地方公共団体情報システム
非機能要件の標準について

令和４年８月

デジタル庁

デジタル社会共通機能グループ

地方業務システム基盤チーム

非機能要件の標準の位置づけ

○　地方公共団体情報システムの標準化に関する法律（以下「標準化法」という。）第７条に基づき、デジタル庁・及び総務省は、いわゆる非機能要件（サイバーセキュリティに係る事項その他の各地方公共団体情報システムに共通する事項）について標準化のため必要な基準を定めなければならないとされている。

○　非機能要件の標準は、デジタル庁及び総務省が令和２年９月に全国意見照会を経て、策定・公表している。

【地方公共団体情報システムの標準化に関する法律（令和３年法律第４０号）（抄）】

第五条　（略）
２　基本方針には、次に掲げる事項を定めるものとする。
　一・二　略
　三　各地方公共団体情報システムに共通する基準を定めるべき次に掲げる事項に関する基本的な事項
　　イ　電磁的記録において用いられる用語及び符号の相互運用性の確保その他の地方公共団体情報システムに係る互換性の確保に係る事項
　　ロ　サイバーセキュリティに係る事項
　　ハ　クラウド・コンピューティング・サービス関連技術を活用した地方公共団体情報システムの利用に係る事項
　　ニ　イからハまでに掲げるもののほか、各地方公共団体情報システムに共通する基準を定めるべき事項
（後略）

第七条　内閣総理大臣及び総務大臣は、第五条第二項第三号イからニまでに掲げる事項について、デジタル庁令・総務省令で、地方公共団体情報システムの標準化のため必要な基準を定めなければならない。
２・３　（略）

（標準化基準に適合する地方公共団体情報システムの利用）
第八条　地方公共団体情報システムは、標準化基準に適合するものでなければならない。
２　（略）

非機能要件の標準の内容

○ 「非機能要件の標準」は、「非機能要求グレード（地方公共団体版）」（平成26年3月・JLIS作成（※））において、業務・システムの分類「グループ②」として示された要求グレードのうち、クラウド調達時の扱いが「○：クラウドの対象と成り得る項目」とされている項目を中心に、必要と考えられる項目の「選択レベル」を基準として、最新の状況等を鑑み修正・追加をしたもの。

※JLISが、IPAが作成した「非機能要求グレード2013年4月版」を基に、地方公共団体が業務システムを調達する際に、業務システムに共通する非機能要件として一部を改変したもの。

○ 具体的には、基幹業務システムの可用性、性能・拡張性、運用・保守性、移行性、セキュリティ、システム環境・エコロジーに係る、機能要件以外の要件について規定している。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと
										－	*	0	1	2	3	4	5	
A.3.1.1	可用性	災害対策	復旧方針	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代替の機器として、どこに何が必要かを決める。	○	P48	2	同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [+]コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	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		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化の構成は省く など）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。 DR（Disaster Recovery）サイトとは、災害などで業務の続行が不可能になった際に、緊急の代替拠点として使用する施設や設備のこと。
A.3.2.1	可用性	災害対策	保管場所分散度（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。	○		2	1ヶ所（遠隔地）	遠隔地1ヶ所 [+]コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（近隣の別な建物と遠隔地）	2ヶ所（遠隔地）		【注意事項】 ここで遠隔地とは、主系サーバ等の設置場所と同時被災の恐れがない遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。 A.3.2.2（保管方法（外部保管データ））と合わせて考慮し、整合するようにレベルを選択すること。
A.3.2.2	可用性	災害対策	保管方法（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ための方法。	○	P49	2	ネットワーク経由でストレージへのリモートバックアップを含む	A.3.2.1と同じ拠点へのリモートバックアップを想定。 [−]媒体での外部保管のみによる運用を許容できる場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	媒体による外部保管のみ	ネットワーク経由でストレージへのリモートバックアップを含む				【注意事項】 A.3.2.1（保管場所分散度（外部保管データ））と合わせて考慮し、整合するようにレベルを選択すること。

非機能要件の標準の拡充等の観点

○ 「非機能要件の標準」は、デジタル社会の実現に向けた重点計画（令和４年６月７日閣議決定）に基づき、先行事業での検証結果を踏まえて、必要な拡充等を行うこととしている。

○ ガバメントクラウド先行事業において、現行の非機能要件の標準をガバメントクラウド上に構築する基幹業務システムにおいて満たせるかについて検証を進めているところであり、現時点までの検証過程において、

