるパッチについては適用の対象外とするためレベル1とする。なお、セキュリティパッチの適用方針は「5. セキュリティ要件」項番132（セキュリティリスク管理（セキュリティパッチ適用方針））で定義済みのため、本項目では対象外とする。
27							パッチ適用タイミング	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	新規のパッチがリリースされるたびに適用を行う			2	C	定期保守時にパッチ適用を行う	2	C	定期保守時にパッチ適用を行う	2	C	定期保守時にパッチ適用を行う	－	－	－	2	C	定期保守時にパッチ適用を行う	予防保守として障害パッチの適用を定期的に行うことが望ましいため、定期保守時にパッチ適用を行うレベル2とする。ただし、緊急度の高いパッチがリリースされた際には速やかに適用可否を検討して対応する。なお、セキュリティパッチの適用タイミングは「5. セキュリティ要件」項番10（セキュリティリスク管理（セキュリティパッチ適用タイミング））で定義済みのため、本項目では対象外とする。
28							パッチ検証の実施有無	パッチ検証を実施しない	障害パッチのみパッチ検証を実施する	障害パッチとセキュリティパッチの両方でパッチ検証を実施する				2	C	障害パッチとセキュリティパッチの両方でパッチ検証を実施する	2	C	障害パッチとセキュリティパッチの両方でパッチ検証を実施する	2	C	障害パッチとセキュリティパッチの両方でパッチ検証を実施する	－	－	－	2	C	障害パッチとセキュリティパッチの両方でパッチ検証を実施する	障害パッチ・セキュリティパッチに関わらずテスト環境にて事前検証を行う必要がある。事前検証したうえで本番環境へのパッチ適用を行うため、レベル2とする。
29			活性保守	サービス停止の必要がない活性保守が可能なコンポーネントの範囲。			ハードウェア活性保守の範囲	活性保守を行わない	一部のハードウェアにおいて活性保守を行う	全てのハードウェアにおいて活性保守を行う				1	C	一部のハードウェアにおいて活性保守を行う	1	C	一部のハードウェアにおいて活性保守を行う	1	C	一部のハードウェアにおいて活性保守を行う	－	－	－	－	－	－	活性保守はシステム停止を伴わないため、業務への影響を最小限に抑えることができる。しかし、保守作業中に想定外の事象が発生した場合、稼動中のシステムに影響を与え、システム障害に繋がるリスクがある。そのため、活性保守を行った実績があり、かつリスクが少ない機器に対してのみ活性保守を行う。よって、レベル1とする。なお、具体的な対象機器については、基本設計で定義する。また保守作業に影響を及ぼさないよう、各システム間の接続用ネットワークスイッチは管理系及び業務系で機器を分別する。分別方針は業務影響度を鑑み、基本設計での留意点とする。
30							ソフトウェア活性保守の範囲	活性保守を行わない	一部のソフトウェアにおいて活性保守を行う	全てのソフトウェアにおいて活性保守を行う				－	C	運用スケジュールや計画停止の有無をインプットとし基本設計で定義する	－	C	運用スケジュールや計画停止の有無をインプットとし基本設計で定義する	－	C	運用スケジュールや計画停止の有無をインプットとし基本設計で定義する	－	－	－	－	－	－	運用スケジュール・計画停止の有無・ハードウェア仕様に影響されるため、OS・ミドルウェア・アプリケーションのパッチ適用時の活性保守有無は基盤基本設計での留意点とする。
31			定期保守頻度	システムの保全のために必要なハードウェアまたはソフトウェアの定期保守作業の頻度。			定期保守頻度	定期保守を実施しない	年1回	半年に1回	月1回	週1回	毎日	業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する														ソフトウェアの定期保守作業の一部であるパッチ適用は、各製品のパッチリリーススケジュールに合わせて実施スケジュールを制定することが望ましい。 基本アプリケーション設計で利用が決定した各製品のパッチリリーススケジュールを踏まえて、基盤基本設計で定義する。
32			予防保守レベル	システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守。			予防保守レベル	予防保守を実施しない	定期保守時に検出した予兆の範囲で対応する	（定期保守とは別に）一定間隔で予兆検出を行い、対応を行う	リアルタイムに予兆検出を行い、対応を行う			1	C	定期保守時に検出した予兆の範囲で対応する	1	C	定期保守時に検出した予兆の範囲で対応する	1	C	定期保守時に検出した予兆の範囲で対応する	－	－	－	1	C	定期保守時に検出した予兆の範囲で対応する	本システムにおいては、システムを安定稼動させるため、障害発生の予兆検出を行う必要がある。ハードウェア保守ベンダーによる定期保守作業時に予兆検出を行うため、レベル1とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	オンライン資格確認 医療機関等向けサブシステム 選択レベル	理由	オンライン資格確認 中間サーバー連携等サブシステム 選択レベル	理由	オンライン資格確認 運用管理サブシステム 選択レベル	理由	オンライン資格確認 資格確認システム接続端末 選択レベル	理由	オンライン資格確認 資格確認サービス機関等端末 選択レベル	理由	選択理由
33		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧			2 C	復旧用製品による復旧	2 C	復旧用製品による復旧	2 C	復旧用製品による復旧	- -	-	- -	-	目標復旧時間が12時間以内と定めているため、復旧時間の短縮が必要となる。バックアップソフトなどの復旧用製品を利用する復旧作業を想定し、レベル2とする。
34					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要				1 C	一部の業務について代替業務運用が必要	0 C	無し	0 C	無し	- -	-	- -	-	■医療機関等向けサブシステム 医療機関等での業務に代替運用を必要とする業務が一部有り、レベル1とする。 ■中間ｻｰﾊﾞｰ連携等サブシステム 資格情報同期等、システム抜きの代替業務運用が考えられないため、レベル0とする。 ■運用管理サブシステム 何らかのシステム無しの代替業務運用が考えられないため、レベル0とする。
35			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目。			障害復旧自動化の範囲	障害復旧作業は全て手動で実施する	一部の障害復旧作業を自動化する	全ての障害復旧作業を自動化する				1 C	一部の障害復旧作業を自動化する	1 C	一部の障害復旧作業を自動化する	1 C	一部の障害復旧作業を自動化する	- -	-	- -	-	障害復旧に関するオペレーションが発生する例としてバックアップデータからのリカバリ等が挙げられる。ミドルウェアの導入等によりリカバリ作業の一部自動化を想定しているため、レベル1とする。
36			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目。			対応可能時間	ベンダの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う				業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。									
37							駆けつけ到着時間	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。									
38							SE到着平均時間	SEの駆けつけ無し	SE到着が異常検知から数日中	SE到着が異常検知からユーザの翌営業日中	SE到着が異常検知からユーザの翌営業開始時まで	SE到着が異常検知から数時間内	SEが常駐	業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。									
39			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法。			保守部品確保レベル	確保しない	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保する				1 C	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	1 C	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	1 C	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	- -	-	- -	-	障害発生や予防保守等で部品交換が必要となった場合に速やかに交換対応を行うため、保守対象のハードウェアは保守部品を確保する必要がある。また、本システムを構成する機器の保守契約はライフサイクルとして定めた期間を保証する必要がある。よって、レベル1とする。
40							予備機の有無	予備機無し	一部、予備機有り	全部、予備機有り				1 C	一部、予備機有り	1 C	一部、予備機有り	1 C	一部、予備機有り	- -	-	- -	-	※【C-1-1】可用性要件　項番13、15、17、22（耐障害性（サーバー、端末、ネットワーク機器、ストレージ））で定義済み。
41		運用環境	開発・テスト環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。		○	開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する				2 C	運用環境と同一の開発環境を設置する（保守環境を想定）	2 C	運用環境と同一の開発環境を設置する（保守環境を想定）	2 C	運用環境と同一の開発環境を設置する（保守環境を想定）	- -	-	- -	-	フェーズ2はフェーズ1運用時のサイジング計測結果を反映し、フェーズ1運用環境とは別に新規に構築した環境で運用する方針である。その場合、フェーズ1とフェーズ2について、運用開始前はそれぞれの運用環境を開発環境とする。フェーズ2運用開始後は、フェーズ1運用環境を開発環境（保守環境）として利用することを想定している。 そのため、レベル2とする。 なお、保守環境はSWとHWの構成は同じである（冗長構成等も含む）が、規模は動作確認に必要な分のみ配備する環境を想定している。
42				ユーザがシステムの動作を試験する目的で導入する環境についての項目。		○	テスト環境の設置有無	システムの試験環境を設置しない	システムの開発用環境と併用する	専用の試験用環境を設置する				2 C	専用の試験用環境を設置する	2 C	専用の試験用環境を設置する	2 C	専用の試験用環境を設置する	- -	-	- -	-	医療機関等からの接続確認等で用いる検証環境を導入することを検討する。そのため、レベル2とする。
43			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。		○	マニュアル準備レベル	各製品標準のマニュアルを利用する	システムの通常運用のマニュアルを提供する	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			2 B	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	2 B	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	2 B	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	- -	-	- -	-	IPA非機能要求グレードで定義されるモデルシステムより、本システムは「社会的影響が限定されるシステム」と想定される。この場合、本項目の推奨レベルは2であるため、レベル2とする。
44			リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。		○	リモート監視地点	リモート監視を行わない	構内LANを介してリモート監視を行う	遠隔地でリモート監視を行う				2 C	遠隔地でリモート監視を行う	2 C	遠隔地でリモート監視を行う	2 C	遠隔地でリモート監視を行う	- -	-	- -	-	資格確認サービス機関等でのリモート監視を想定している。そのため、レベル2とする。
45						○	リモート操作の範囲	リモート操作を行わない	定型処理のみリモート操作を行う	任意のリモート操作を行う				1 C		1 C		1 C		- -	-	- -	-	事前に資格確認サービス機関で了承された操作のみをリモート操作で行うことを想定しているため、レベル1とする。
46			外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。		○	外部システムとの接続有無	外部システムと接続しない	社内の外部システムと接続する	社外の外部システムと接続する				2 C	社外の外部システムと接続する	2 C	社外の外部システムと接続する	0 C	外部システムと接続しない	- -	-	- -	-	■医療機関等向けサブシステム 医療機関等、医療機関等認証局、医療等ID発行・管理機関 ■中間ｻｰﾊﾞｰ連携等サブシステム 医療保険者等向け中間サーバー等、収納管理システム ■運用管理サブシステム 外部システムとの接続無しを想定している。
47							監視システムの有無	監視システムは存在しない	既存監視システムに接続する	新規監視システムに接続する				2 C	新規監視システムに接続する	2 C	新規監視システムに接続する	2 C	新規監視システムに接続する	- -	-	- -	-	新規に監視システムを設置し、システム内の機器を管理対象とするので、レベル2とする。
48							ジョブ管理システムの有無	ジョブ管理システムは存在しない	既存ジョブ管理システムに接続する	新規ジョブ管理システムに接続する				2 C	新規監視システムに接続する	2 C	新規監視システムに接続する	2 C	新規監視システムに接続する	- -	-	- -	-	新規にジョブ管理システムを設置し、システム内の機器を管理対象とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認												選択理由
														医療機関等向けｻﾌﾞｼｽﾃﾑ			中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ			運用管理ｻﾌﾞｼｽﾃﾑ			資格確認ｼｽﾃﾑ接続端末			資格確認ｻｰﾋﾞｽ機関等端末			
								0	1	2	3	4	5	選択レベル		理由	選択レベル		理由	選択レベル		理由	選択レベル		理由	選択レベル		理由	
49		保守要件	保守契約（ハードウェア）	保守が必要な対象ハードウェアの範囲。		○	保守契約（ハードウェア）の範囲	保守契約を行わない	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）			業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
50			保守契約（ソフトウェア）	保守が必要な対象ソフトウェアの範囲。		○	保守契約（ソフトウェア）の範囲	保守契約を行わない	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う	マルチベンダのサポート契約を行う（一部対象外を許容）	マルチベンダのサポート契約を行う（システムを構成する全製品を対象）			業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
51			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。		○	ライフサイクル期間	3年	5年	7年	10年以上			業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
52			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目。			メンテナンス作業役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施				1	C	一部ユーザが実施	1	C	一部ユーザが実施	1	C	一部ユーザが実施	1	C	一部ユーザが実施	–	–	–	–	–	–	資格サービス確認機関と運用保守ベンダの共同作業を想定しているため、レベル1とする。
53			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。			一次対応役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施				1	C	一部ユーザが実施	1	C	一部ユーザが実施	1	C	一部ユーザが実施	1	C	一部ユーザが実施	–	–	–	–	–	–	資格サービス確認機関と運用保守ベンダの共同作業を想定しているため、レベル1とする。
54			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目。			ベンダー側常備配備人数（ハードウェア保守ベンダー）	常駐しない	1人	複数人				業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
							ベンダー側常備配備人数（運用保守ベンダー）	常駐しない	1人	複数人				業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
55							ベンダー側対応時間帯（ハードウェア保守ベンダー）	対応無し	ベンダの定時時間内（9～17時）	夜間のみ非対応（9～21時）	引継ぎ時に1時間程度非対応有り（9～翌8時）	24時間対応		業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
							ベンダー側対応時間帯（運用保守ベンダー）	対応無し	ベンダの定時時間内（9～17時）	夜間のみ非対応（9～21時）	引継ぎ時に1時間程度非対応有り（9～翌8時）	24時間対応		業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
56							ベンダー側対応者の要求スキルレベル（ハードウェア保守ベンダー）	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている		3	C	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	3	C	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	3	C	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	–	–	–	–	–	–	基盤に関する保守作業を実施するハードウェア保守ベンダー要員を想定しており、予防保守作業等を実施する必要があるため、レベル3とする。
							ベンダー側対応者の要求スキルレベル（運用保守ベンダー）	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている		3	C	手順書に則り、システム運用処理及び業務運用処理を実施できる	3	C	手順書に則り、システム運用処理及び業務運用処理を実施できる	3	C	手順書に則り、システム運用処理及び業務運用処理を実施できる	–	–	–	–	–	–	手順書に則り保守作業を実施する運用保守ベンダー要員を想定しており、システム運用処理及び業務運用処理を実施する必要があるため、レベル3とする。
57							エスカレーション対応（ハードウェア保守ベンダー）	指定無し	オンコール待機	拠点待機	現地待機			業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														
							エスカレーション対応（運用保守ベンダー）	指定無し	オンコール待機	拠点待機	現地待機			業務アプリケーションの基本設計をインプットとして、基盤基本設計で定義する。														

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認												選択理由
														医療機関等向けサブシステム			中間サーバー連携等サブシステム			運用管理サブシステム			資格確認システム接続端末			資格確認サービス機関等端末			
								0	1	2	3	4	5	選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		選択レベル	理由		
58			導入サポート	システム導入時の特別対応期間の有無および期間。			システムテスト稼動時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上		4	C	※具体的な期間は、開発スケジュール決定後	4	C	※具体的な期間は、開発スケジュール決定後	4	C	※具体的な期間は、開発スケジュール決定後	－	－	－	－	－	－	テスト稼動時に発生した問題の早期解決を図るため、テスト期間中ハードウェア構築ベンダーは導入サポートを提供する必要があるため、レベル4（1ヶ月以上）となる。※具体的な期間は、開発スケジュール決定後に定義する。
59							システム本稼動時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上		4	C	※具体的な期間は、開発スケジュール決定後	4	C	※具体的な期間は、開発スケジュール決定後	4	C	※具体的な期間は、開発スケジュール決定後	－	－	－	－	－	－	本稼動時に発生した問題の早期解決を図るため、本稼動開始後にハードウェア構築ベンダーは導入サポートを提供する必要があるため、レベル4（1ヶ月以上）となる。※具体的な期間は、開発スケジュール決定後に定義する。
60			オペレーション訓練	オペレーション訓練実施に関する項目。			オペレーション訓練実施の役割分担	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施			3	C	全てベンダが実施	3	C	全てベンダが実施	3	C	全てベンダが実施	－	－	－	－	－	－	本システムは、接続する他システムが複数あることもあり、オペレーションを行うにあたって前提となる知識を必要としている。そのため、ベンダーからのオペレーション訓練時に必要な知識も得ることが重要である。そのため、レベル3とする。
61							オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施			2	C	通常運用に加えて保守運用の訓練を実施	2	C	通常運用に加えて保守運用の訓練を実施	2	C	通常運用に加えて保守運用の訓練を実施	－	－	－	－	－	－	運用を円滑に開始するためオペレーション訓練としては、通常運用作業及び保守運用作業においてオペレーション訓練を行うことが望ましいため、レベル2とする。ただし、復旧作業に関する訓練も一部可能な範囲で事前に整備した復旧手順を使用して実施する。
62							オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催				2	C	定期開催	2	C	定期開催	2	C	定期開催	－	－	－	－	－	－	システムの運用中には、システム変更作業により運用作業内容に変更が発生する可能性がある。そのため、本番稼動後は熟練度の向上を目的として運用保守担当者により、定期的に実施することが望ましい。なお、運用作業内容の変更による影響が大きい場合等、必要に応じて追加開催も検討する。よって、以上の2点からレベル2とする。
63			定期報告会	保守に関する定期報告会の開催の要否。			定期報告会実施頻度	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	4	C	月1回	4	C	月1回	4	C	月1回	－	－	－	－	－	－	本システムは、マイナンバー普及や医療機関等の参画増大により、データ量が増大することが想定されているシステムである。稼動状況の分析等を行うため業務サイクルを考慮し、レベル4とする。
64							報告内容のレベル	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	障害および運用状況報告に加えて、改善提案を行う			3	C	障害および運用状況報告に加えて、改善提案を行う	3	C	障害および運用状況報告に加えて、改善提案を行う	3	C	障害および運用状況報告に加えて、改善提案を行う	－	－	－	－	－	－	本システムは、マイナンバー普及や医療機関等の参画増大により、データ量が増大することが想定されているシステムであり、改善を要する運用項目が発生すると思われる。そのため、報告においては改善提案を加える必要があるので、レベル3とする。

【C-1-4】移行要件

本資料の構成、目次（本編）

移行要件

移行に係る共通要件と教育に係る要件として必要な作業項目（作業プロセス）を洗い出した説明資料

本資料の構成、目次（補足資料）

補足1．医療機関等のシステム導入・利用開始に関する補足資料

移行要件の特記事項（トピック）として、【医療機関等のシステム導入・利用開始】に関する補足説明資料

補足２．シリアル番号の移行に関する補足資料

移行要件の特記事項（トピック）として、【シリアル番号の移行】に関する補足説明資料

補足３．医療保険者等のオンライン資格確認サービスへの対応に関する補足資料

移行要件の特記事項（トピック）として、【医療保険者等のオンライン資格確認サービスへの対応】に関する補足説明資料

移行要件

1 移行要件の定義

- 「医療保険者等向け中間サーバー等ソフトウェア　設計・開発業務等　調達仕様書」では、移行に関する要件は『**9章　導入要件定義**』としてまとめられ、**“導入に係る要件”**と**“教育訓練に係る要件”**とで構成されていた。
- オンライン資格確認サービスにおいても、同様に**“移行（導入）”**と**“教育”**を合わせて移行要件と定義する。

医療保険者等向け中間サーバー等

医療保険者等向け中間サーバー等ソフトウェア
設計・開発業務等　調達仕様書　目次（抜粋）

9．導入要件定義
- 9．1　導入に係る要件
  - 9．1．1　導入に係る前提条件
  - 9．1．2　本稼動実施計画書の作成
  - 9．1．3　本稼動判定要領の作成
  - 9．1．4　本稼動リハーサルの実施
  - 9．1．5　導入作業の実施
- 9．2　教育訓練に係る要件
  - 9．2．1　教育訓練実施計画書の作成
  - 9．2．2　教育訓練実施体制
  - 9．2．3　教育訓練の対象及び内容
  - 9．2．4　教育訓練用教材の作成
  - 9．2．5　教育訓練環境の準備
  - 9．2．6　教育訓練実施時の支援

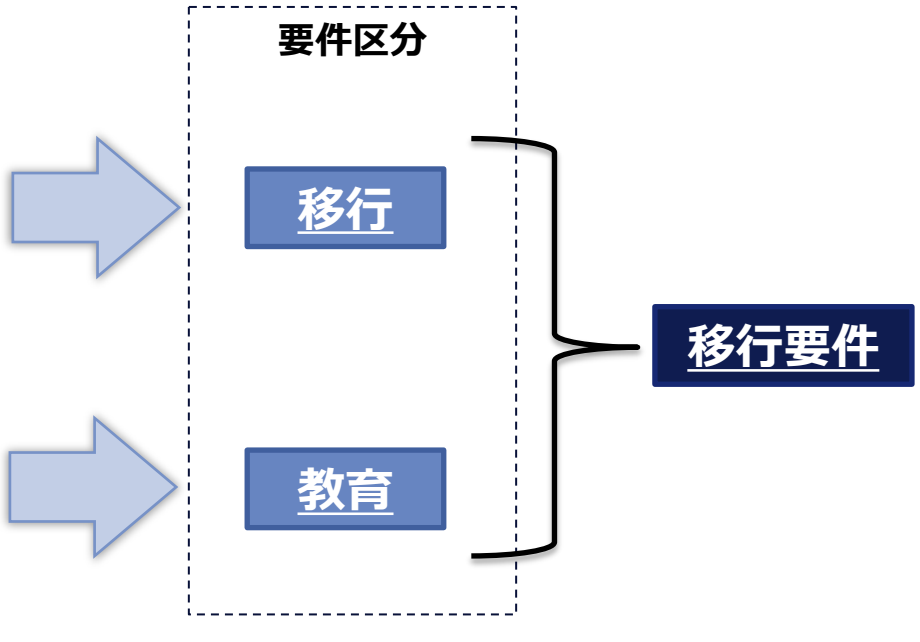


図１　導入要件定義と移行要件（要件区分）の対応

移行要件

2 移行要件の重点項目（調達要件に資する情報整理）

- オンライン資格確認サービスに係る移行要件について、今後設計開発等を委託する事業者（以降「受託事業者」）に要求する内容を重点項目として以下のとおり整理する。

表１　移行要件に関する重点項目

項番	大項目	中項目	小項目	内容
4-1	移行要件	移行に係る要件	共通要件	移行計画、役割分担、移行リハーサル、本番切り替え、移行判定、関係する他調達事業者との調整
4-2			システム要件	トピック① 医療機関等の導入に関するシステム要件
4-3			データ移行要件	トピック② シリアル番号の初期突合
				トピック③ 医療保険者の資格確認用情報の初期登録
4-4			機能移行要件	アプリケーション切替
4-5		教育に係る要件	教育要件	教育訓練実施計画書、教育訓練実施体制と役割、教育訓練スケジュール、教育訓練内容、教育訓練環境の準備、教育訓練実施報告書

- このうち、“共通要件” と “教育要件” については、具体的な作業項目を次ページ以降に整理（情報提供）する。
- また、移行に係る要件のうち、以下の３つのイベントを特記事項（トピック）として別紙資料で説明する。
  - トピック①　全国の医療機関等が段階的にシステムを導入することに関するシステム要件　→【補足１】
  - トピック②　シリアル番号の初期突合（住基ネットとの連携、機関別符号取得との関係）　→【補足２】
  - トピック③　医療保険者の資格確認用情報（加入者情報の不足分）の初期登録　→【補足３】

移行要件

3 移行作業の共通要件として記載すべき事項の整理

- 移行に係る作業は、移行計画を定め、移行計画に則って移行作業を実施し、本番移行作業を実施することおよび完了したことを確認する移行判定を行うという３ステップを実施する。
- 移行作業の実施にあたって、オンライン資格確認の導入に伴い医療機関等窓口での業務に支障がないようにしなければならないため、事前に「移行リハーサル」を実施することが望ましい。
- また、医療機関等における端末導入や医療保険者からの資格確認情報の初期登録などを効率的に実施できるよう、必要に応じて移行用のツールを作成することも考えられる。
- 移行に係る共通要件として受託事業者に要求する内容を以下の表に示す。

表２　調達仕様書の共通要件に記載すべき事項と受託事業者が記載すべき内容

受託事業者に要求する事項	受託事業者が移行計画を定め実施すべき内容
1. 移行計画	・移行方式 （拠点展開・業務展開の段階的移行方法、移行ツールの作成有無・概要） ・移行対象資産の定義 （移行対象システム、移行対象データ、移行対象機能） ・移行実施の関係者 ・移行リハーサルの実施内容、範囲 （移行リハーサル実施者、実施回数、移行データのインタフェース確認、不正データの確認、移行時間・手順の確認、移行作業実施後の業務確認、切り戻し手順の確認など） ・移行スケジュール （システム移行期間、システム停止可能日時、並行稼動の有無など）
2. 移行作業の実施	
2-1. 移行リハーサル	
2-2. 本番移行作業	
3. 移行判定	・移行判定基準 （移行判定者、システム稼働前に移行が完了していることを判定するための基準） ・移行作業完了報告

移行要件

4 教育要件に記載すべき事項の整理

- 教育に係る共通要件として受託事業者に要求する内容を以下の表に示す。
- 教育の実施方法については、一般的に、集合型研修(説明会)やデモンストレーション、e-ラーニング等が考えられるが、医療機関等利用者に対しては業務の影響や利用環境等の制約を考慮した現実的な手段を採用する必要がある。
- フェーズ１での教育実施後は、教育完了の判定と今後の改善を目的として、教育対象者からアンケートや教育参加率等の情報収集を行うことが望ましい。

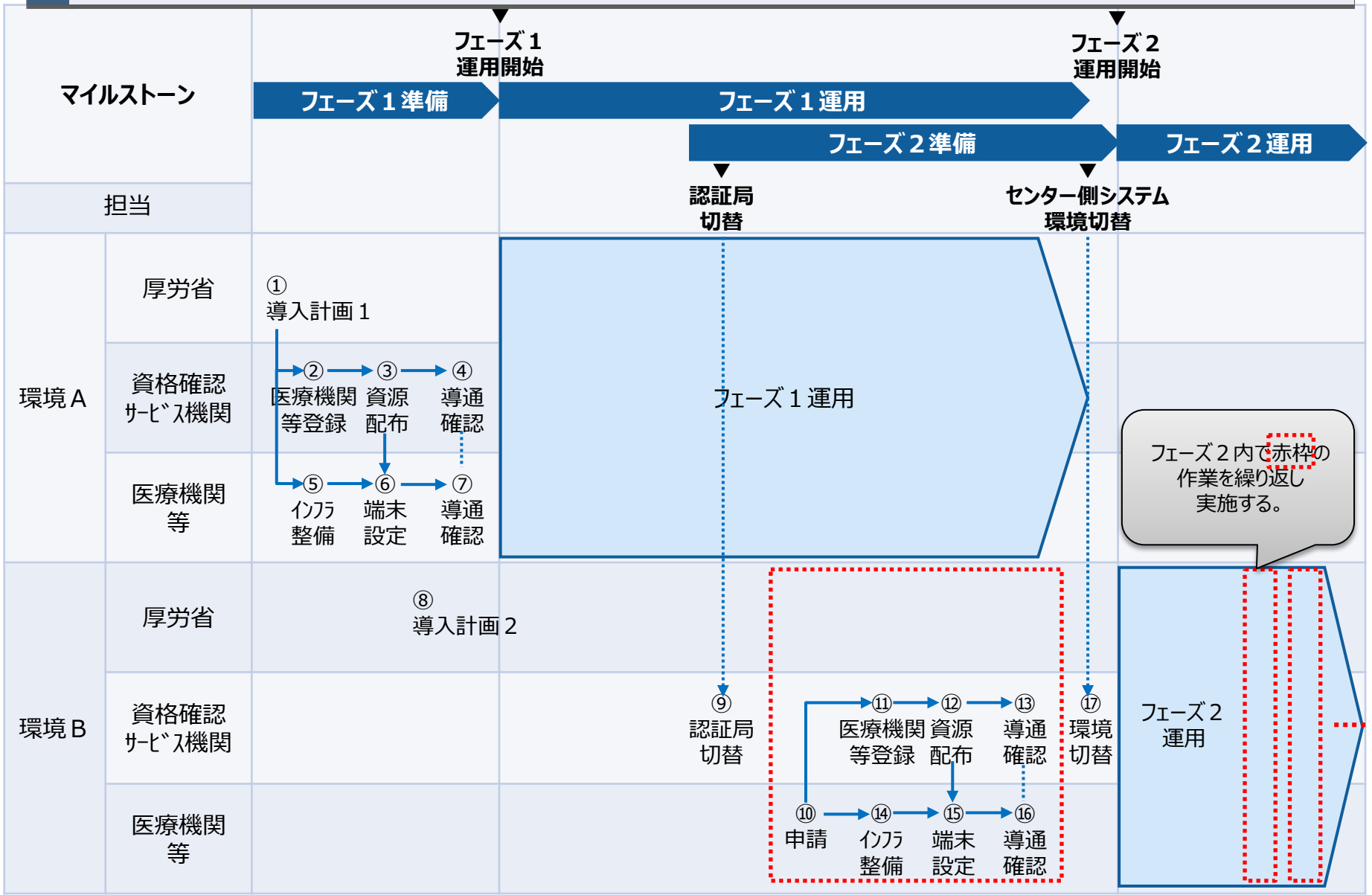
表３　調達仕様書の教育要件に記載すべき事項と受託事業者が記載すべき内容

受託事業者に要求する事項	受託事業者が教育計画を定め実施すべき内容
1. 教育計画	・教育の目的 ・対象者 （医療機関等利用者、資格確認サービス機関利用者、運用・保守実施者など） ・教育コンテンツ ・研修方法 （集合研修形式／デモンストレーション／eラーニング／資料配布など） ・教材、教育環境（デモンストレーションやe-ラーニングを実施する場合は動作環境が必要） ・実施スケジュール ・実施場所 ・習熟確認 （アンケート、教育参加率、習熟度確認テストなど）
2. 教育実施	
3. 教育判定 （習熟確認）	

補足１．医療機関等のシステム導入・利用開始に関する補足資料

補足１．医療機関等のシステム導入・利用開始に関する補足資料

1 医療機関等向け移行作業のイメージ（案）



補足１．医療機関等のシステム導入・利用開始に関する補足資料

2 医療機関等向け移行作業概要（案）

No.	移行作業名	作業内容	ﾀｲﾐﾝｸﾞ ﾌｪｰｽﾞ１ ﾌｪｰｽﾞ２	担当（●主、△副）		
				厚労省	資格確認 ｻｰﾋﾞｽ機関	医療機関等
①	導入計画１	フェーズ１の１００医療機関等を選定し、導入説明等を行う。	1	●		△
②	医療機関等登録	医療機関等を認証局に登録する。	1		●	△
③	資源配布	オンライン資格確認システムの資源等を医療機関等へ配布する。	1		●	
④	導通確認 (システム側)	オンライン資格確認システムと医療機関等の導通確認おける資格確認システム側の作業を実施する。	1		●	△
⑤	インフラ整備	医療機関等側が端末機器及びネットワークの整備を行う。	1			●
⑥	端末設定	医療機関等の端末にオンライン資格確認システムから配布された資源等を設定する。	1		△	●
⑦	導通確認 (医療機関等側)	資格確認システムと医療機関等の導通確認おける医療機関側の作業を実施する。	1		△	●
⑧	導入計画２	フェーズ２の医療機関等の導入計画を策定する。	2 前	●		
⑨	認証局切替	オンライン資格確認システム側の医療機関等の認証局の切替を行う。	2 前		●	
⑩	申請	医療機関等がオンライン資格確認システム利用申請を行う。	2		△	●
⑪	医療機関等登録	医療機関等を認証局に登録する。	2		●	△
⑫	資源配布	オンライン資格確認システムの資源等を医療機関等へ配布する。	2		●	
⑬	導通確認 (システム側)	オンライン資格確認システムと医療機関等の導通確認おけるオンライン資格確認システム側の作業を実施する。	2		●	△
⑭	インフラ整備	医療機関等側が端末機器及びネットワークの整備を行う。	2			●
⑮	端末設定	医療機関等の端末にオンライン資格確認システムから配布された資源等を設定する。	2		△	●
⑯	導通確認 (医療機関等側)	オンライン資格確認システムと医療機関等の導通確認おける医療機関側の作業を実施する。	2		△	●
⑰	環境切替	フェーズ１の検証環境からフェーズ２の本番環境へシステム切替を実施する。	2		●	

補足１．医療機関等のシステム導入・利用開始に関する補足資料

3 医療機関等向け移行にかかる留意事項

- 医療機関等向け移行に関して、オンライン資格確認システム側の設計・開発スコープに特に影響を及ぼす留意事項について以下に示す。

医療機関等の導入計画の策定について

厚労省・資格確認サービス機関側で検討いただく留意事項	システム側の対策
・フェーズ２の医療機関等の導入方針・スケジュールの提示 ✓ 医療機関への導入を何年かけて行うか ✓ 計画的な段階的導入（地域、医療機関等種別）を図るか、等	・厚労省・資格確認サービス機関が策定したフェーズ２の医療機関等の導入方針に沿った基盤設計（増設等）を検討する。

医療機関等の大量申請にかかる考慮

厚労省・資格確認サービス機関側で検討いただく留意事項	システム側の対策
・フェーズ２における医療機関等の大量申請の受付・審査についての対応方針の検討 ✓ 一時的な人員増加による対応 ✓ 部分的な自動化（※） ※医療機関等の審査・承認は人的判断が必要となるため、完全自動化は実施できないと想定	・医療機関等の申請の自動化範囲の方針により自動化に向けた機能を検討する。以下に自動化機能の例を示す。 -電子申請・受付機能 -審査結果登録機能 -結果通知書の作成機能（結果を郵送する場合） -結果通知連絡機能（電子的に連絡する場合） 等

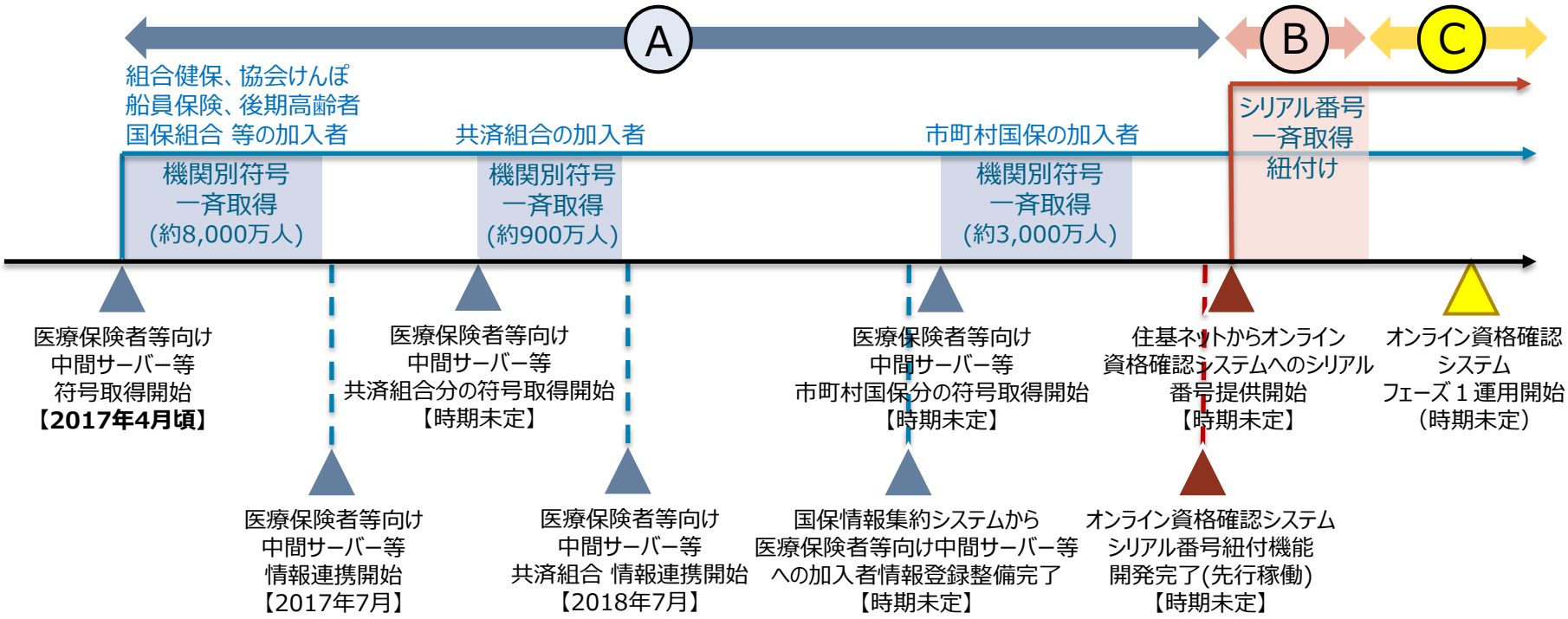
各フェーズにおける運用環境・検証環境（導通確認用環境）の整備について

厚労省・資格確認サービス機関側で検討いただく留意事項	システム側の対策
・全体スケジュールとの整合性をとった、各々のフェーズの運用環境と検証環境（導通確認用環境）、保守環境等の整備方針の検討	・以下の観点で検討する。 -検証・移行に必要な各環境の構成検討 -データの切替方法（フェーズ１からフェーズ２へのデータ移行等） -ネットワークの切替方法（医療機関等向け、中間サーバ等向け）

補足２．シリアル番号の移行に関する補足資料

補足２．シリアル番号の移行に関する補足資料

1 シリアル番号の紐付けにまつわる各種イベントの関係図



- 期間A（医療保険者等向け中間サーバー等が符号取得し始めてから、シリアル番号と処理通番の情報を住基ネットから受領し始めるまで）
  - 医療保険者等向け中間サーバー等の機関別符号の取得が先に開始するため、その際、先に生成される処理通番を住基ネット側で保管または後から取得する等の暫定措置をしてもらえるかが課題（★後述）
- 期間B（対象者全員のシリアル番号と処理通番の情報を住基ネットから一斉に受領する期間）
  - 期間Ｂの開始時点で、対象者全員※の最新のシリアル番号と処理通番の紐付情報を一斉に提供してもらうことが条件となる。

    ※対象者とは、医療保険加入者（上記のとおり共済組合と市町村国保加入者含む）のうち利用者用証明書の交付を受けている人
- 期間C（随時、発行されたりや更新されたりするシリアル番号と処理通番の情報（差分）を住基ネットから随時受領する期間）
  - 期間Ｂ以降は、マイナンバーカード（利用者用証明書）の新規発行を受けた人はシリアル番号と処理通番の情報を、再発行や更新手続きを行った人は新・旧のシリアル番号のセットを、住基ネットから随時受領することとなる。

補足２．シリアル番号の移行に関する補足資料

2 (前頁の期間Aにおける) シリアル番号の初期突合に関する課題

- 前頁の期間Aにおける課題について、総務省/J-LISに照会したところ以下の回答があった。（照会番号：J011）

問い合わせ内容（2017/2/9）

【オンライン資格確認開始前の移行について】
オンライン資格確認においては、運用開始前の初期移行として、対象者全員の紐付情報（シリアル番号と処理通番）を取得しておく必要があります。また、全対象者のうち、医療保険者等向け中間サーバー等においては、2017年の4月頃以降から市町村国保以外の加入者（約8,000万人）の符号取得が開始されます。これらの符号取得開始から初期移行までに符号を取得した加入者の紐付情報（シリアル番号と処理通番）は、初期移行時に一括で提供いただける認識でよろしいでしょうか。

回答（2017/2/14）

初期移行時の一括提供は可能となります。システム的な改修については、対応費用として国費等での裏づけなど必要となるため現時点では着手にいただっておりません。また改修に必要となる、シリアル連携をするための暫定的な方法なども現時点では決まっておりません。案ベースでご提示させて頂いてる、処理通番とシリアル番号を紐付ける方法を実現するには、機関別符号の払出し依頼時の要求電文を一時保管をしておくことで、再度シリアルと一緒に処理通番を返すことが可能となります。このための制度上必要な整理や判断を早急に詰める必要があると認識しております。

- この回答のとおり、医療保険者等向け中間サーバー等が既に機関別符号及び処理通番を取得した対象者に対しては、住基ネットワーク側で要求電文を一時保管してもらうことにより、資格確認サービス機関及び取りまとめ機関では特段の措置（機関別符号の再取得要求等）は不要であることが分かった。
- ただし、住基ネット側でその措置を行うための、制度上の整理や判断がなされていないことから、医療保険者等向け中間サーバー等において機関別符号取得が開始される来月（2017年4月）までに間に合うよう早急に決定していただく必要がある。