・各要件の検証計画を立てる際に要件の解釈に疑義が生じた点

・ガバメントクラウドの特性を踏まえ、選択レベル・条件を変更すべき点

等について、先行事業参加団体・事業者からの意見を踏まえ、要件を見直した。併せて、地方公共団体における情報セキュリティポリシーに関するガイドラインの改定の検討状況も踏まえ、選択レベル等を見直すとともに、意見照会で自治体等から寄せられた質問・意見等も勘案した。

【デジタル社会の実現に向けた重点計画（令和４年６月７日閣議決定）（抄）】

② 非機能要件の拡充

標準非機能要件（セキュリティを含む。）については、先行事業での検証を踏まえて、令和４年（2022 年）夏を目途に、必要に応じて拡充する。

非機能要件の標準の拡充等の観点

○ 活用シートにおける「選択時の条件」において、

・[－]は、選択レベルを下げる場合の条件

・[＋]は、選択レベルを上げる場合の条件

を記載している。

従来の活用シートでは、[－]、[＋]ともに選択レベルを１つ上げる（または下げる）場合の条件としていましたが、２つ以上上げる（または下げる）ことも可能としました。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		選択時の条件	レベル								備考「利用ガイド」第4章も参照のこと
										－	＊	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データによりシステムのデータが復旧可能かどうか確認するための項目。 外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○		2	システムの復旧に外部データを利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [－] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらから抽出したデータによって情報システムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	外部データによりシステムの全データが復旧可能	外部データによりシステムの一部のデータが復旧可能	システムの復旧に外部データを利用できない				【注意事項】 外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。
C.2.3.5	運用・保守性	保守運用	OS等パッチ適用タイミング	OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、サーバー及び端末のOS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは即時に適用する。	○	P29	4	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [－]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	緊急性の高いパッチのみ即時に適用し、それ以外は障害対応時等適切なタイミングで適用を行う	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチがリリースされるたびに適用を行う	【注意事項】 リリースされるパッチの種類（個別パッチ／集合パッチ）によって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E4.3.4）。 また、マイナンバー利用事務系のOSについては最新のパッチを速やかに適用すること。 なお、事前検証なくパッチを適用しなければならないというわけではない。