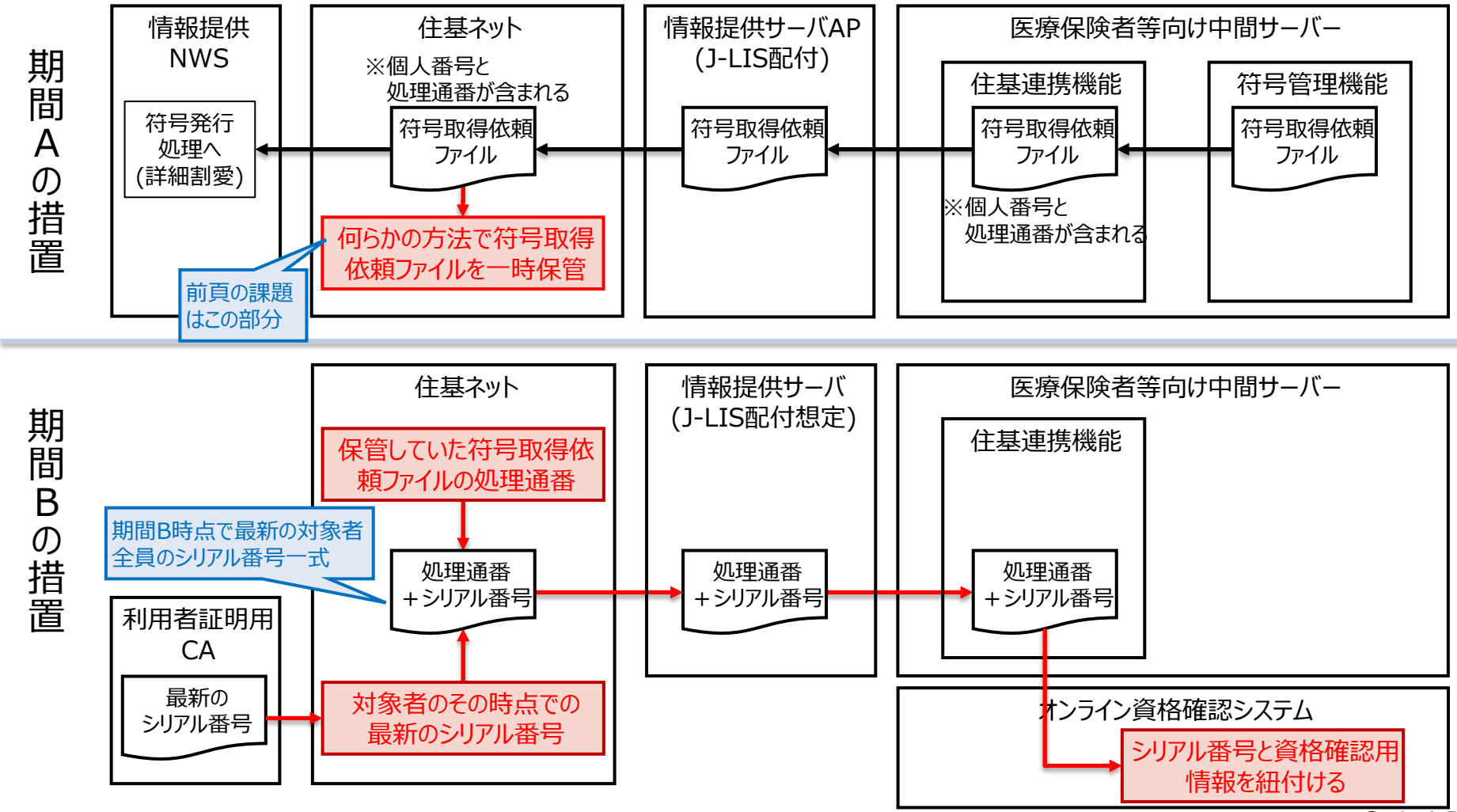
補足２．シリアル番号の移行に関する補足資料

3 期間Ａ・期間Ｂにおけるシリアル番号の初期移行イメージ

- 期間Ａ、期間Ｂにおけるシリアル番号の初期移行時の処理イメージを以下に示す。

※下図は大まかな処理イメージ。連携方式や連携ファイルの仕様は、設計開発工程において総務省/J-LIS様と調整して決定する必要がある。

※シリアル番号＋処理通番の紐付情報を授受する仕組みは、医療保険者等向け中間サーバー等の資源・機能の流用を前提としている。



補足３．医療保険者等のオンライン資格確認サービスへの対応に関する補足資料

補足３．医療保険者等のオンライン資格確認サービスへの対応に関する補足資料

1 主な考慮すべきポイント

- 医療保険者等におけるオンライン資格確認サービスへの対応に際して、特に整理検討が必要な事項として以下2点が考えられる。本項では、これらについて留意すべきポイント等を整理する。

  ➢ 中間サーバー等における現行業務への影響

  ➢ 医療保険者等の資格確認用情報の初期登録（※）に係るスケジュール

  ※今回、保険者インターフェースとして追加変更となった情報項目の登録、及び市町村国保（国保情報集約システム）と中間サーバー等との接続開始を指す。なお、現行の加入者情報登録IFにも存在するが、任意項目のため未登録の状態となっている情報に関する登録作業も含む。

2 現行業務への影響

- 現行業務への影響を最小化するために、考慮すべき主な事項を記す。

項番	事項	内容
1	既存データの継続利用	既に中間サーバー等に登録されている情報については、現行業務で使用されているため、初期登録後も継続して利用できる必要がある。
2	テスト環境等の整備	現行システムが運用中のため、オンライン資格確認サービス導入に伴う各種検証を目的とした接続検証環境及び保守環境相当の環境を新たに用意する必要がある。
3	本番環境の作業スケジュール	本番環境に対してリリース等の変更作業を行う場合、週末等、サービス停止日を前提とした作業スケジュールを検討する必要がある。

3 医療保険者等の初期登録について

- フェーズ１において求められるオンライン資格確認のサービスレベルにより、医療保険者等の初期登録に係るスケジュール要件は異なるものと思われる。想定されるサービスレベル案を以下に示す。

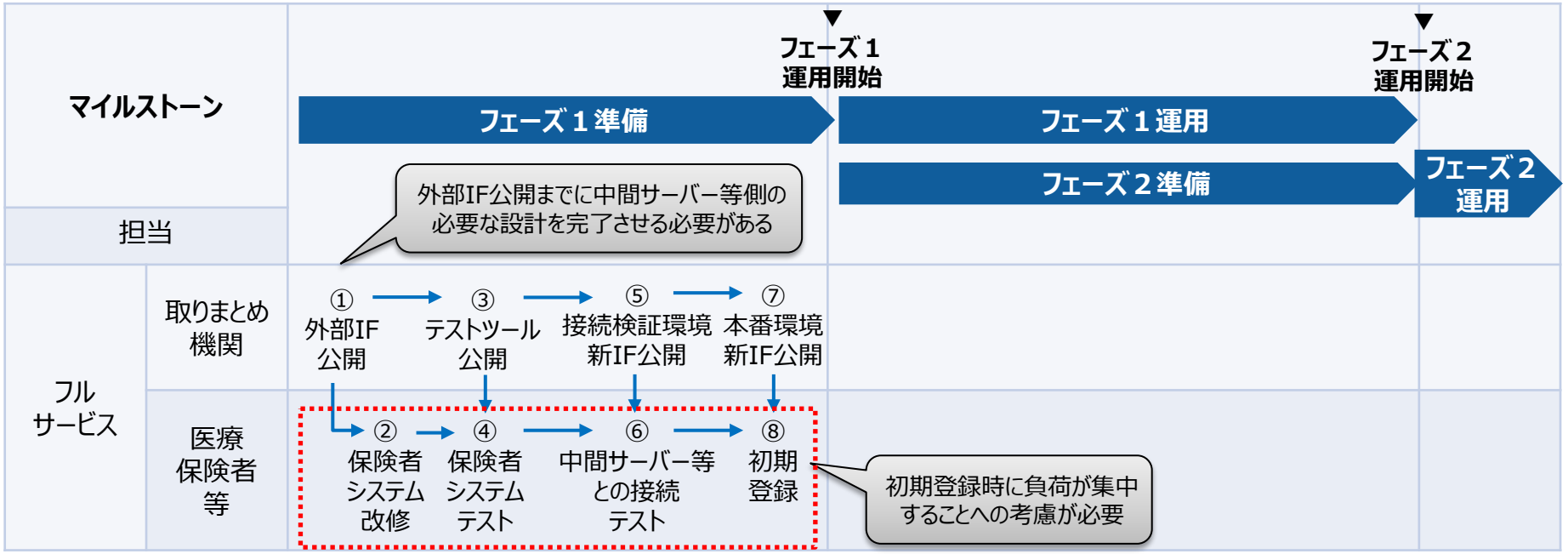
項番	フェーズ１ サービスレベル案	サービス内容
1	フルサービス	フェーズ１より、全医療保険者等の加入者にて今回対象とした資格確認用情報等すべてを確認可能とする
2	スモールスタート	フェーズ1については、現在、中間サーバー等に登録されている情報の範囲での資格確認を許容する

4 初期登録に係るスケジュール要件（サービスレベル案別）

- 各サービスレベル案で求められる初期登録に係るスケジュール要件を以下に示す。

項番	フェーズ１ サービスレベル案	初期登録に係るスケジュール要件	想定される 初期登録方式
1	フルサービス	・フェーズ１開始までに中間サーバー等および全医療保険者等のシステム改修を行い、初期登録を完了させる必要がある。 ・市町村国保（国保情報集約システム）については、上記対応に加えて、初期登録の中で機関別符号の取得も含め完了させる必要がある。	一斉登録 （新IFへの 一斉切替）
2	スモールスタート	・経過措置として、フェーズ1開始から一定の期間は、現行インターフェースでの資格情報等の登録が許容される。（新旧インターフェースの並行運用） ・経過措置期間満了までに、各医療保険者等（市町村国保含む）はシステム改修を行い、準備が整った保険者から新IFへの切替申請を行い、初期登録を完了させる必要がある。	保険者ごとの 段階的登録 （新IFへの 保険者単位での 順次切替）

5 初期登録までの想定作業スケジュール（フェーズ１のサービスレベル：フルサービス）



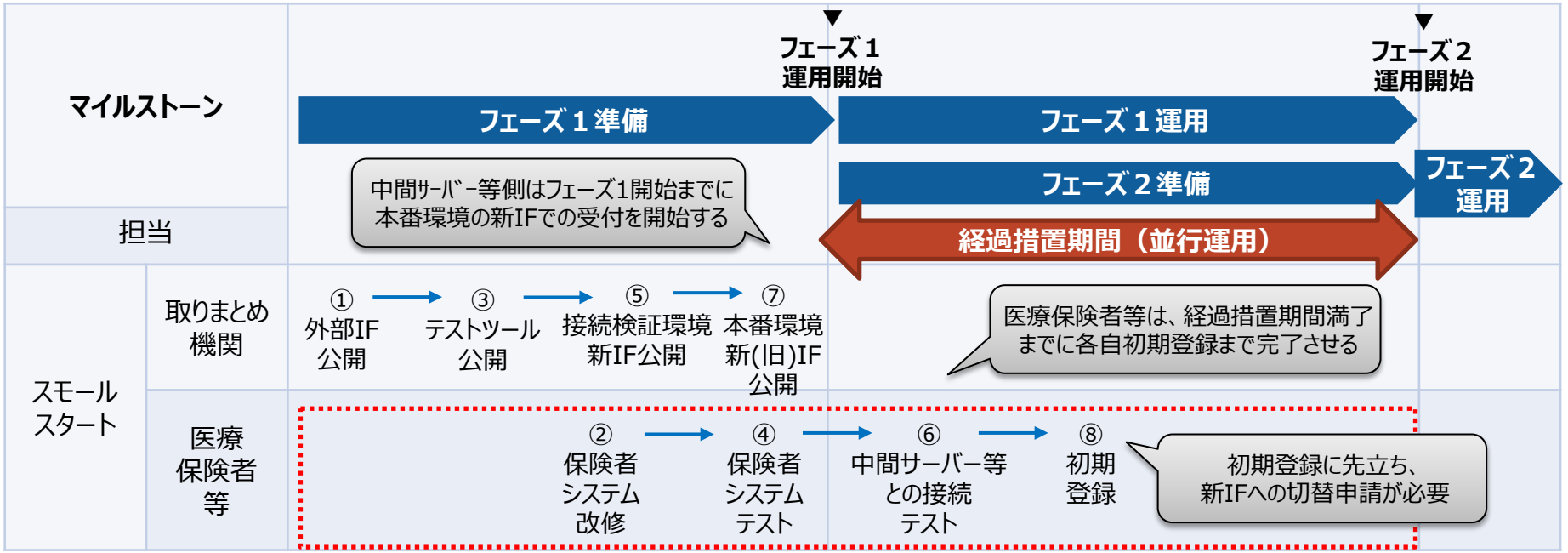
・フェーズ１開始までに中間サーバー等／医療保険者等双方のシステム改修、テスト等を完了させ、初期登録を実施する必要があるため、非常にタイトなスケジュールとなることが予想される。

・一斉登録となるため、中間サーバー等側としては新旧IFの並行運用の考慮は不要。
一方、フェーズ1開始までに対応が間に合わない医療保険者等が出てきた場合、初期登録やフェーズ１運用開始時期の延伸等、マスタスケジュールの見直しが求められる可能性がある。

・初期登録時は、全医療保険者等の登録作業が集中するため、高負荷対策が別途必要となる可能性がある。

※各機関の予算措置や調達等に係るスケジュールは考慮していない。

6 初期登録までの想定作業スケジュール（フェーズ１のサービスレベル：スモールスタート）



・医療保険者等は経過措置期間満了までに初期登録を完了すればよいため、医療保険者等ごとに適宜のスケジュールでの対応が可能。

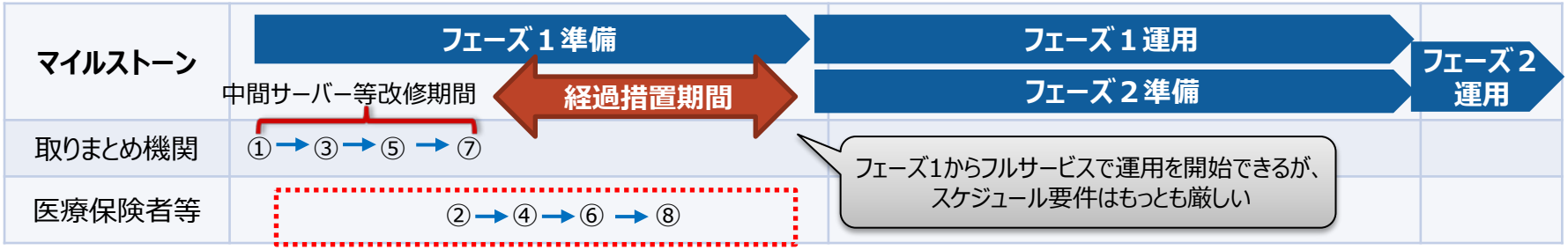
・初期登録の時期が医療保険者等ごとに分散されるため、初期登録に係る負荷の平準化を見込むことができる。

・医療保険者等ごとの段階的登録を許容するため、中間サーバー等側は新旧IFの並行運用を想定する必要がある。
また、医療保険者等の切替申請等に基づき、保険者単位で新IFへの切替えを可能とする仕組みが必要となる。

※上記はフェーズ1開始までに新IFでの受付を可能とし、フェース2開始までを経過措置期間と仮置きした場合のもの。

7 初期登録までの想定作業スケジュール（その他：段階的登録＆フルサービス）

- その他、フェーズ１開始までに経過措置期間を設け、段階的登録を行ったうえで、フェーズ1からフルサービスで運用を開始する案も考えられるが、この場合、中間サーバーの改修（オンライン資格確認システムとの接続テスト等含む）を極めて短期間で完了させる必要が生じるため、スケジュール要件としてはもっとも厳しいものとなる。

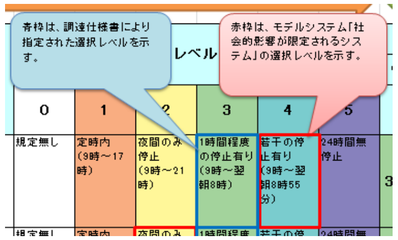


8 その他留意すべき事項

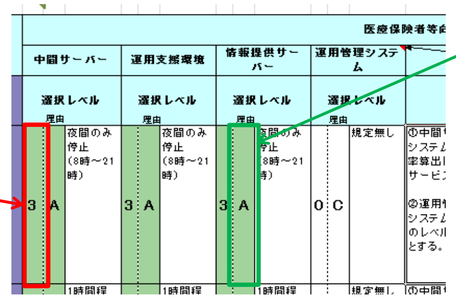
項番	サービスレベル案	留意事項	内容
1	スモールスタート	経過措置期間（並行運用）中のサービス制限	・経過措置期間中は、医療保険者等ごとにオンライン資格確認で確認できる情報に差異が生じるため、医療機関等側の運用上、考慮が必要。 ・同様に、オンライン資格確認システムの医療機関側IFにおいても考慮が必要。
2		フェーズ1での検証に向けた先行団体の選定	・フェーズ1の対象となる医療機関等も踏まえたうえで、経過措置期間中に先行して初期登録を行ってもらう医療保険者等を選定する必要がある。
3	共通	並行する改修スケジュール等の考慮	・中間ｻｰﾊﾞｰ等にて別途予定されている共済組合対応等、並行する改修案件等を踏まえ、全体スケジュールの整合性を確保する必要がある。 ・保険者システム（国保集約含む）側の改修スケジュールへの考慮も必要。
4		被保険者番号（オンライン確認用）の証印字対応	・被保険者番号（オンライン確認用）の被保険者証への印字を、前述のスケジュールとは別線表で対応する場合、別途整理が必要。
5		対象とする加入者の範囲	・いつ時点の加入者から初期登録の対象とするか、整理が必要。

（1）選択レベルの表記例

以下に本資料の表記例を示します。



対象システムに該当する非機能要件レベル



【IPA非機能要求グレード選択レベルの選択理由】
下記、Aから順に優先順位となる。

A. 調達仕様書の記載から判断
B. モデルシステム「社会的影響が限定されるシステム」から判断
C. 監視等のオンライン業務に直接影響が無いことから判断
D. 個別に検討し、判断
E. 中間サーバーの運用に準ずることから判断

（2）非機能要件及び選択レベル

非機能要求グレード活用シート(原本の範囲)　／　要件定義工程における検討結果

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認										選択理由
								0	1	2	3	4	5	医療機関等向けサブシステム		中間サーバー連携等サブシステム		運用管理サブシステム		資格確認システム接続端末		資格確認サービス機関等端末		
								選択レベル						選択レベル		選択レベル		選択レベル		選択レベル		選択レベル		
1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	ユーザが遵守すべき情報セキュリティに関する組織規程やルール、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、遵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） ・情報セキュリティポリシー ・不正アクセス禁止法 ・個人情報保護法 ・電子署名法 ・プロバイダ責任法 ・特定電子メール送信適正化法 ・SOX法 ・IT基本法 ・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 ・FISMA ・FISC ・PCI DSS ・プライバシーマーク ・TRUSTe など		○	遵守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り				1 A	有り	1 A	有り	1 A	有り	1 A	有り	1 A	有り	1 A	有り	調達仕様書より、遵守および参考とする文書が規定されていることから、レベル1を選択する。 ・政府機関の情報セキュリティ対策のための統一基準 ・厚生労働省情報セキュリティポリシー ・厚生労働省保有個人情報管理規定 情報セキュリティ対策の検討に当たって、遵守および参考とする文書は「1．基盤要件定義書_はじめに（制約条件）」にて記載する。 また、セキュリティ要件において追加で参考とする文書を下記に示す。 文書名：情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 発行元：内閣官房情報セキュリティセンター 発行時期：2015/5/21 ■資格確認システム接続端末■ ※「医療情報システムの安全管理に関するガイドライン」が規定されている。
2		セキュリティリスク分析	セキュリティリスク分析	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。		○	リスク分析範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲			1 D	重要度が高い資産を扱う範囲、あるいは、外接部分	1 D	重要度が高い資産を扱う範囲、あるいは、外接部分	1 D	重要度が高い資産を扱う範囲、あるいは、外接部分	1 D	重要度が高い資産を扱う範囲、あるいは、外接部分	1 D	重要度が高い資産を扱う範囲、あるいは、外接部分	オンライン資格確認システムは、特定個人情報などの重要情報を取り扱うシステム（医療保険者等向け中間サーバー等）と物理的に分離する想定のため、脅威が現実のものとなった場合、上記データを取り扱うシステムと比べて影響が低いと想定する。 このため、システムリスクを分析する範囲は開発範囲全てではなく、重要度が高い資産を扱う範囲に限定し、レベル1を選択する。 ■資格確認システム接続端末■ 「医療情報システムの安全管理に関するガイドライン」が規定されており、医療機関のポリシーに依存するが、資格確認システム接続端末に起因するセキュリティリスクについては分析を行う必要があると考える。 選択レベルは他のサブシステムと同様のレベル1を選択する。
3		セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント（設計書や環境定義書、実装済みソフトウェアのソースコードなど）に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。		○	ネットワーク診断実施の有無	無し	有り					1 D	有り	1 D	有り	1 D	有り	– –	–	1 D	有り	「政府機関の情報セキュリティ対策のための統一基準」において情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要とされている。 本システムのように、重要な情報資産を取り扱うシステムに対しては、実施されている情報セキュリティ対策が有効に機能しているか妥当性を確認するため、専用のツール等によるネットワーク診断、Webアプリケーション、データベース診断を実施することが推奨されることから、各診断種別のレベルとしてレベル1を選択する。 ※ただし、データベース診断については中間サーバーの非機能要求検討時に追加した項目であり、IPA非機能要求グレードにおいても重要項目となっていないことから、実施方法については基本設計以降のフェーズで決定することとする。 ■資格確認システム接続端末■ ※「医療情報システムの安全管理に関するガイドライン」が規定されており、医療機関のポリシーにも依存するため、セキュリティ診断のレベル選定対象外とする。 また、端末のためデータベース診断の実施は対象外とする。 ■資格確認サービス機関等端末■ 端末のためデータベース診断の実施は対象外とする。
4						○	Web診断実施の有無	無し	有り					1 D	有り	1 D	有り	1 D	有り	– –	–	1 D	有り	
5							データベース診断実施の有無	無し	有り					1 D	有り	1 D	有り	1 D	有り	– –	–	– –	–	

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル 0	1	2	3	4	5	オンライン資格確認 医療機関等向けｻﾌﾞｼｽﾃﾑ 選択レベル			中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ 選択レベル			運用管理ｻﾌﾞｼｽﾃﾑ 選択レベル			資格確認ｼｽﾃﾑ接続端末 選択レベル			資格確認ｻｰﾋﾞｽ機関等端末 選択レベル			選択理由
6		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目。 セキュリティリスクの見直しには、セキュリティホールや脆弱性、新たな脅威の調査等が含まれる。			セキュリティリスク見直し頻度	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施				2	D	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	2	D	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	2	D	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	1	D	セキュリティに関するイベントの発生時に実施（随時）	2	D	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	「政府機関の情報セキュリティ対策のための統一基準」では情報セキュリティ対策を定期的に見直し、さらに外部環境の急激な変化等が発生した場合は、適宜見直しを行うことが必要とされている。 また、医療保険者等向け中間サーバー等の資産を利活用する想定であることから、中間サーバーの調達仕様書に記載されている「遵守すべき文書の見直しが実施された場合は、その内容を適切に反映し、セキュリティ対策の見直しを行う」についても一部遵守する必要があるため、セキュリティリスク見直し頻度についてはレベル2を選択する。 本システムでは遵守すべき文書である「政府機関の情報セキュリティ対策のための統一基準」及び「医療情報システムの安全管理に関するガイドライン第4.2 版」の改訂が発生した場合にはセキュリティリスクの見直しを行う必要がある。 ■資格確認システム接続端末■ ※「医療情報システムの安全管理に関するガイドライン」が規定されており、医療機関のポリシーに依存するため、資格確認サービス機関による定期保守は実施しない想定だが、ウィルス感染、不正侵入、DoS攻撃、情報漏えいなどの情報セキュリティに関するインシデントが発生した際には何かしらの対応が発生し得ると想定し、レベル1を選定する。
7							セキュリティリスクの見直し範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	セキュリティリスクの見直し範囲は「項番2.セキュリティリスク分析」にて定義した範囲とし、レベル1を選択する。 ■資格確認システム接続端末■ 医療機関等のポリシーによって運用されるものの、運用開始後に発覚した脅威に対するリスク分析は必須と考え、他のサブシステム同様のレベル1を選定する。
8			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目。 また、検討するにあたり、発見された脅威についての対応範囲について明らかにする。			運用開始後のリスク対応範囲	対応しない	重要度が高い資産に関連する、あるいは、外接部分の脅威に対応	洗い出した脅威全体に対応				2	D	洗い出した脅威全体に対応	2	D	洗い出した脅威全体に対応	2	D	洗い出した脅威全体に対応	0	D	対応しない	2	D	洗い出した脅威全体に対応	セキュリティリスク対策では洗い出した脅威全体に対応することが重要であるため、運用開始後のリスク対応範囲としてレベル2を選択する。 但し、実際に実施する対策のレベルについてはシステムの全体構成、周辺環境なども検討したうえで判断することとする。 ■資格確認システム接続端末■ 医療機関等の運用によるため、脅威に対する対応はしない想定。
9							リスク対策方針	無し	有り					1	D	有り	1	D	有り	1	D	有り	0	D	無し	1	D	有り	発見されたリスクに対してはセキュリティ対策でリスク低減することをリスク対策方針とし、レベル1を選択する。 ■資格確認システム接続端末■ リスク分析は実施するが、対策方針の決定は医療機関等により決定する想定のため、レベル0を選定する。
10			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。			セキュリティパッチ適用範囲	セキュリティパッチを適用しない	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	－	－	－	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	「政府機関の情報セキュリティ対策のための統一基準」において、セキュリティパッチの適用は情報システム全体への影響を考慮した上で、措置を講ずることが必要であるとされている。 全てのセキュリティパッチに対して情報システム全体への影響を考慮した上で該当するセキュリティパッチを選択し適用することとし、セキュリティパッチ適用範囲は「項番2.セキュリティリスク分析」にて定義した範囲とし、レベル1を選択する。 ■資格確認システム接続端末■ 医療機関等側の運用保守ポリシーに依存するため、本検討からは対象外とする。
11							セキュリティパッチ適用方針	セキュリティパッチを適用しない	緊急性の高いセキュリティパッチのみ適用	全てのセキュリティパッチを適用				1	D	緊急性の高いセキュリティパッチのみ適用	1	D	緊急性の高いセキュリティパッチのみ適用	1	D	緊急性の高いセキュリティパッチのみ適用	－	－	－	1	D	緊急性の高いセキュリティパッチのみ適用	「政府機関の情報セキュリティ対策のための統一基準」において、セキュリティパッチの適用は情報システム全体への影響を考慮した上で、措置を講ずることが必要であるとされている。 全てのセキュリティパッチに対して情報システム全体への影響を考慮した上で、緊急性の高いセキュリティパッチを選択し適用することとし、相当するレベル1を適用方針とする。 なお、適用時には、システムへの影響確認が必要なため、テスト環境で十分に検証を実施した後、本番環境への適用を行うこととする。 ■資格確認システム接続端末■ 医療機関等側の運用保守ポリシーに依存するため、本検討からは対象外とする。
12							セキュリティパッチ適用タイミング	セキュリティパッチを適用しない	障害パッチ適用時に合わせて実施	定期保守時に実施	パッチ出荷時に実施			2	D	定期保守時に実施	2	D	定期保守時に実施	2	D	定期保守時に実施	－	－	－	2	D	定期保守時に実施	セキュリティパッチ等の適用を適宜正確かつ迅速に行うことが求められると想定される。 セキュリティパッチの適用タイミングはパッチの緊急性のレベルに合わせて実施することが望ましい。 適用タイミングは基本的に定期保守時に実施することとし、レベル2を選択する。ただし、緊急かつ重要なセキュリティパッチについては、パッチ出荷後なるべく早い段階で適用することとする。適用はテスト環境で十分に検証を実施した後、本番環境への適用を行うこととする。 ■資格確認システム接続端末■ 医療機関等側の運用保守ポリシーに依存するため、本検討からは対象外とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認												選択理由
														医療機関等向けｻﾌﾞｼｽﾃﾑ			中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ			運用管理ｻﾌﾞｼｽﾃﾑ			資格確認ｼｽﾃﾑ接続端末			資格確認ｻｰﾋﾞｽ機関等端末			
								0	1	2	3	4	5	選択レベル			選択レベル			選択レベル			選択レベル			選択レベル			
13		アクセス・利用制限	認証機能	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、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、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カード等を用いた認証等がある。		○	管理権限を持つ主体の認証	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			3	D	複数回、異なる方式による認証	3	D	複数回、異なる方式による認証	3	D	複数回、異なる方式による認証	2	D	複数回の認証	3	D	複数回、異なる方式による認証	取り扱う情報は重要情報であり、管理者権限を持つアカウントの乗っ取りによる情報漏洩などの脅威に対抗するため、複数回の異なる方式による認証行うこととし、レベル3を選択する。 ただし、要件定義を進めていく中で、業務要件により変更する可能性あり。 ■資格確認システム接続端末■ 医療機関等窓口における業務運用を鑑み、多要素認証は必須としない想定とするが、医療機関等の担当者が資格確認システム接続端末を利用する際には、少なくとも端末（OS）へのログイン認証とオンライン資格確認システムへのログイン認証の2回は行う必要があると考えるため、レベル2（複数回の認証）を選定する。
14							管理権限を持たない主体の認証	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			1	D	1回	1	D	1回	1	D	1回	2	D	複数回の認証	3	D	複数回、異なる方式による認証	情報資産へのアクセスを許可された者のみに限定する想定ため、利用者を識別するための認証を行うレベル1を選択する。 ■資格確認システム接続端末■ 項番13と同様 ■資格確認サービス機関等端末■ 資格確認サービス機関や運用保守事業者にて利用する端末でありオンライン資格確認システム全体の稼働に影響を及ぼす業務・運用を行うことから、認証についてレベル3（多要素認証）を選定する。詳細については基本設計以降の設計フェーズにて確定させる。
15			利用制限	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、ソフトウェアやハードウェアにより制限するか確認するための項目。 例）ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。		○	システム上の対策における操作制限度	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を許可				1	B	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を許可	1	B	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を許可	1	B	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を許可	－	－	－	1	B	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を許可	各種情報資産の格付け及び取扱制限等の管理ルールを策定し、利用者の職責に応じたアクセス制御・利用制限を行うことを想定している。 また、選定モデルが推奨していることからも、レベル1を選択する。 ※ただし、資格確認サービス機関等端末について、運用・保守業者が定常作業や緊急時作業を行う際には、資格確認サービス機関に許可をもらった上で、操作制限を解除する可能性がある。 ■資格確認システム接続端末■ 医療機関等側の管理ルールに依存するため、本検討からは対象外とする。
16							物理的な対策による操作制限度	無し	必要最小限のハードウェアの利用や操作のみを許可					1	D	必要最小限のハードウェアの利用や操作のみを許可	1	D	必要最小限のハードウェアの利用や操作のみを許可	1	D	必要最小限のハードウェアの利用や操作のみを許可	－	－	－	1	D	必要最小限のハードウェアの利用や操作のみを許可	サーバー機器等を配置するデータセンタに対して、運用保守業者等を特定・認証し、権限に応じて入退室を許可するなどの利用制限が求められていることが想定される。 このことから物理的な対策による操作制限度としてレベル1を選択する。 ■資格確認システム接続端末■ 医療機関等側の管理ルールに依存するため、本検討からは対象外とする。
17			管理方法	認証に必要な情報（例えば、ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。			管理ルールの策定	実施しない	実施する					1	D	実施する	1	D	実施する	1	D	実施する	－	－	－	1	D	実施する	「資_03 オンライン資格確認サービスにおける利用者管理」の整理結果より、主体のアクセス権を適切に管理するため、アカウントを管理（登録、更新、停止、削除等）するための機能をシステムとして備えることを想定している。 上記から、認証に必要な情報の管理を実施する必要がありレベル1を選択する。 なお、具体的な管理ルールは基本設計にて策定する。 ■資格確認システム接続端末■ 医療機関等側の管理ルールに依存するため、本検討からは対象外とする。
18		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。		○	伝送データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				2	D	重要情報を暗号化	2	D	重要情報を暗号化	2	D	重要情報を暗号化	2	D	重要情報を暗号化	2	D	重要情報を暗号化	「政府機関の情報セキュリティ対策のための統一基準」では機密情報を取り扱う情報システムにおいて、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときには、当該機能を設けることが求められている。本システムでは、特定個人情報などを扱うシステムとは物理的に切り離す方針であるものの、重要情報を扱うことに変わりはない。このため、重要情報の暗号化が必須であると考える。 よって、伝送データの暗号化の有無についてレベル2を選択する。 なお、暗号化の対象、暗号化方式などの詳細については基本設計以降の設計フェーズにて確定させる。
19						○	蓄積データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				2	B	重要情報を暗号化	2	B	重要情報を暗号化	2	B	重要情報を暗号化	－	－	－	－	－	－	バックアップデータの暗号化を行い、漏えい時の被害を最小限にすることを想定しているため、選定モデルが推奨するレベル2 を選択する。 なお、暗号化の対象、暗号化方式などの詳細については性能面なども考慮し、基本設計以降の設計フェーズにて確定させる。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ データは全てサーバ側のデータベース及びストレージ装置に格納し、端末側にデータを蓄積する想定ではないため、対象外とする。
20							鍵管理	無し	ソフトウェアによる鍵管理	耐タンパデバイスによる鍵管理				1	D	ソフトウェアによる鍵管理	1	D	ソフトウェアによる鍵管理	1	D	ソフトウェアによる鍵管理	－	－	－	－	－	－	暗号鍵（秘密鍵）が万が一外部に漏えいした場合、オンライン資格確認システム全体の安全性や安定稼働に甚大な影響を及ぼすため、安全に保管しなければならない。ここでは設備費用面（安価な策）を鑑み、ソフトウェアによって鍵ファイルを安全に管理する方式（レベル1）を選択する。 ※ただし、指針・ガイドライン等により鍵の複製をより厳格に防止する対策等を求められる場合にはその限りではない。（レベル2（耐タンパデバイスによる鍵管理）を採用する可能性がある） ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 認証に用いる鍵の管理はサーバで実施する想定のため、端末は対象外とする。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認																選択理由
								0	1	2	3	4	5	医療機関等向けｻﾌﾞｼｽﾃﾑ			中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ			運用管理ｻﾌﾞｼｽﾃﾑ			資格確認ｼｽﾃﾑ接続端末			資格確認ｻｰﾋﾞｽ機関等端末			
								選択レベル						選択レベル			選択レベル			選択レベル			選択レベル			選択レベル			
21		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 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。		○	ログの取得	実施しない	実施する					1	D	実施する	1	D	実施する	1	D	実施する	－	－	－	1	D	実施する	論点整理(資_06)より、オンライン資格確認システムは大多数の個人情報を取り扱うシステムであるため、システムへのアクセスログを証跡管理対象として収集・管理しておく必要があると考えている。 HW/NW機器のログや、ミドルウェアのログ等についても、モデル推奨値はレベル1となっている。 上記より、レベル1を選定する。 ■資格確認システム接続端末■ 障害対策の観点から、医療機関等側の端末ログを取得するかどうかは、HISベンダーや医療機関等側の運用を確認して検討する必要があり、現時点での検討からは対象外とする。
22						○	ログ保管期間	6ヶ月	1年	3年	5年	10年以上有期	永久保管	2	D	3年	2	D	3年	2	D	3年	－	－	－	2	D	3年	論点整理(資_06)より、保管期間については、IPAにより公開されている「企業における情報システムのログ管理に関する実態調査」（平成28 年6 月）に基づき整理を行った結果「3年間」とすべきと提示している。 HW/NW機器のログや、ミドルウェアのログ等についても、モデル推奨値はレベル2となっている。 上記より、レベル2を選定する。 ※なお、証跡ログについて、J-LISから四半期単位での提示を求められている。（問合せ管理台帳：J015より） 上記要件により、3ヶ月以上のDISK上での保管要件が発生したため「DISK内保管：6ヵ月」という期間を設定する。 ■資格確認システム接続端末■
23						○	不正監視対象（装置）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	－	－	－	－	－	－	モデルシステムの推奨レベルであるレベル1を選定する。 具体的なサーバー、ストレージ等への不正アクセス等の監視のための、ログを取得範囲については、要件定義以降の設計フェーズにて、セキュリティ分析の対象を決定した上で確定させる。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 不正監視はサーバ側にて集約されたログ情報を用いて行う事を想定しているため、端末は対象外とする。
24						○	不正監視対象（ネットワーク）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	1	B	重要度が高い資産を扱う範囲、あるいは、外接部分	－	－	－	－	－	－	モデルシステムの推奨レベルであるレベル1を選定する。 具体的なネットワーク上の不正なパケット等を監視するためのログの取得範囲については、要件定義以降の設計フェーズにて、セキュリティ分析の対象を決定した上で確定させる。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 監視対象は、システムを敷設するデータセンターのネットワーク機器（FW、ルータ等）と想定されるため、端末は対象外とする。
25						○	不正監視対象（侵入者・不正操作等）	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	－	－	－	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	資格確認サービスの基盤について、中間サーバーと同センター内に設置する方針で仮定義しているため、不正な侵入者等を監視するために設置する監視カメラ等による監視の範囲は中間サーバーと同等のレベル1を選択する。 ■資格確認システム接続端末■ 医療機関等のセキュリティレベルに依存するため、本件等の対象外とする。
26							確認間隔	無し	セキュリティに関するイベントを認識した時に実施（随時）	セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施	常時確認			2	D	セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施	2	D	セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施	2	D	セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施	－	－	－	2	D	セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施	重要情報を取り扱うシステムであり、証跡管理だけでなく、不正行為に迅速に対処するため、通信内容の監視及びサーバー装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知できることが求められると想定される。セキュリティに関するイベントの発生時にはアラートなどで検知できる仕組みを導入するとともに、定期的なログの確認を実施することにより不正を監視する必要がある。よって確認間隔としては「セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施」の対応とすることとし、レベル2を選択する。 監視対象および監視対象に対する定期確認間隔等は、基本設計以降の設計フェーズにて確定する。 ■資格確認システム接続端末■ 医療機関の運用に依存するため、本件等の対象外とする。
27			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目。			デジタル署名の利用の有無	無し	有り					0	D	無し	0	D	無し	0	D	無し	0	D	無し	0	D	無し	オンライン資格確認システムはクローズドネットワークでの接続を前提としており、情報改ざん等のリスクは低いと考えられるため、処理性能を優先してデジタル署名は利用しないこととし、レベル0を選定する。
28							確認間隔	無し	セキュリティに関するイベントを認識した際に実施（随時）	セキュリティに関するイベントを認識した際に実施（随時）＋定期的に実施	常時確認			2	D	セキュリティに関するイベントを認識した際に実施（随時）＋定期的に実施	2	D	セキュリティに関するイベントを認識した際に実施（随時）＋定期的に実施	2	D	セキュリティに関するイベントを認識した際に実施（随時）＋定期的に実施	－	－	－	－	－	－	システムに保持される重要な情報資産やプログラム及びその設定ファイルに対し、不正アクセス、改ざん、すり替え等の攻撃に対する検知や防止を行えるよう、セキュリティ対策を施すことが求められると想定される。 セキュリティに関するイベントの発生時にはアラートなどで検知できる仕組みを導入するとともに、定期的なログの確認を実施することにより改ざんによる不正を監視する必要がある。 よって確認間隔としては「セキュリティに関するイベントを認識した時に実施（随時）＋定期的に実施」の対応とすることとし、レベル2を選択する。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 本項目は、データ検証における確認間隔を定義する項目である。 データは全てサーバ側にて管理される想定のため、端末は対象外とする。

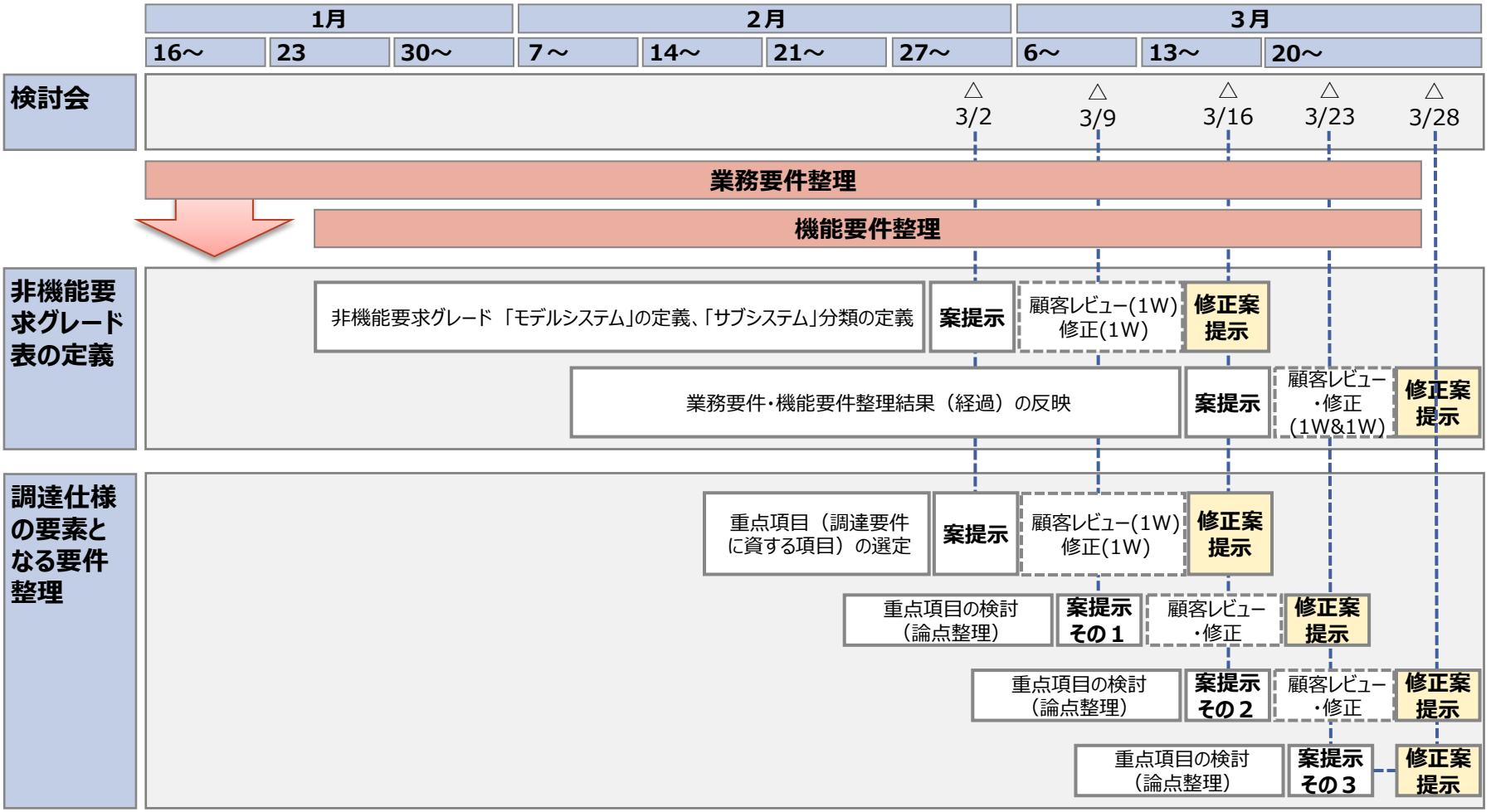
項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						オンライン資格確認										
														医療機関等向けｻﾌﾞｼｽﾃﾑ		中間ｻｰﾊﾞｰ連携等ｻﾌﾞｼｽﾃﾑ		運用管理ｻﾌﾞｼｽﾃﾑ		資格確認ｼｽﾃﾑ接続端末			資格確認ｻｰﾋﾞｽ機関等端末			
								0	1	2	3	4	5	選択レベル		選択レベル		選択レベル		選択レベル			選択レベル			選択理由
29		ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。		○	通信制御	無し	有り					1	D	有り		1	D	有り		－	－	－	－	－	－	本システムでは、通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上で遮断する機能を備えること、不正な通信、サービス停止攻撃等に対し通信の遮断や通信量の抑制等により、サービス停止の脅威を軽減する機能を備えることが求められると想定される。 選定モデルの推奨レベルや中間サーバー等の選定結果を鑑み、レベル1を選択する。 ※FWの外側であるレセプトオンライン請求用ネットワークや職員拠点ネットワーク、運用管理ネットワーク等、既存資源の流用部分についてはこの限りではない。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 不正検知時の通信遮断の仕組みは、サーバ側のミドルウェアにて実現する想定のため、端末は対象外とする。
30			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。		○	不正通信の検知範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	1	D	重要度が高い資産を扱う範囲、あるいは、外接部分	－	－	－	－	－	－	外部ネットワークからのマルウェアの侵入や、万が一マルウェアに侵入された場合の外部ネットワークへの不正な通信等を監視し、侵入の検知、防止及び当該マルウェアによる外部通信の遮断等を行うことが求められると想定する。マルウェアの侵入や外部ネットワークへの不正な通信等を監視するために、不正通信の検知範囲を重要度が高い資産を扱う範囲、あるいは、外接部分とし、レベル1を選択する。 外接部分としては、医療機関等との接続部分等を想定とする。 不正アクセス等による被害を最小化するため、不正通信を監視し、不正な通信の遮断・通知が行えるようIPS(侵入防止システム)/IDS(侵入検知システム)の導入を行う必要がある。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 検知の仕組みはサーバ側のミドルウェアにて実現する想定のため、端末は対象外とする。
31			サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。		○	ネットワークの輻輳対策	無し	有り					1	D	有り		1	D	有り		1	D	有り	－	－	－	－	－	－	不正な通信、サービス停止攻撃等に対し、通信の遮断や通信量の抑制等により、サービス停止の脅威を軽減する機能を備えることが必要と想定されているためレベル1を選択する。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ ネットワークの輻輳対策は、データセンター側の機器に対してで行う想定のため、端末は対象外とする。
32		マルウェア対策	マルウェア対策	マルウェア（ウィルス、ワーム、ボット等）の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。		○	マルウェア対策実施範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				2	D	システム全体		2	D	システム全体		2	D	システム全体	2	D	システム全体	本システムは紐付情報や資格情報、医療等IDなど、重要情報を扱うシステムであり、システム全体としてマルウェアの感染防止機能を確実に動作させる必要があると想定しているため、マルウェア対策実施範囲は中間サーバーと同様にレベル2を選択する。
33							リアルタイムスキャンの実施	実施しない	実施する					1	D	実施する		1	D	実施する		1	D	実施する	1	D	実施する	IPAの非機能要求グレードではウィルス定義ファイルの更新方法やタイミングについて検討することが必要とされており、常に最新の状態となるようにすることが望ましいとされている。マルウェアによる情報資産の不正取得、改ざんや消去などを防止するため、定期的なフルスキャンとともに、リアルタイムスキャンを実施することが推奨されることからレベル1を選択する。 リアルタイムスキャンの実施対象などの詳細は性能面も考慮の上、基本設計以降の設計フェーズにて確定させる。
34							フルスキャンの定期チェックタイミング	無し	不定期（フルスキャンを行えるタイミングがあれば実施する）	1回/月	1回/週	1回/日		3	D	1回/週		3	D	1回/週		3	D	1回/週	3	D	1回/週	リアルタイムスキャンのチェック時点では検出されなかったマルウェアに対して、最新のウィルス定義ファイルによるチェックを行うためには定期的なフルスキャンが必要となる。 オンライン資格確認システムはクローズドネットワークでの接続を前提としているため、最新のマルウェアの脅威にさらされるリスクは医療保険者等向け中間サーバー等と同等と考え、レベル3（フルスキャンは1回/週）を選択する。 フルスキャンの実施対象などの詳細は、基本設計以降の設計フェーズにて確定させる。
35		Web対策	Web実装対策	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。		○	セキュアコーディング、Webサーバーの設定等による対策の強化	無し	対策の強化					1	D	対策の強化		1	D	対策の強化		－	－	－	－	－	－	セキュリティパッチ等によるソフトウェアの脆弱性の修正は、オペレーティングシステムやミドルウェア等のソフトウェア製品だけでなく、本調達で設計・開発するソフトウェアについても考慮すること（脆弱性が生じないよう留意して設計・開発し、定期的な検査を通じた確認により修正を適用できるようにすること。）が求められると想定する。 サーバーが備える機能のうち、不要な機能を停止又は制限すること、公開してはならないWebコンテンツが公開されないように管理することなどの対策を実施することとし、レベル1を選択する。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ 本項目の対策はWeb/APサーバに対して行う想定のため、、端末は対象外とする。
36						○	WAFの導入の有無	無し	有り					1	B	有り		1	B	有り		0	D	無し	－	－	－	－	－	－	設計・開発するソフトウェアについてもセキュリティを考慮することは必須であり、業務アプリケーション側でのセキュアコーディング等により実現されることが必要であるが、新たに発見された脅威に対し、速やかに対応する必要がある場合、WAFの導入による対策が効果的となる。また、選定モデルの推奨値により、レベル1を選択する。 ■運用管理サブシステム■ 外部システムとの接続がないことから、WAF導入によるコストメリットも少ないと考えられるため、レベル0を選定する。 ■資格確認システム接続端末■ ■資格確認サービス機関等端末■ WAFはWeb/APサーバに導入する想定のため、端末は対象外とする。

【参考C-1】
非機能要件重点項目の整理結果

非機能要件の進め方

1 スケジュール

- 昨年11月に仮定義した非機能要求グレード表を、課題検討結果及び業務要件、機能要件の整理結果（経過）を踏まえて再定義する。また、そのうち調達仕様の要素となる要件項目について優先的に整理を行う。
- 機能要件整理と合同の検討会議の場で、要件の個別論点や補足資料を提示し、協議及び成果物のレビューを行う。



重点項目の検討について

1 概要

- 本資料で示す検討結果は以下のとおりである。
  なお、移行要件については別資料「【C-1-4】移行要件」にて説明する。

非機能重点項目の選定案（大項目のみ抜粋）

項番	大項目	要件整理検討会での経緯
1-1 ～ 1-5	信頼性要件/事業継続性要件	① 3/9 提示済み ② 3/23 一部追記　※サービス時間と業務処理量(CRL)
2-1 ～ 2-4	性能・拡張性要件	① 3/9 提示済み ② 3/16 提示済み ③ 3/23 一部追記　※レスポンスタイムに関すること
3-1 ～ 3-4	運用・保守要件	① 3/23 提示
4-1 ～ 4-5	移行要件	① 3/9 一部提示済み　※シリアル番号移行に関すること ② 3/23 一部提示　※医療機関、医療保険者移行に関すること ※説明は「【C-1-4】移行要件」を参照
5-1 ～ 5-6	情報セキュリティ要件	① 3/16 提示済み

本資料の構成、目次（本編）

１．信頼性要件/事業継続性要件

重点項目のうち、【信頼性要件/事業継続性要件（1-1～1-5）】に関する要求事項の整理結果とその理由を抜粋した説明資料

２．性能/拡張性要件

重点項目のうち、【性能/拡張性要件（2-1～2-4）】に関する整理結果とその理由を抜粋した説明資料

３．運用/保守要件

重点項目のうち、【運用/保守要件（3-1～3-5）】に関する整理結果とその理由を抜粋した説明資料

４．情報セキュリティ要件

重点項目のうち、【情報セキュリティ要件（5-1～5-6）】に関する整理結果とその理由を抜粋した説明資料

本資料の構成、目次（補足資料）

補足１．業務量試算に関する補足資料

性能/拡張性要件のうち、【規模要件(業務処理量)（2-1）】に関する補足説明資料

補足２．医療機関側レスポンスに関する補足資料

性能/拡張性要件のうち、【性能目標値／オンラインレスポンス（2-3）】に関する補足説明資料

１．信頼性要件/事業継続性要件

1．信頼性要件/事業継続性要件 重点項目

1 信頼性要件/事業継続性要件 重点項目　整理結果一覧

- 整理結果を以下に示す。
- 整理結果について、現時点の想定であるため、今後の検討結果により変更が発生する可能性がある。

項番	大項目	中項目	小項目	整理結果	理由
1-1	信頼性要件/事業継続性要件	システム稼働要件	運用スケジュール	本事業では、医療機関等向けサービス時間帯は制限を設ける（例：8時～21時（土日祝日含む））ことと仮定する（※１）。 資格確認用情報の更新（医療保険者等向け中間サーバー等との連携）は、医療機関等向けサービス時間帯を含め、終日実行可能とする（ただし、メンテナンスやバックアップの時間帯を除く）。	・【C-1-1】可用性要件　項番１を参照。

※１：医療機関等向けサービス時間帯は、本事業では一定の制限（8時～21時（土日祝日含む）と仮定するが、以下のとおり、相反する「利便性」と「コスト」の両側面から適正に判断し最終決定する必要がある。

	医療機関向けサービス時間帯を長時間化する場合のメリット／デメリット
利便性	◎ **医療機関等や患者(被保険者)にとって、より多くの利用ニーズに応えられる** ※医療機関等向けサービス時間帯を延ばすほど、休日診療や夜間診療、救急外来等でも利用の幅も広がる。
コストメリット	● **運用保守コスト、システム基盤コストが増大する** ※医療機関等向けサービス時間中の運用保守要員を維持する必要がある。 ※サービス停止中に行う処理（バックアップ等）を短時間で処理できる基盤が必要となる。
タイムラグ（資格確認用情報の鮮度）	– 変わらない ※医療機関等向けサービス時間帯でも、資格確認用情報の更新（中間サーバー等との連携）は技術的に可能

1．信頼性要件/事業継続性要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
1-2	信頼性要件/事業継続性要件	事業継続性	耐障害性	冗長性を確保したシステム構成とし、システム障害が発生した際には迅速かつ円滑な切り替えによって、業務機能の速やかな回復が可能とすること。障害が発生した片系から、正常稼働する片系のシステム機器における切り替え時間を「60分未満」とする。費用対効果を考慮し、過剰な冗長性を有することがないよう配慮すること。単一のハードウェア障害または故障部位の交換による業務機能への影響を局所化するため、ハードウェアの単一障害点をできる限り排除した構成とすること。受託者は、機器の仕様等により、除外することができない単一障害点が存在する場合には、それに対する対策や制約について検討すること。	・サーバーやネットワーク機器により冗長構成を構築し、円滑な切替を実現する。 ・切替時間については、【C-1-1】可用性要件 項番６を参照。 ・システム規模が小さくないため多数の機材を購入することから、費用対効果を意識する。 ・冗長化については、【C-1-1】可用性要件　項番12～23を参照。
1-3		可用性	稼働率	システムの稼働率は、サービス提供を行う合計時間（計画停止や災害による停止を除く）に対する、業務のすべてが稼働している合計時間の割合とする。医療機関等向けサービスの稼働率の目標は、99.99%とする。医療保険者等向け中間サーバー等との連携について、稼働率の目標は99.9%とする。	・稼働率は、【C-1-1】可用性要件 項番７を参照。

1．信頼性要件/事業継続性要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
1-4	信頼性要件/事業継続性要件	可用性	目標復旧水準（業務停止時）	システム障害が発生した場合の各システムの復旧目標は以下の通りとする。 ＜目標復旧時間＞ 12時間以内 ＜目標復旧地点＞ 1営業日前の時点 ＜目標復旧レベル＞ 全ての業務を復旧対象とする	・医療保険者等向け中間サーバー等と連携し、資格確認に必要なデータを収集するため、業務停止時からの復旧については、同システムの要件と合わせる。 ・【C-1-1】可用性要件 項番８～10を参照。
1-5		完全性	データ保護	医療保険者等向け中間サーバ等から連携し蓄積されたオンライン資格確認システム情報の搾取や漏えいを防止するため、保護すべき情報に対してアクセス制御を行うことに加えて、保存された情報及び情報にアクセスするための通信回線を暗号化する機能を備えること。 情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。	・医療保険者等向け中間サーバー等と連携し収集したデータのため、同システムと同様のデータ保護を必要とする。 ・【C-1-1】可用性要件 項番26を参照。
1-6		災害対策	システム復旧方針	大規模災害時のシステム復旧対策は不要とする。	・資格情報等の供給元である医療保険者等向け中間サーバー等が、左記方針で構築されているため。 ・堅牢なデータセンターを採用することにより災害時の倒壊はないとし、大規模災害時にもシステム復旧は不要と想定している。

2．性能/拡張性要件

2．性能/拡張性要件 重点項目

1 性能/拡張性要件 重点項目整理結果一覧

項番	大項目	中項目	小項目	整理結果	理由
2-1	性能/拡張性要件	規模要件(業務処理量)	通常時/ピーク時の業務量	資格確認に係る業務量を、以下に記す。 ■通常時 ①医療機関等からの資格確認要求 ・・・ 約500万件/日 ②医療保険者等向け中間サーバー等から連携する資格情報 ・・・ 約18.2万件/日 ③医療保険者等向け中間サーバー等から連携するシリアル情報 ・・・ 約16万件/日 ■ピーク時 ①医療機関等からの資格確認要求 ・・・ 約1,000件/秒 ②医療保険者等向け中間サーバー等から連携する資格情報 ・・・ 約529万件/日 ③医療保険者等向け中間サーバー等から連携するシリアル情報 ・・・ 約23万件/日	・通常時の業務量は、「補足１．業務量試算に関する補足資料　１　業務処理件数（平均）」を参照 ・ピーク時の業務量②と③は、「補足１．業務量試算に関する補足資料　２　業務処理件数（ピーク）」を参照 ・ピーク時の業務量①は、「補足１．業務量試算に関する補足資料　３～４　医療機関側業務トランザクション量の算出」を参照 ・ピーク時の業務量②について、「補足１．業務量試算に関する補足資料　５～７」参照

2．性能/拡張性要件 重点項目

1 性能/拡張性要件 重点項目整理結果一覧

項番	大項目	中項目	小項目	整理結果	理由
2-2	性能/拡張性要件	規模要件(業務処理量)	ピーク特性	①医療機関等からの資格確認要求 ・・・ 診療時間開始後１時間 ②医療保険者等向け中間サーバー等から連携する資格情報 ・・・ 証一斉更新（７月） ③医療保険者等向け中間サーバー等から連携するシリアル情報 ・・・ 特になし	・【C-1-2】性能・拡張性要件　項番6、7を参照。 ・②について、「補足１．業務量試算に関する補足資料　５～７」参照。
2-3		性能目標値	オンラインレスポンス	設計開発工程及びフェーズ１でのプロトタイプ運用期間中に性能評価（必要に応じて性能向上策）を実施し、その結果に基づいて定量的な性能要件を決定すること。	・「補足２．医療機関側レスポンスに関する補足資料」参照。
2-4		ﾘｿｰｽ拡張性	サーバー処理能力増強	本システムの利用の拡大に対して柔軟に対応できるように、方式設計指針案を当初に提示し、アーキテクチャを設計すること。また、必要に応じて機能や性能を拡張できる柔軟性を有したプログラム開発手法を採用すること。	・フェーズ１からフェーズ２への移行では、医療機関等からの要求が大幅に増加するため、スケールアウトを意識している。 ・【C-1-2】性能・拡張性要件　項番31、32を参照。

3. 運用/保守要件

3．運用・保守要件 重点項目

1 運用保守要件の整理

- オンライン資格確認サービスに係る運用・保守要件について、今後、設計・開発等を委託する事業者（以降「受託事業者」）に要求する内容を重点項目として整理する。
- なお、運用・保守要件については、業務要件をインプットとした非機能要件整理の中で要求事項が明確になるものもあるが、本調査研究事業において整理中の業務・機能要件との関連性が低いものも多いため、それらについては一般的に情報システムに求められるという観点で記載をしている。

2 受託事業者に関する想定

オンライン資格確認サービスの運用・保守は、関連する複数の運用・保守実施者によって遂行されるものと想定している。
そのため、受託事業者に対しては、以下のような役務作業を求めることが一般的であると考える。

- 次ページ以降に示すような運用・保守要件を踏まえた上で、必要に応じ適宜見直しを行い、運用・保守設計作業を実施すること。
- 基盤構築の実施者等と連携し、運用マニュアル／保守マニュアル等、必要なドキュメントを整理すること。
- 運用計画（案）／保守計画（案）を策定すること。
- 運用・保守実施者が円滑に運用・保守作業を実施できるよう、運用・保守に関する引継ぎを実施すること。

3．運用･保守要件 重点項目

3 運用･保守要件 重点項目　整理結果一覧

- 重点項目として整理した運用･保守要件について、以降に示す。

表１　運用･保守要件に関する重点項目（1）

項番	大項目	中項目	小項目	整理内容	理由
3-1	運用･保守要件	通常運用	運用時間	医療機関向けのオンラインサービス時間、医療保険者等向け中間サーバー等との連携にかかる運用スケジュール等を前提とすること。（具体的な時間については信頼性要件の重点項目1-1参照）	･信頼性要件 重点項目1-1にて定義した運用スケジュールに基づく。 ･【C-1-3】運用･保守性要件 項番1を参照。
			バックアップ	故障時において、信頼性要件にて定義した目標復旧水準（信頼性要件の重点項目1-4）を満たす復旧が可能となるよう、業務継続に必要となるデータを対象に自動バックアップ運用を行うこと。	･信頼性要件 重点項目1-4を満たすためのバックアップレベルが必要なため。 ･【C-1-3】運用･保守性要件 項番3～9を参照。
			運用監視	システムを構成するサーバー、ネットワーク機器や、アプリケーションプロセス、データベース等を対象に、システムの正常稼働を監視し、故障発生時に運用者が遅滞なくエラー検知できること。 また、サーバのCPU使用状況等、リソース監視を行うこと。	･信頼性要件 重点項目1-3で定義した稼働率を満たすためにも、システムの稼働監視は必須と考えられるため。 ･フェーズ2に向けたサイジングのためにもリソース監視は必要と考えられるため。 ･【C-1-3】運用･保守性要件 項番10～18を参照。

3．運用･保守要件 重点項目

3 運用･保守要件 重点項目　整理結果一覧

表１　運用･保守要件に関する重点項目（2）

項番	大項目	中項目	小項目	整理内容	理由
3-1	運用･保守要件	通常運用	時刻同期	システムを構成するサーバ、ネットワーク機器等について、外部標準時刻サーバ等との時刻同期を行うこと。	・本システムは外部システムとの接続も存在し、また、各機器の時刻整合性を保つことはセキュリティ観点上も重要なため。 ・【C-1-3】運用･保守性要件 項番19を参照。
3-2		保守運用	計画停止	システムメンテナンスや定期保守作業のために計画停止が必要な場合は年間計画にて策定し、原則として医療機関等向けオンラインサービス等の運用スケジュールに変更のない範囲で実施すること。（ただし、緊急時を除く）	・特に医療機関向けのオンラインサービスについて運用スケジュールの変更は影響が大きいため。 ・【C-1-3】運用･保守性要件 項番20～21を参照。
			運用負荷軽減	サーバーソフトウェア、端末ソフトウェア（資格確認サービス機関等端末）の更新作業等においては、一部の保守作業の自動化を検討し、運用負荷の軽減を図ること。	・システムを構成するサーバ等の機器数が相応に多いことが予想され、手動のみでの作業では運用負荷が高いため。 ・【C-1-3】運用･保守性要件 項番22～24を参照。
			パッチ適用ポリシー	保守実施者より定期的にパッチリリース情報を受領し、適用要否の判断／検証を実施した上で、原則として定期保守作業時にパッチ適用を行うこと。 具体的にはパッチ適用方針を策定した上で、パッチ適用運用を実施すること。	・【C-1-3】運用･保守性要件 項番25～28を参照。

3．運用・保守要件 重点項目

3 運用・保守要件 重点項目　整理結果一覧

表１　運用・保守要件に関する重点項目（3）

項番	大項目	中項目	小項目	整理内容	理由
3-3	運用・保守要件 運用・保守要件	障害時運用	復旧作業	業務停止を伴う障害が発生した場合、目標復旧時間内での復旧が可能となるよう、バックアップソフト等の復旧用製品を活用する等して復旧時間の短縮を図ること。	・信頼性要件 重点項目1-3、1-4にて定義した稼働率や目標復旧時間を満たす必要があるため。 ・【C-1-3】運用・保守性要件 項番33～38を参照。
			システム異常検知時の対応	システム異常検知時に、稼働率や目標復旧水準等を考慮した対応が可能となるよう保守実施者の対応時間帯や駆けつけ時間等を整理すること。	
3-4		運用環境	開発・テスト環境の設置	不具合対応や機能追加におけるシステム改修時に、運用環境へのリリース前に、テスト環境にて事前の動作確認テストを実施すること。	・運用開始後も継続的にシステム品質を維持するために必要なため。 ・【C-1-3】運用・保守性要件 項番41～42を参照。
			マニュアル準備レベル	通常運用及び保守運用のマニュアルを整備すること。	・【C-1-3】運用・保守性要件 項番43を参照。
			リモートオペレーション	遠隔地からのリモートでの監視や定型操作を可能とすること。	・システム機器を設置するデータセンターと、運用拠点とは別拠点となる可能性があるため。 ・【C-1-3】運用・保守性要件 項番44-45を参照。

3．運用･保守要件 重点項目

3 運用･保守要件 重点項目　整理結果一覧

表１　運用･保守要件に関する重点項目（4）

項番	大項目	中項目	小項目	整理内容	理由
3-5	運用･保守要件	保守要件	保守契約（ハードウェア）（ソフトウェア）	障害発生時に迅速な保守対応が可能となるよう、保守実施者に対する要件として、一元的な保守対応（マルチベンダサポート契約）を求めること。	・ハードウェア／ソフトウェアに関する保守について、迅速な保守サポートが必要となるため、一元的な保守窓口の設置を求める。 ・【C-1-3】運用･保守性要件 項番49～50を参照。
			メンテナンス作業役割分担	メンテナンス作業や故障時の一次対応について、ユーザ／保守実施者等の主体ごとの役割分担を明確にすること。	・メンテナンス作業や故障時の一次対応について、関連主体の意識齟齬がないよう、予め整理が必要なため。 ・【C-1-3】運用･保守性要件 項番52～53を参照。
			一次対応役割分担		
			導入サポート	システムテストは受託事業者が主体で実施することとなるが、関連する他の実施者の支援が必須のため、求めるサポート内容を明確にすること。 また、本稼働開始時の導入サポートについて、運用･保守実施者が特別に対応が必要な期間･内容を明確にすること。	・システム導入時において、円滑に運用開始できるよう、関連する他の実施者に対する具体的な要求事項を示す必要があるため。 ・【C-1-3】運用･保守性要件 項番58～59を参照。

４．情報セキュリティ要件

４．情報セキュリティ要件 重点項目

1 情報セキュリティ要件の検討方針

- 重点項目として選定した情報セキュリティ要件の各項目について、一般的な事例や中間サーバー等の設計を参考に説明内容を整理する。

項番	大項目	中項目	小項目	内容・キーワード
5-1	情報セキュリティ要件	権限管理	アクセス管理 アカウント管理	「データアクセス権」「アカウント設計」
5-2		システム管理・運用	システム管理・運用	「維持管理」
5-3		マルウェア対策	マルウェア対策	「マルウェア対策」
5-4		鍵管理	鍵管理	「暗号鍵管理」「ライフサイクル」
5-5		不正アクセス・内部不正対策	不正アクセス・内部不正対策	「不正追跡・監視」「不正検知」
5-6		その他	その他	「各種ガイドライン遵守」「仮想化に係る対策」「ネットワークにおける対策」「運用業者端末における対策」「設備管理に係る対策」

４．情報セキュリティ要件 重点項目

2 情報セキュリティ要件 重点項目　整理結果一覧

- 以下に整理結果を示します。
- 整理結果について、現時点の想定であるため、今後の検討結果により変更が発生する点はご了承下さい。

項番	大項目	中項目	小項目	整理結果	理由
1	情報セキュリティ要件	権限管理 不正アクセス・内部不正対策		以下に示す権限管理、アクセス制御及びアカウントの管理を行えるよう、機能の実装を行うこと。また、不正アクセス・内部不正対策を講じること。	・「業務一覧　資_03 オンライン資格確認サービスにおける利用者管理」の整理結果より。 ・「論点一覧 資_06 組織認証管理」の整理結果より。 ・【C-1-5】セキュリティ要件項番１３～17を参照。 ・取り扱う情報は重要情報であり、管理者権限を持つアカウントの乗っ取りによる情報漏洩などの脅威に対抗するため、認証は必須と考える。また、アカウント情報を適切に管理しセキュリティレベルの維持が求められると考えられるため。
1-1			アクセス管理 不正追跡・監視 不正検知	情報資産へのアクセスを許可された者のみに限定するため、利用する主体（職員、システム運用要員、医療機関等）を識別するための認証を行うこと。	
1-2				各種情報資産の格付け及び取扱制限等の管理ルールを策定し、利用者の職責に応じたアクセス制御・利用制限を行うこと。	
1-3				システム管理者権限をもつ主体の認証については、多要素認証を行う機能を持たせる等、厳格なアクセス制限を行うこと。	
1-4				管理者に対するアクセス制御を検討し、内部の要員によるデータ漏えいを防止する仕組みを実現すること。	
1-5			アカウント管理	主体のアクセス権を適切に管理するため、アカウント管理（登録、更新、停止、削除等）するための機能を備えること。	

４．情報セキュリティ要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
2	情報セキュリティ要件	システム管理・システム運用におけるセキュリティ対策	維持管理	以下に示すシステム管理・システム運用におけるセキュリティを確保できるよう、機能の実装を行うこと。	・【C-1-5】セキュリティ要件 項番10~12 項番13～17 項番19 項番21～26 項番29~34 を参照。 ・論点整理(資_06)より、オンライン資格確認システムは大多数の個人情報を取り扱うシステムであるため、システムへのアクセスログ等を証跡管理対象として収集・管理しておく必要があると考えている。 ・「政府機関の情報セキュリティ対策のための統一基準」では機密情報を取り扱う情報システムにおいて、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときには、当該機能を設けることが求められている。 また、セキュリティパッチの適用は情報システム全体への影響を考慮した上で、措置を講ずることが必要であるとされている。
2-1				システムを構成する機器を管理し、不正な機器の置き換えや不正なソフトのインストールによるセキュリティ侵害を防止できるようにすること。	
2-2				システムのバックアップに当たり、バックアップを実施する権限の管理やアクセス制御を行い、バックアップデータの漏えい時の被害を最小限にできること。	
2-3				サーバ機器への不正アクセス等による被害を予防する為、サーバへの不正アクセスの防止や万が一侵入された場合の検知・通知を行えるようにすること。	
2-4				調達の中で設計・開発するソフトウェアの緊急性の高いセキュリティパッチなどの適用を適宜正確かつ迅速に行うこと。 脆弱性が生じないよう留意して設計・開発し、定期的な検査を通じた確認により修正を適用できるようにすること。	

4．情報セキュリティ要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
3	情報セキュリティ要件	マルウェア対策 不正アクセス・内部不正対策	パターンファイル更新等 不正追跡・監視 不正検知	以下に示すマルウェア対策、不正アクセス・内部不正対策を講じること。	・【C-1-5】セキュリティ要件 項番29~34を参照。 ・本システムは紐付情報や資格情報、医療等IDなど、重要な情報を扱うシステムであり、システム全体としてマルウェアの感染防止機能を確実に動作させる他、内部不正による情報漏えい等に十分考慮する必要があると想定している。 また、上記のような重要度が高い資産を取り扱うシステム範囲において、感染した場合の通信遮断等の対策を講じる必要があると考えられるため。
3-1				アンチウィルスソフトウェア等の導入によりマルウェアへの対策を講じるための機能を備えること。	
3-2				外部ネットワークからのマルウェアの侵入や、万が一マルウェアに侵入された場合の外部ネットワークへの不正な通信等を監視し、侵入の検知、防止及び当該マルウェアによる外部通信の遮断等を行うこと。	
3-3				システムに保持される重要な情報資産やプログラム及びその設定ファイルに対し、マルウェアによる不正アクセス、改ざん、すり替え等の攻撃、内部不正に対する検知や防止を行えるよう、セキュリティ対策を施すこと。	
3-4				新たに発見されるマルウェアに対応するため、機能の更新が可能であること。	
3-5				システム全体としてマルウェアの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を管理できること。	

４．情報セキュリティ要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
4	情報セキュリティ要件	鍵管理		以下に示す暗号鍵管理を行うこと。	
4-1			暗号鍵管理	システム暗号鍵を用いる場合は、暗号鍵をソフトウェア等により保護・管理ができること。 ただし、本システムと連携する外部システムにおいて、ガイドライン等で管理方式が指定されている場合はこの限りではない。	・【C-1-5】セキュリティ要件 項番20を参照。 ・暗号鍵（秘密鍵）が万が一外部に漏えいした場合、オンライン資格確認システム全体の安全性や安定稼働に甚大な影響を及ぼすため、安全に保管しなければならない。 ここでは設備費用面（安価な策）を鑑み、ソフトウェアによって鍵ファイルを安全に管理すると仮定する。
4-2			ライフサイクル	暗号鍵の使用にあたり、生成、利用、廃棄などのライフサイクル管理と、鍵の使用におけるアクセス制御を行うこと。	

４．情報セキュリティ要件 重点項目

項番	大項目	中項目	小項目	整理結果	理由
5	情報セキュリティ要件	その他	各種ガイドライン遵守等	順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン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こと。	・【C-1-5】セキュリティ要件 項番１を参照。 ・調査研究事業においても、各種ガイドラインに準拠することが求められているため、今後行われる要件定義、設計・開発についても同様に準拠する必要があると考えるため。 ＜参考＞ ・政府機関の情報セキュリティ対策のための統一基準 ・厚生労働省情報セキュリティポリシー ・厚生労働省保有個人情報管理規定 ・医療情報システムの安全管理に関するガイドライン ・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（案）

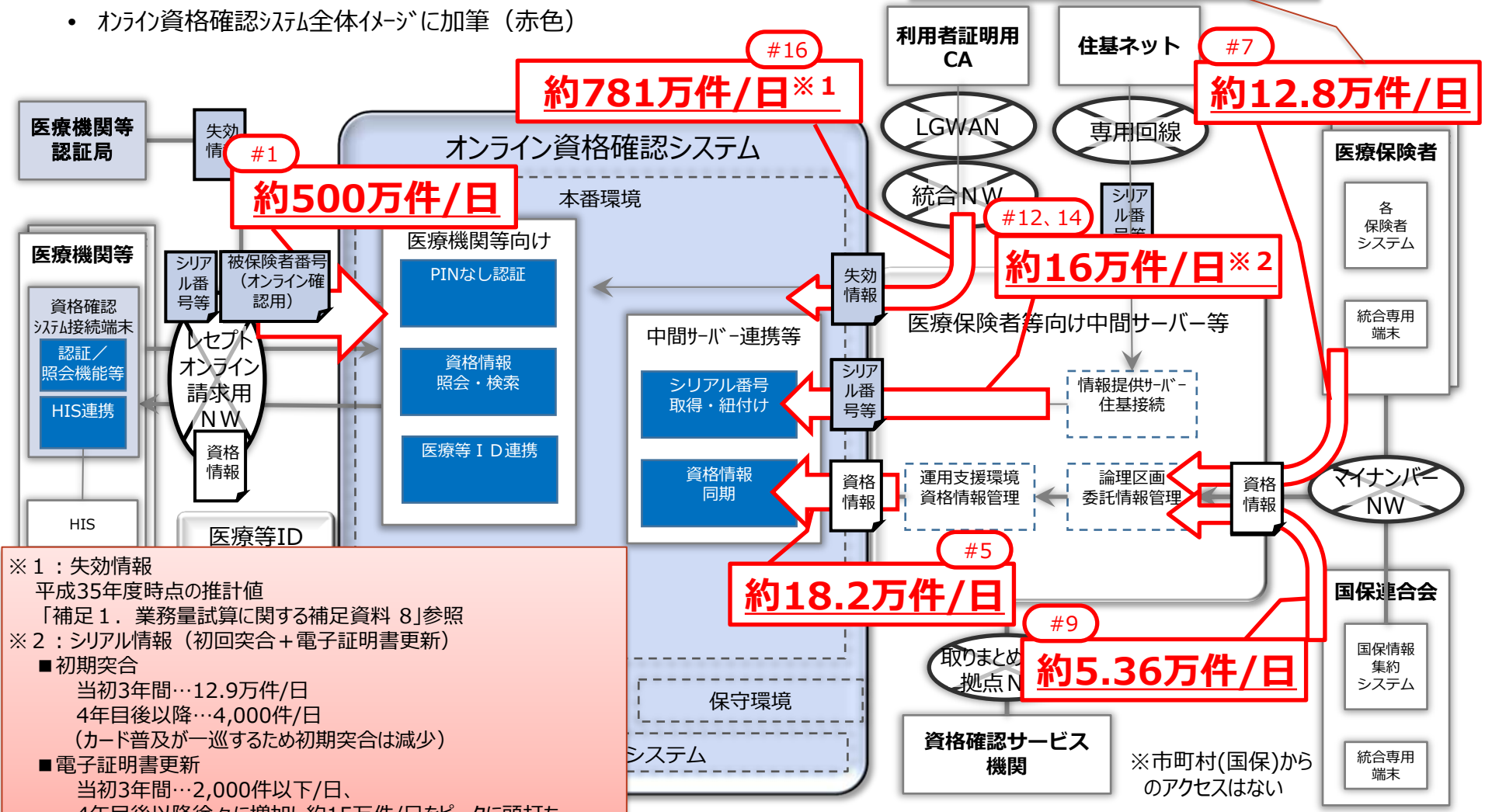
補足１．業務量試算に関する補足資料

補足１．業務量試算に関する補足資料

1 業務処理件数（平均）

- ｵﾝﾗｲﾝ資格確認ｼｽﾃﾑ全体ｲﾒｰｼﾞに加筆（赤色）

“**#7**”等は【A-5-1 別紙1】業務処理件数算出項目一覧の#を示す。算出根拠は同別紙を参照。



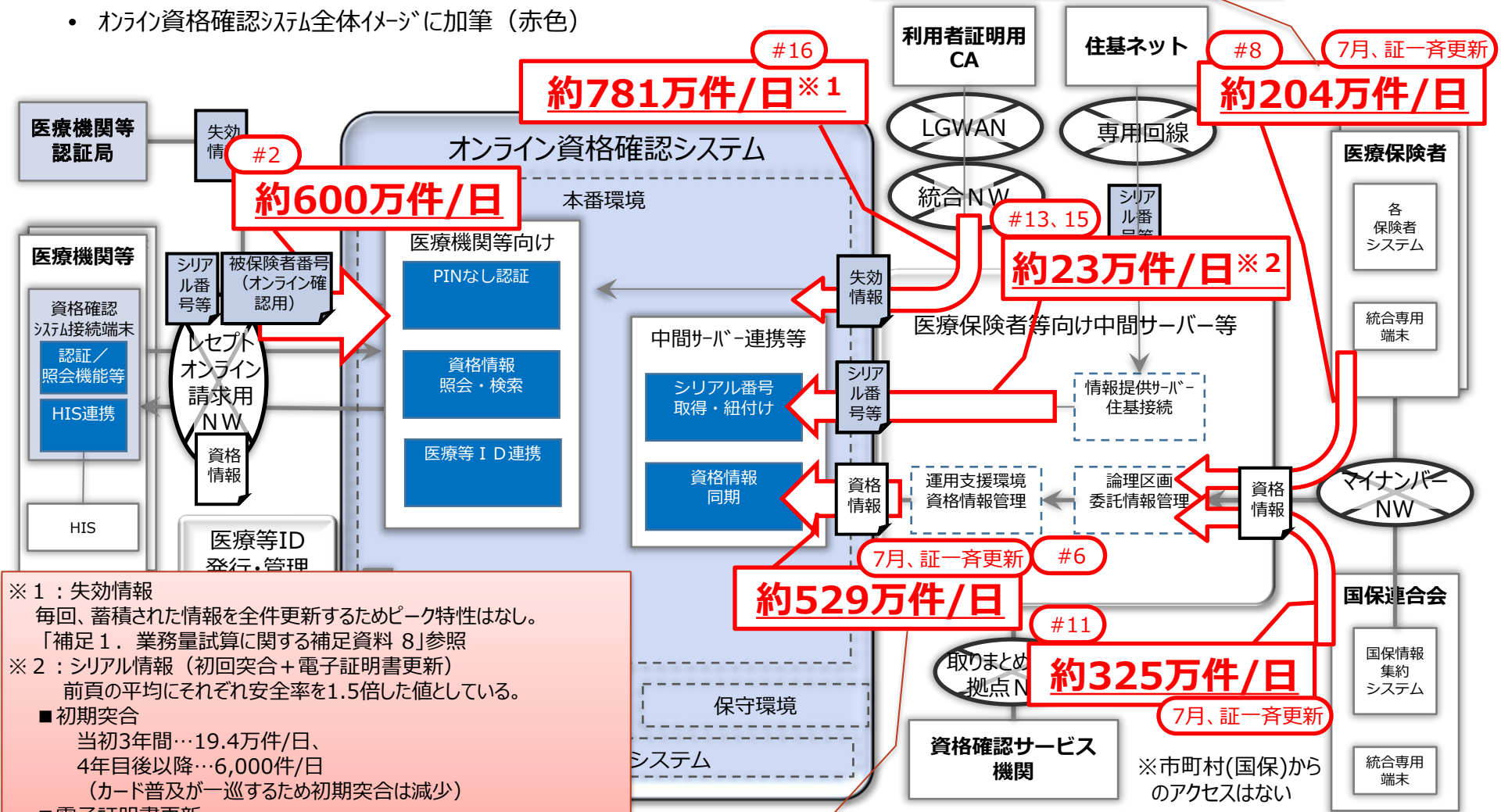
※１：失効情報
　平成35年度時点の推計値
　「補足１．業務量試算に関する補足資料 8」参照
※２：シリアル情報（初回突合＋電子証明書更新）
　■初期突合
　　当初3年間…12.9万件/日
　　4年目後以降…4,000件/日
　　（カード普及が一巡するため初期突合は減少）
　■電子証明書更新
　　当初3年間…2,000件以下/日、
　　4年目後以降徐々に増加し約15万件/日をピークに頭打ち。

補足１．業務量試算に関する補足資料

2 業務処理件数（ピーク）

- ｵﾝﾗｲﾝ資格確認ｼｽﾃﾑ全体ｲﾒｰｼﾞに加筆（赤色）

“#8” 等は、【A-5-1 別紙1】業務処理件数算出項目一覧の#を示す。算出根拠は同別紙を参照。



※１：失効情報
毎回、蓄積された情報を全件更新するためピーク特性はなし。
「補足１．業務量試算に関する補足資料 8」参照

※２：シリアル情報（初回突合＋電子証明書更新）
前頁の平均にそれぞれ安全率を1.5倍した値としている。
■初期突合
当初3年間…19.4万件/日、
4年目後以降…6,000件/日
（カード普及が一巡するため初期突合は減少）
■電子証明書更新
当初3年間…3,000件以下/日、
4年目後以降…22.4万件/日

「補足１．業務量試算に関する補足資料５～７」参照

補足１．業務量試算に関する補足資料

3 医療機関側業務トランザクション量の算出　（１）算出式と算出結果

- 医療機関側オンライン業務のトランザクション量のピークについて、診療開始後１時間に集中すると仮定すると、算出式は次のように考えられる。

医療機関側オンライン業務のトランザクション量（ピーク）
＝　（①業務処理件数（ピーク）（件/日）×　②診療開始後１時間の業務集中割合　）÷　3,600秒

- 各項の値は、以下の値とする。

項目	用いる数字	理由
①業務処理件数（ピーク）	約600万件/日	※【A-5-1 別紙1】業務処理件数算出項目一覧の#2を参照
②業務集中割合	0.54	次項「②業務集中割合の見積り」を参照

⇒ 600万件/日　×　⑧業務集中割合（0.54）÷　3,600秒
⇒ 900
　≒ **約1,000件/秒**

補足１．業務量試算に関する補足資料

4 医療機関側業務トランザクション量の算出　（２）②業務集中割合の見積り

- 各医療機関の業務を勘案し、最初の１時間（朝９時前後の１時間）の業務集中割合を医療機関種類毎に仮定し、業務量の加重平均を算出する。

- 各医療機関種別毎の特性に応じた、業務集中割合の考え方は以下のとおり。

  病院　　受付能力や再来受付機等を考慮し、最初の１時間に外来受付が集中すると想定し、80%と仮定
  診療所　　対面での資格確認が前提であるため、実態は受付待ちが生じるものと想定し、60%と仮定。
  歯科　　朝からの急な外来は多くなく、再来時も予約診療を行っているケースが多いと想定し、30%と仮定。
  調剤薬局　病院や診療所での診療後（処方せん発行後）に訪問するケースが多いと想定し、40%と仮定

- 算出方法は、以下のとおりとする。
  - 病院／診療所／歯科／調剤別オンライン請求件数内訳比率は、支払基金と国保連合会における実施比率が同一であると仮定し、支払基金の統計情報（基金年報）の値から算出する。

医療機関種類	病院	診療所	歯科	調剤
業務集中割合仮定	80%	60%	30%	40%
オンライン請求件数割合 ※1	17%	36%	3%	44%
割合積	0.14	0.22	0.01	0.18

⇒加重平均 **54%**

※１：　前スライド表のオンライン請求件数合計に対する各医療機関種類毎件数の割合

補足１．業務量試算に関する補足資料

5 資格情報の業務処理件数の算出　（１）業務処理件数（平均）

市町村国保以外

■協会けんぽ、健保組合、国保組合、広域連合の1日当たりの得喪の処理件数（想定）の算出

加入者情報管理情報　年間業務量（協会けんぽ、健保組合、国保組合、広域連合）　÷　年間業務日数　≒　116,957件/日　・・・・・①

28,069,767件/年
※医療保険者等向け中間サーバー等の設計書より

240日
※年間業務日数は240日と仮定

■共済組合の1日当たりの得喪の処理件数（想定）の算出

加入者情報管理情報年間業務量（健保組合）　×　加入者数補正　÷　年間業務日数　≒　11,073件/日　・・・・・②

8,858,279件/年
※医療保険者等向け中間サーバー等の設計書より

3/10
※共済組合の加入者数は、健保組合の3/10と仮定

240日
※年間業務日数は　240日と仮定

業務処理件数（平均）

＝　①　＋　②　＝　116,957件/日　＋　11,073件/日　≒　**128,030件/日**　・・・・・③

市町村国保

■市町村国保の1日当たりの得喪の処理件数（想定）の算出

市町村国保　年間業務量（被保険者増　＋　被保険者減）　÷　年間業務日数　≒　**53,600件/日**　・・・・・④

12,874,319件/年
※国民健康保険事業年報　平成26年度 保険者別データ 国民健康保険事業状況報告書（事業年報）Ａ表 より

240日
※年間業務日数は240日と仮定

「資格確認サービスで取り扱う資格情報の同期」の業務処理件数（平均）

業務処理件数（平均）

＝　③　＋　④　＝　128,030件/日　＋　53,600件/日　≒　**約182,000件/日**

補足１．業務量試算に関する補足資料

6 資格情報の業務処理件数の算出　（２）業務処理件数（ピーク）

- 年に一度、加入者全員分の被保険者証の「有効期限」（市町村国保、国保組合、後期高齢）と高齢者受給者証（後期高齢を除く）の「有効期限」が一斉更新される。
- 通常の加入者情報等の登録や更新に加え、７月に上記更新業務が10日間程度の期間に行われると仮定しており、この時期がピークであると想定している。

市町村国保以外

下記の被保険者証と高齢者受給者証の「有効期限」を、10日間で全て更新すると仮定する。

更新対象の証の合計枚数 被保険者証（国保組合、後期高齢） 高齢者受給者証（国保組合）	÷	更新 業務日数	≒	約190万件/日 ・・・・・⑤
約1,900万枚		10日		

上記に業務処理件数（平均）加えたものが、業務処理件数ピークとなる。

業務処理件数（ピーク）

＝ ③ ＋ ⑤ ＝ 約12.8万件/日 ＋ 約190万件/日 ≒ **約204万件/日** ・・・・・⑥

補足１．業務量試算に関する補足資料

6 資格情報の業務処理件数の算出　（２）業務処理件数（ピーク）　（続き）

市町村国保

下記の被保険者証と高齢者受給者証の「有効期限」を、10日間で全て更新すると仮定する。

更新対象の証の合計枚数 被保険者証（市町村国保）	÷	更新 業務日数	≒	約320万件/日 ・・・・・⑦
約3,200万枚		10日		

上記に業務処理件数（平均）加えたものが、業務処理件数ピークとなる。

業務処理件数（ピーク）

＝ ④ ＋ ⑦ ＝ 約5.36万件/日 ＋ 約320万件/日 ≒ **約325万件/日・・・・⑧**

「資格確認サービスで取り扱う資格情報の同期」の業務処理件数（ピーク）

業務処理件数（ピーク）

＝ ⑥ ＋ ⑧ ＝ 約204万件/日 ＋ 約325万件/日 ≒ **約529万件/日**

7 中間サーバー等区間連携　業務処理件数の増加

- 医療保険者等向け中間サーバー等「委託区画、運用支援環境および統一区画」の各区画間連携の業務処理件数は、オンライン資格確認対応後には現行の中間サーバー等より、増加する。

	現行中間サーバー等	オンライン資格確認対応後	備考
平均	約117,000（件/日）	約182,000（件/日）	現行中間サーバー等の値は、中間サーバー等の設計書から
ピーク時	約835,000（件/日）	約5,290,000（件/日）	現行中間サーバー等の値は、中間サーバー等の設計書から

- 業務処理件数（ピーク）の増加が大きいので、医療保険者等向け中間サーバー等のシステム基盤増強時は、既存システム基盤設計を精査することが必要である。

※「有効期限」切れの情報を保険者インターフェースへ追加するなど、証一斉更新時の保険者運用変更も業務量増加対応の一案である。

補足１．業務量試算に関する補足資料

8 利用者証明用CA連携に関する業務処理件数の算出　利用者証明用電子証明書の失効情報の取得件数

- 利用者証明用CAから失効情報（以下、CRL情報）を取得する業務処理において以下の２つの重要な要件がある。

  ① CRL情報は利用者証明用CAが消去しない限り、有効性確認を行う資格確認サービス機関側で消去できないため、**CRL情報はマイナンバーカードの普及に従い年を追う毎に日々増加する**。

  ② CRL情報は利用者証明用CAが**毎朝6時～7時にリポジトリを最新版に更新する**ため、資格確認サービス機関では、その後、医療機関等向け**資格確認サービスの開始時刻に間に合うようにCRL情報を取込まなくてはならない**。

- まず、CRL情報に登録される（または削除される）ケースを以下に整理する。
  - CRL情報は、紛失や盗難、本人の意向等による失効申請があった場合、死亡時、一時保留及び危殆化の疑いがある場合の再交付等の際に登録される。
  - 利用者証明用電子証明書の有効期間満了に伴う更新時は証明書は失効せず、CRL情報には登録されない。（有効期間に関しては、CRL情報の確認とは別に、有効期限切れのチェックを行うこととされている。）
  - 氏名や住所等の４情報を変更する際も、利用者証明用電子証明書は失効せず、CRL情報には登録されない。（券面記載情報の変更する際は、カード表面の「追記領域」に手書きしてカード自体は回収(交換)しないこととされている。また、利用者証明用電子証明書には４情報が記載されていないため失効しない。）
  - 有効期間満了日を過ぎた利用者証明用電子証明書のCRL情報は登録されない。（有効期間満了日を過ぎた時点で、当該証明書のCRL情報は順次削除されるものと考えられる。）

- その上で、想定されるマイナンバーカードの普及に伴い、CRL情報の件数の増加を次ページ以降に試算する。

参考：『新制度（個人番号制度）に関する技術仕様等（正式版）201507版』（2016/11/10受領）

補足１．業務量試算に関する補足資料

- ① CRL情報のデータ件数の増加の試算
  今後の設計要件の参考とするため、マイナンバーカードの普及に伴うデータ量を以下のとおり試算する。

(1) CRL情報が増減する各ケースについて、試算上の考え方（前提、パラメータ）を以下に整理する。

CRL情報の増減のケース		増減	次ページの試算での考え方
CRL情報に登録されるケース	紛失等による失効申請	増	普及枚数の**0.5%**が年間に失効申請される想定。 （運転免許証の再交付の割合が年間0.5%～1%であることから） 普及枚数 × 0.5%
	死亡による失効	増	総務省統計の平成28年の死亡者数130万人に対し、マイナンバーカードの普及率を乗じて算出する。 130万人 × （普及枚数 ÷ 1億3千万人）
	更新申請による失効	増	氏名や住所の変更では利用証明用電子証明書は更新されない。 更新申請は暗証番号の変更など稀なケースと考えられるので試算の考慮の対象外とする。
	交付前破棄や危殆化による失効や一次保留など	増	稀なケースであることと、発生数を予想できる事由ではないことから試算の考慮の対象外とする。
CRL情報に登録されないケース	電子証明書の有効期限切れによる更新	なし	電子証明書の有効期限切れにより旧電子証明書の失効情報は登録されないため対象外とする。
CRL情報から削除されるケース	CRL情報に登録された電子証明書の有効期限が満了した場合	減	CRL情報は有効期限を残している電子証明書が失効した場合に登録されるが、紛失や死亡による失効は電子証明書の有効期間をすべて（５年）を残して失効するとして試算する。

補足１．業務量試算に関する補足資料

(2) 試算結果

※ 人口は1億3千万人として試算。
※ マイナンバーカードの普及は、平成30年に6,000万枚、平成31年に8,700万枚とし、平成33年に13,000万枚に達すると仮定。

(単位：万件)

年度	普及枚数	失効情報の増加		失効情報の減少		CRL情報の件数（有効期限内の失効情報の累積件数）
		紛失等による失効件数	死亡による失効件数	有効期限の満了による消滅	備考	
～平成29年まで	3,000	22	44	0		**66**
平成30年	6,000	30	60	0		**156**
平成31年	8,700	43	87	0		**382**
平成32年	11,400	57	114	0		**286**
平成33年	13,000	65	130	0		**457**
平成34年	13,000	65	130	-21	平成28年以前の失効分はCRL情報から消去される	**631**
平成35年	13,000	65	130	-45	平成29年以前の失効分はCRL情報から消去される	**781**

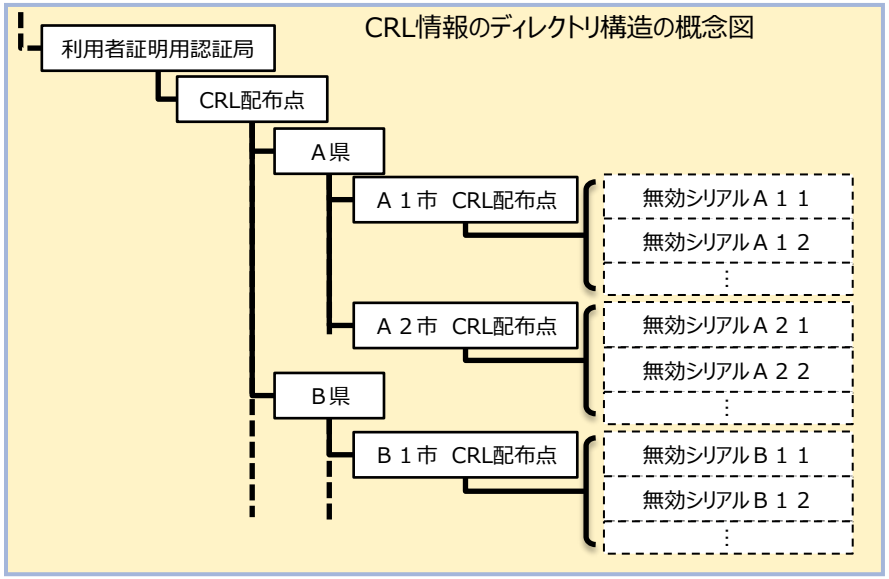
- マイナンバーカードの普及の過渡期では、**カードの普及に伴ってCRL情報の件数は増え続ける**と想定される。
- **マイナンバーカードの普及が安定する頃には、CRL情報の増加数も頭打ち**になる。
- **有効期間満了を迎える頃（平成34年以降）、徐々に過去のCRL情報が消去され累積件数も頭打ち**になる。

補足１．業務量試算に関する補足資料

- ② CRL情報の取得時間帯の制約について
  利用者証明用CAで、前日登録分の証明書失効情報を含むCRL情報が公開されるのは午前7時であるため、資格確認サービスのサービス開始時刻までに取得することを考慮すると時間的余裕は少ない。
  ここでは、今後の設計要件の参考とするため、利用者証明用CAからのCRL提供形態について以下に整理する。

  - CRL情報の提供に関する仕様
    - CRL情報の提供方法はLDAPv3によるディレクトリ構造からのリポジトリの抽出である。
    - 下図のように、都道府県、市区町村のディレクトリがあり、市区町村毎にCRL情報が格納されている。

➢ 全体
「CRL情報のルート」を指定すると、その下部構造（全国分）を全て取得できる。
➢ 都道府県
「A県」を指定すると、その下部のすべての市区町村分のCRL情報を取得できる。
➢ 市区町村
「B県」「B1市」を指定し、当該市区町村分のCRL情報を取得できる。



- 上記のとおり、地域（都道府県・市区町村）単位で抽出することは可能だが、オンライン資格確認においては全国分のCRL情報を必要とすることから、地域単位で抽出方法は有用ではない。
- 一方、期間指定の抽出ができないため、**毎回全件（過去も含めた全国分）を取得する必要がある**。

出典：『失効情報及び紐付け情報提供に関する仕様書　1．1 版　平成27年5月15日』

補足２．医療機関側レスポンスに関する補足資料

補足２．医療機関側レスポンスに関する補足資料

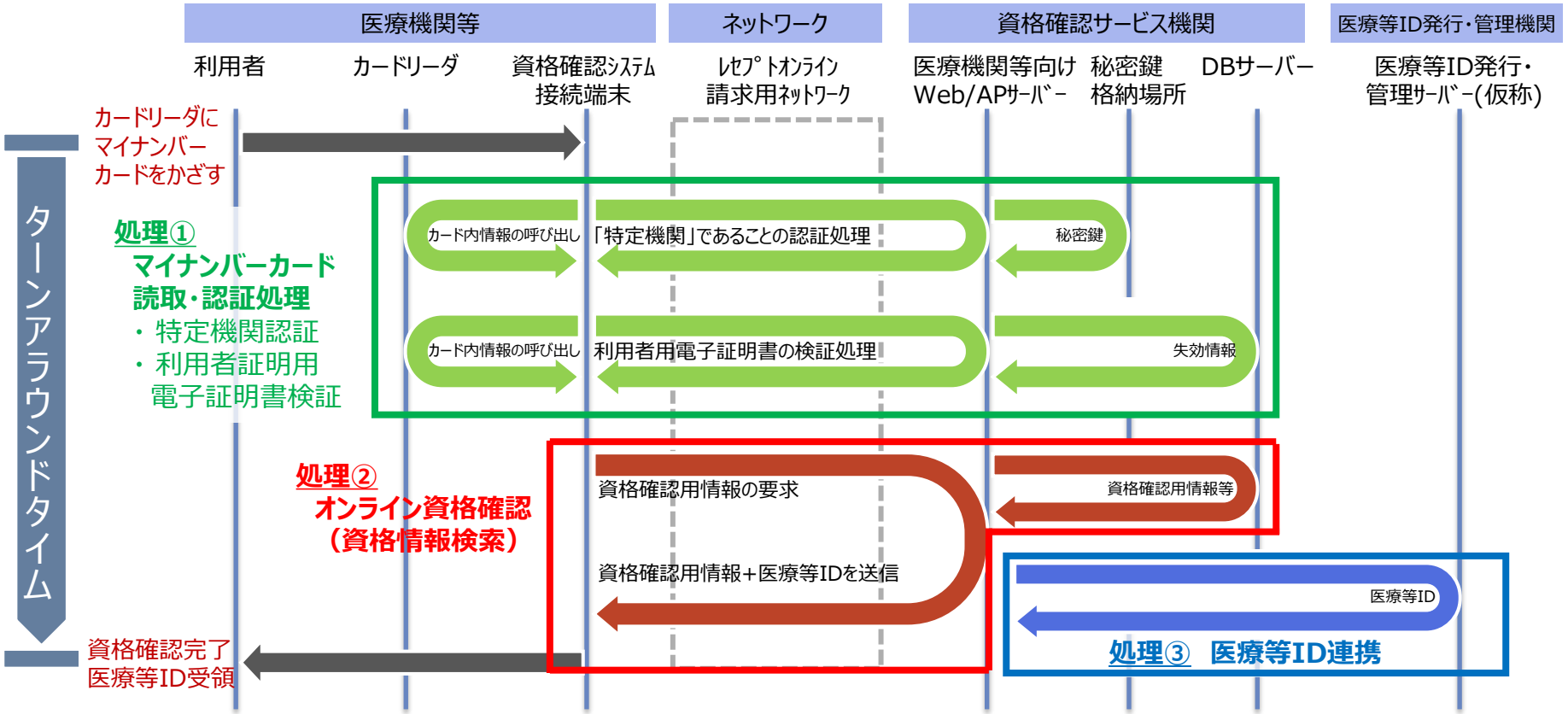
1 医療機関側のレスポンスタイム

- 医療機関側での業務要件を考慮するにあたり、患者が医療機関等窓口のカードリーダにマイナンバーカードを置いてから、端末に資格確認用情報（結果）が返されるまでに要する時間（ターンアラウンドタイム）は特に重要な要件である。
- 本調査研究では、上記ターンアラウンドタイムを、患者がその場で待つことのできる時間であることを前提に業務フローを検討してきたところ（業務要件に係る論点「医療_07」等）。
- しかしながら、現時点では定量的な性能要件（○秒以内）を決めるにあたって必要となる前提（端末、マイナンバーカードの読み取りアプリ、ネットワーク等）がそろっていない状況である。
- そこで、今後委託する設計開発事業者に対し、設計開発工程およびフェーズ１でのプロトタイプ運用期間中での性能評価（必要に応じて性能向上策）を要求し、その結果に基づいて定量的な性能要件を決定することが望ましいと考える。
- なお、本資料では、マイナンバーカードを使用したオンライン資格確認処理イメージを図解した上で、それぞれ性能を求められる構成要素ごとに、性能要件を決めるために必要な事項を整理する。

補足２．医療機関側レスポンスに関する補足資料

2 マイナンバーカードを使用したオンライン資格確認処理イメージ（簡略版・想定）

- 医療機関等窓口にて、マイナンバーカードをかざしてから資格確認結果および医療等IDを受領するまでの目標時間を「ターンアラウンドタイム」と定義する。このターンアラウンドタイムの間には、大別して下図の３つの処理が実行される。
  - **処理①　マイナンバーカード読取・認証処理**　※特定機関認証および利用者証明用電子証明書検証
  - **処理②　オンライン資格確認（資格情報検索）**　※検索結果には医療等IDも含む想定
  - **処理③　医療等ID連携**　※処理②中に実行されるバックグラウンド処理

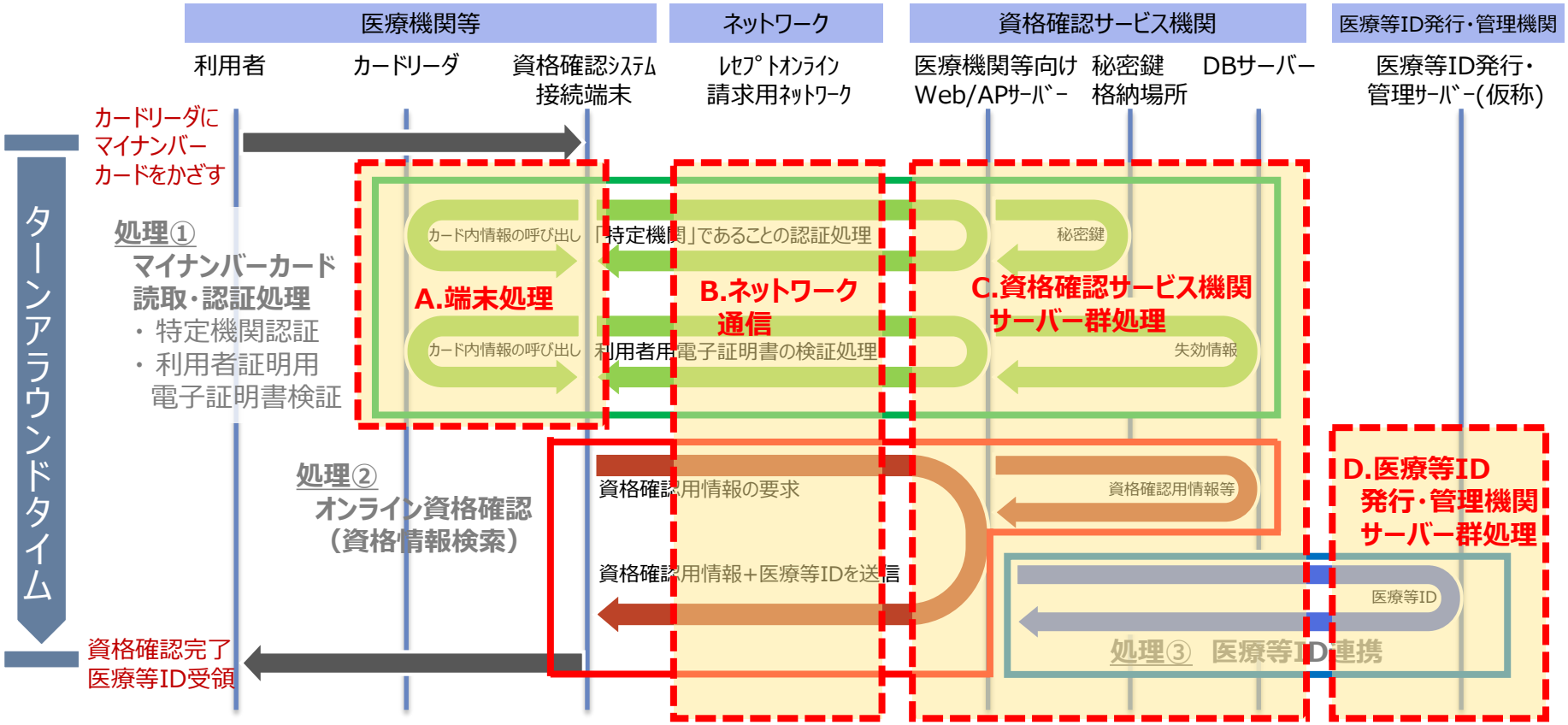


※上図は処理のイメージを図解したものであり、矢印の位置や長さ・大きさは、処理の正確な順序や処理時間の尺度を示すものではない。

補足２．医療機関側レスポンスに関する補足資料

3 ターンアラウンドタイムを決定する４つの構成要素

- また、ターンアラウンドタイムを決定する構成要素は、下図のとおり、【A.端末処理】、【B.ネットワーク通信】、【C.資格確認サービス機関のサーバー群処理】および【D.医療等ID発行・管理機関のサーバー群処理】の４つに分類できる。



※上図は処理のイメージを図解したものであり、矢印の位置や長さ・大きさは、処理の正確な順序や処理時間の尺度を示すものではない。

※ 資格確認サービス機関のサーバー群と医療等ID発行・管理機関のサーバー群との間は、ここでは物理的な乖離はない（同一のデータセンターに設置する）と仮定し、ネットワーク通信にかかる性能要件（遅延）は考慮していない。

補足２．医療機関側レスポンスに関する補足資料

4 各構成要素の性能要件（レスポンスタイム）を定めるために必要なこと

- 前述のとおり、定量的なレスポンスタイムは設計開発工程以降に性能評価した上で決定する必要があるが、設計開発委託事業を調達するにあたり、対象となる処理のレスポンスタイムの目標値（目安）を仮定する必要がある。
- 各業務処理ごとのレスポンスタイムについて留意点を以下に示す。

■ 処理① マイナンバーカード読取・認証処理（A.端末 ⇔ C.資格確認サービス機関のサーバー群）

- サーバーだけでなく、医療機関等で使用する資格確認システム接続端末にも、マイナンバーカード内の情報を読み取って特定機関認証処理および利用者証明用電子証明書検証処理を行うためのカードアプリケーションの実装が必要である。
- 設計開発委託業務を調達するにあたって端末処理のレスポンスタイムの目標値を定める必要があるが、そのカードアプリケーションは今後利用者証明用CAから開示される仕様に基づいて開発する必要があることから、現時点（本調査研究事業）においては定量的な数値の定義が困難である。

■ B.ネットワーク通信のレスポンス

- フェーズ１では現行レセプトオンライン請求用ネットワークを活用する前提であるが、医療機関側の回線契約によって接続形態や帯域等が様々であり、資格確認サービス機関として（設計開発の調達要件として）レスポンスタイム要件を、網羅的かつ画一的に定義することができない。
- 実際にレセプトオンライン請求用ネットワーク通信にかかる時間のある程度の目安を計るためには、フェーズ１でのプロトタイプ運用時にかかる時間やトラフィック量を計測し、求められるネットワーク帯域の試算を行う必要がある。この際、ネットワーク通信量がピークになると想定されるレセプト請求期間（毎月上旬）での実測も（現業の請求業務に支障がないよう十分配慮した上で）時間を計測することが望ましい。

補足２．医療機関側レスポンスに関する補足資料

4 各構成要素の性能要件（レスポンスタイム）を定めるために必要なこと

■ 処理② オンライン資格確認（A.端末 ⇔ C.資格確認サービス機関のサーバー群）

- 定量的なレスポンスタイムを定義するためには、設計開発工程以降に方式設計を確定させ、性能測定を行った上で医療機関等向けWeb/APサーバー、秘密鍵格納場所（HSMを導入する場合）およびDBサーバーそれぞれの性能設計（サイジング）を行う必要がある。
- 一方、設計開発委託業務を調達するための目標値は、医療保険者等向け中間サーバー等ソフトウェア設計・開発等業務調達（後述）を参考に、”現時点での想定であり、今後の検討結果により変更が発生し得る”と留保しつつ、外部環境に依存する処理時間を除いた資格確認サービス機関のサーバー群内の処理時間の要件を仮定することが考えられる。本調査研究では、患者がその場で待つことのできる時間であることを前提に業務フローを検討してきたことを考慮すると、資格確認サービス機関のサーバー群内の処理時間の要件を「１秒以内」と仮定する。

※ 参考：以下に、資格確認サービス機関のサーバー群内の性能設計上の留意点を挙げる。

- 医療機関等向けWeb/APサーバーは、全国の医療機関からの要求を受けて並列処理しなければならないため、負荷分散装置（ロードバランサ）によって複数台のサーバーに分散処理する方式が必要である。また、将来的な処理の増加に耐えうるよう、必要に応じて分散処理性能をスケールアウトできる構成としておくことが望ましい。
- DBサーバーにかかる性能要件は、ハードウェアスペック（メモリやCPU）やデータベースのクラスタ化等により性能や拡張性を向上することに加え、アプリケーション設計開発においても処理性能を意識した設計（データベースに対する処理(SQL等)設計やテーブルレイアウト設計等）が重要である。
- 医療機関から一定の時間帯（月曜日の朝、開業後まもなく）にピークが想定されることから、平常時のレスポンスタイムだけでなく、ピーク時での順守率（性能劣化の許容範囲）を定めることも重要である。設計開発の委託事業者には、想定ピーク量に応じた性能検証（ラッシュテスト）の実施を要求することが望ましい。

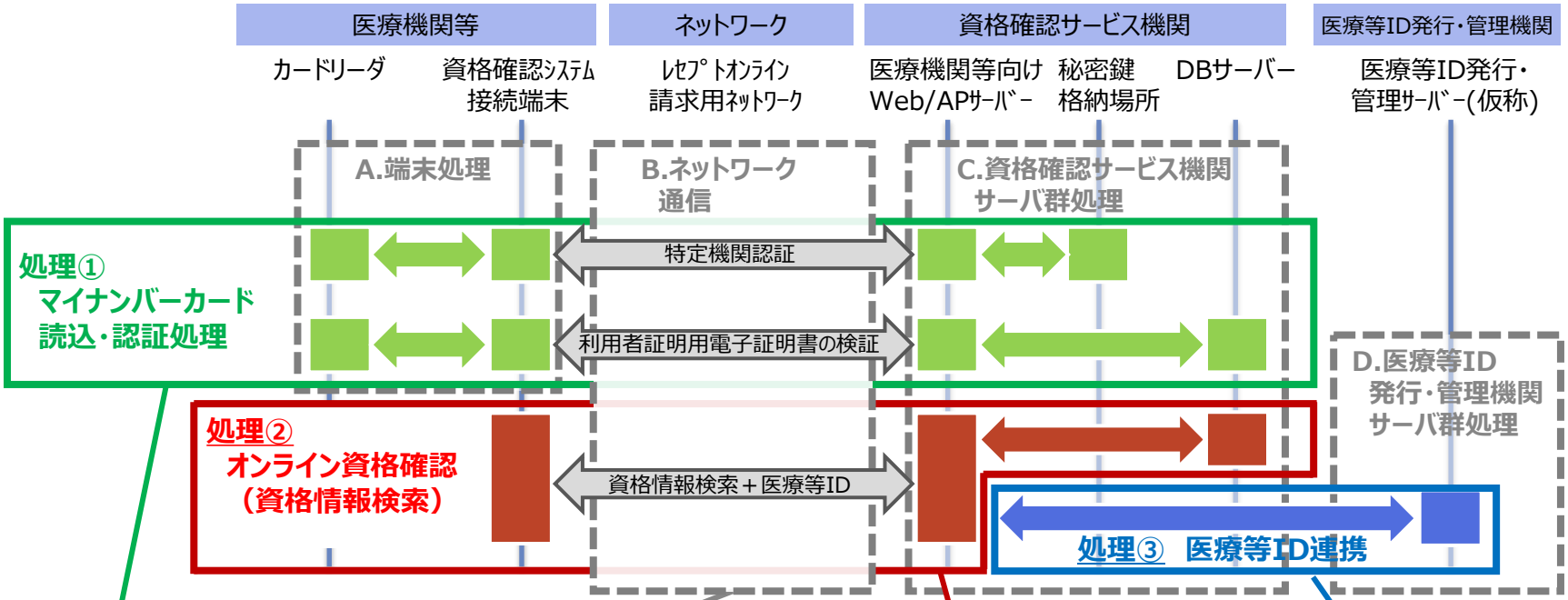
■ 処理③ 医療等ID連携（C.資格確認サービス機関サーバー群 ⇔ D.医療等ID発行・管理機関サーバー群）

- ここでは、上記処理①で仮定した処理時間要件（1秒以内）には医療等ID発行等の処理時間を含んでいないが、医療等ID連携を含めても患者がその場で待つことのできる時間を考慮すると、医療等ID発行・管理機関サーバー群の処理は、上記処理①の処理時間要件に著しく影響を及ぼさないようなレスポンス要件が求められる。

補足２．医療機関側レスポンスに関する補足資料

4 各構成要素の性能要件（レスポンスタイム）を定めるために必要なこと

- 前述の内容を下図に整理する。



処理① マイナンバーカード読込・認証
- 端末にマイナンバーカード内情報を扱うカードアプリケーションの実装が必要。
- そのカードアプリケーションは今後利用者証明用CAから開示される仕様に基づいて開発する必要があり、現時点においては定量的な数値の定義が困難である。

B. ネットワーク通信
- ﾚｾﾌﾟﾄｵﾝﾗｲﾝ請求用ネットワークは医療機関側の回線契約によって接続形態や帯域等が様々であるため、資格確認サービス機関として網羅的かつ画一的に定義することができない。
- 通信時間の目安を計るためには、フェーズ１において実回線を使って計測し、試算を行う必要がある。

処理② オンライン資格確認
- 定量目標は、設計開発工程以降に方式設計を確定し、性能測定を行った上で決定する必要がある。
- 現時点での想定では、今後の検討結果により変更が発生し得る点に留保しつつ、患者がその場で待つことのできる時間を考慮して「１秒以内」と仮定する。

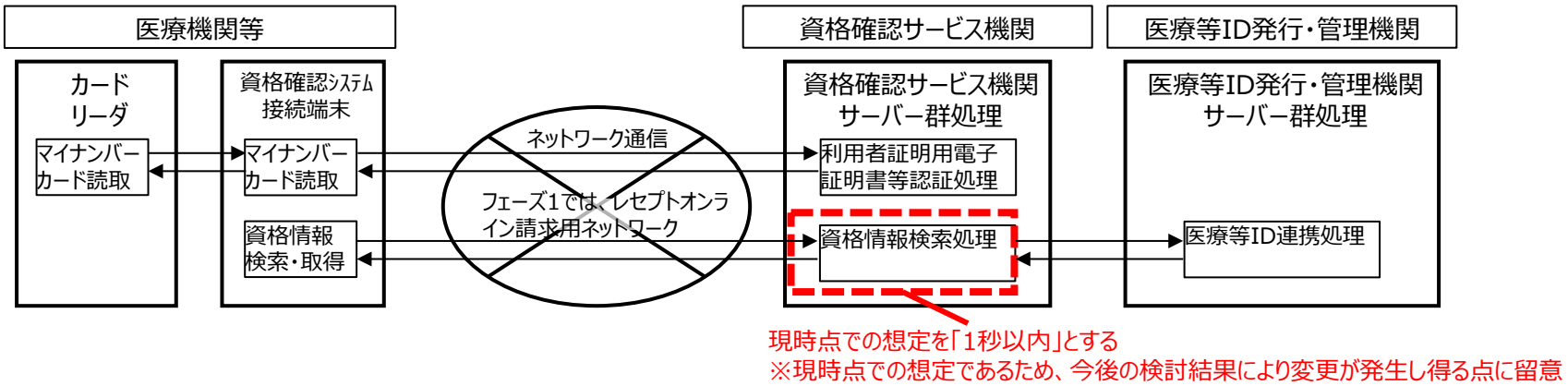
処理③ 医療等ID連携
- 医療等ID発行等の連携を含めても、患者がその場で待つことのできる時間を前提としている。
- そのため、医療等ID発行等処理には、左記に仮定した「１秒以内」に著しく影響を及ぼさないようなレスポンス要件が求められる。

補足２．医療機関側レスポンスに関する補足資料

5 資格確認サービス機関としての処理時間要件（まとめ）

以上の内容を踏まえ、資格確認サービス機関として求められる処理時間の要件を以下に整理する。

- 医療機関等窓口にて、マイナンバーカードをかざしてから資格確認結果および医療等IDを受領するまでの目標時間を「ターンアラウンドタイム」と定義する。このターンアラウンドタイムの間には、大別して以下の処理が実行される。
  - ① マイナンバーカード読取・認証処理
  - ② 資格情報検索処理
  - ③ 医療等ID連携処理（資格確認サービス機関と医療等ID発行・管理機関間）
  - ④ 医療機関等と資格確認サービス機関間のネットワーク通信
- そのうち、マイナンバーカード読取・認証処理（①）に関しては、今後利用者証明用CAから開示される仕様に基づいて開発する必要があることから、現時点においては定量的な数値の定義が困難である。
- 資格情報検索処理（②）に関しては、外的環境に依存する処理（資格確認サービス機関と医療等ID発行・管理機関間の医療等ID連携処理（③）及び医療機関等と資格確認サービス機関間のネットワーク通信※注釈（④））を除いた資格確認サービス機関サーバー群の処理時間の要件として、現時点での想定を「1秒以内」とする。ただし、現時点での想定であるため、今後の検討結果により変更が発生し得る点に留意すること。



※注釈：フェーズ１ではレセプトオンライン請求用ネットワーク活用を想定。医療機関等によって回線契約の形態や帯域等が様々であるため、その処理時間は資格確認サービス機関として網羅的かつ画一的に定義することができない。

補足２．医療機関側レスポンスに関する補足資料

6 【参考】医療保険者等向け中間サーバー等ソフトウェア設計・開発等業務における性能要件(例)

4.2 性能要件

医療保険者等向け中間サーバー等が備えるべき性能要件は以下のとおりである。

4.2.1 レスポンスタイム

医療保険者等向け中間サーバー等の性能要件として定めるレスポンスタイムは、要件定義の段階で、業務要件や業務量等を踏まえ決定し、当省の承認を得ること。

性能要件に関して、受託者に対し、データ量及びトランザクション数に関する参考資料の閲覧を希望する場合には、別途当省が定める手続を行った上で提示することとする。

(1) オンライン処理性能

オンライン処理に係るターンアラウンドタイムのうち、外部環境に依存する処理時間を除いた医療保険者等向け中間サーバー等機能群内の処理時間の要件として、現時点での想定を「表 4-5 想定レスポンスタイム」に示す。

オンライン処理性能にはネットワークを通じてのデータ送受信だけではなく、データベース等への情報提供記録の書き込み等の更新処理性能も考慮すること。

表 4-5 想定レスポンスタイム

項番	システム	レスポンスタイム
1	医療保険者等向け中間サーバー等	1秒以内

※上記は現時点の想定であるため、今後の検討結果により変更が発生し得る点に留意すること。

なお、レスポンス遵守率の性能目標値については、「表 4-6 システム基盤の非機能要求に関するグレード表による性能目標値」のとおりとし、これらの処理性能を満たすハードウェア等のサイジングを行うこと。なお、過剰なサイジングを必要としないように、方式設計指針案を当省に提示し、アプリケーション設計、データベース設計等を実施すること。

表 4-6 システム基盤の非機能要求に関するグレード表[1]による性能目標値

（オンラインレスポンス）［網掛け箇所が本システムの性能目標値］

指標	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5
通常時レスポンス遵守率	遵守率を定めない	60%	80%	90%	95%	99%以上
ピーク時レスポンス遵守率	遵守率を定めない	60%	80%	90%	95%	99%以上
縮退時レスポンス遵守率	縮退をしない	60%	80%	90%	95%	99%以上

※上記は現時点の想定であるため、今後の検討結果により変更が発生し得る点に留意すること。

なお、医療保険者等向け中間サーバー等を経由した情報照会・情報提供における処理時間のイメージを図 4-1 中間サーバー等の処理時間のイメージ図」に示す。

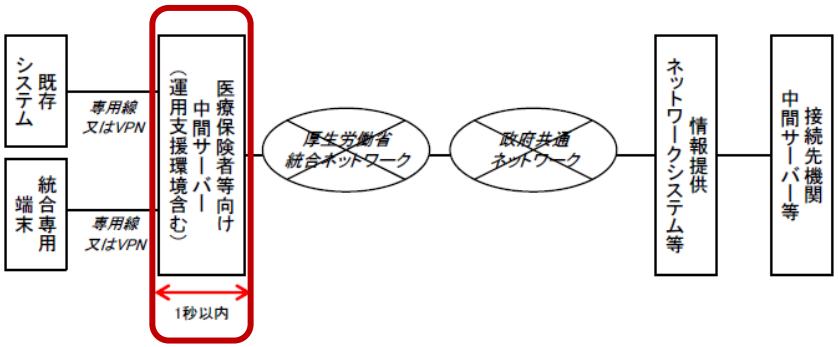


図 4-1 中間サーバー等の処理時間のイメージ図

出典：医療保険者等向け中間サーバー等ソフトウェア設計・開発等業務 調達仕様書（平成27年3月・厚生労働省政策統括官付情報政策担当参事官室）
http://www.mhlw.go.jp/sinsei/chotatu/chotatu/kankeibunsho/20150331-2/index.html