[－]は、選択レベルを~~1つ~~下げる場合の条件

[＋]は、選択レベルを~~1つ~~上げる場合の条件を記載している。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.1.2.2	外部データの利用可否	（選択時の条件） [-] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	（選択時の条件） [-] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらから抽出したデータによって情報システムを復旧できるような場合	明確化のため。
C.2.3.5	OS等パッチ適用タイミング	（メトリクス説明） OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは即座に適用する。 （レベル） レベル3：緊急性の高いパッチのみ即時に適用を行う （備考） 【注意事項】 リリースされるパッチの種類（個別パッチ／集合パッチ）よって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E.4.3.4）。 なお、「即時」と記載しているが、事前検証なくパッチを適用しなければならないというわけではない。	（メトリクス説明） OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、サーバー及び端末のOS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは即時に適用する。 （レベル） レベル3：緊急性の高いパッチのみ即時に適用し、それ以外は障害対応時等適切なタイミングで適用を行う （備考） 【注意事項】 リリースされるパッチの種類（個別パッチ／集合パッチ）によって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E.4.3.4）。 また、マイナンバー利用事務系のOSについては最新のパッチを速やかに適用すること。 なお、事前検証なくパッチを適用しなければならないというわけではない。	明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
E.4.3.4	ウィルス定義ファイル適用タイミング	（備考）	（備考） 【注意事項】 事前検証なく定義ファイルを適用しなければならないというわけではない。 最新のウィルス定義ファイル適用時に、ウィルス検索エンジンのアップデートも検討すること。	ウィルス定義ファイルの適用タイミングにおける注意事項を追記。
E.5.1.1	管理権限を持つ主体の認証	（メトリクス説明） （略） 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カード認証、生態認証等がある。 （選択レベル） レベル1：1回 （選択時の条件） 攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [＋] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合 （備考） 【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。	（メトリクス説明） （略） 複数回、異なる方式による認証を実施することにより、不正アクセスに対する抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。 （選択レベル） レベル3：複数回、異なる方式による認証 （選択時の条件） 攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 （備考） 【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。 認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。 機器等（データ連携サーバ等）は多要素認証の対象としない。	地方公共団体における情報セキュリティポリシーに関するガイドラインにおいて、情報システム管理者に多要素認証を求めているため。 選択レベルを最高レベルに引き上げたことにより、メトリクス説明を選択レベル（レベル３）の記載に合わせるため。 また、同様の理由により、[＋]条件が不要となるため。 認証方式、認証の対象の明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
E.5.2.1	システム上の対策における操作制限	（備考）	（備考） 【注意事項】 利用者に応じて適切に、実行可能なプログラム、コマンド操作、アクセス可能なファイルを設定・管理すること。	利用者の属性に応じたアクセス制御が必要である旨を追記。
E.6.1.1	伝送データの暗号化の有無	（選択レベル） レベル1：認証情報のみ暗号化 （選択時の条件） 内部ネットワークのみ接続する情報システムを想定。ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 （備考） 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。	（選択レベル） レベル3：すべてのデータを暗号化 （選択時の条件） インターネットに直接接続せず、内部ネットワークのみに接続する情報システムを想定。 （備考） 【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。ガバメントクラウド及びISMAPクラウドサービスリストに登録されているクラウドサービスについては、ISMAPの認証の過程で通信のセキュリティ対策の実施を確認しているため、クラウドサービス内の伝送データの暗号化は必須ではない。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。	「地方公共団体の情報システムのクラウド利用等に関する情報セキュリティポリシーガイドライン改定方針」に沿って、選択レベルを変更するため。 内部ネットワークの内容を明確化するため。 「暗号化」の定義の明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
E.6.1.2	蓄積データの暗号化の有無	（選択レベル） レベル1：認証情報のみ暗号化 （選択時の条件） 蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [＋]物理記録媒体の盗難・紛失の可能性が有る場合 （レベル） レベル3： （備考） 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。	（選択レベル） レベル3：すべてのデータを暗号化 （選択時の条件） 蓄積するデータについては、第三者に漏洩しないようすべてのデータの暗号化を実施する。 （レベル） レベル3：すべてのデータを暗号化 （備考） 【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。 システム利用開始時点からの全データを暗号化すること。	「地方公共団体の情報システムのクラウド利用等に関する情報セキュリティポリシーガイドライン改定方針」に沿って、選択レベルを変更するため。 「暗号化」の定義の明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
E.7.1.1	ログの取得	（選択時の条件） 不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある） （備考） 【注意事項】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等	（選択時の条件） 不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （備考） 【注意事項】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ 等	ログ取得が性能に影響を及ぼす可能性は低いため削除。 取得対象ログの例を追記。
E.7.1.3	不正監視対象（装置）	（メトリクス説明） サーバ、ストレージ等への不正アクセス等の監視のために、ログを取得する範囲を確認する。 不正行為を検知するために実施する。 （選択時の条件） 脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。	（メトリクス説明） サーバ、ストレージ、ネットワーク機器、端末等への不正アクセス等の監視のために、ログを取得する範囲を確認する。 不正行為を検知するために実施する。 （選択時の条件） 脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ、ネットワーク機器、端末等の範囲を定めておく必要がある。	明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
E.10.1.1	セキュアコーディング、Webサーバの設定等による対策の強化	（選択時の条件） [-] Webアプリケーションを用いない場合	（選択時の条件） [-] インターネットに接続したWebアプリケーションを用いない場合	インターネット上に公開しないWebアプリケーションは対策効果が見込まれないため。
E.10.1.2	WAFの導入の有無	（選択時の条件） 内部ネットワークのみ接続する情報システムを想定。そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] Webアプリケーションを用いる場合	（選択時の条件） インターネットに直接接続せず、内部ネットワークのみに接続する情報システムを想定。 [+] インターネットに接続したWebアプリケーションを用いる場合	インターネット上に公開しないWebアプリケーションは対策効果が見込まれないため。 内部ネットワークによる脅威の観点では無く、WAF導入の効果の観点で条件を選択するため。
A.1.3.1	RPO（目標復旧地点）（業務停止時）	（レベル） レベル3：障害発生時点（日次バックアップ+アーカイブからの復旧） ※アーカイブとはバックアップ前の一時的に保存されているデータを指す	（レベル） レベル3：障害発生時点（日次バックアップ+一時保存データからの復旧）	一般的には、「アーカイブ」の用語は、一時保存データを指さないため、誤解を生じさせないよう、用語を整理。
A.1.3.2	RTO（目標復旧時間）（業務停止時）	（備考） 【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。	（備考） 【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。 目標復旧時間をSLAに定めていないクラウドサービスを利用する場合は、CSPがSLAで示す稼働率を元に業務停止時間の最大値を算出し、RTOを検討することが考えられる。	クラウドサービスにおいては一般に障害発生時の目標復旧時間が定められていないことを前提に、クラウド部分も含めたRTOの考え方を示すため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
B.1.1.3	データ量（項目・件数）	（備考） 【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民記録システムであれば住民データ・世帯データ・異動データ等がある。	（備考） 【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民記録システムであれば住民データ・世帯データ・異動データ等がある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	クラウドサービスでオートスケール機能等を利用することで、各リソースの拡張性の確保が見込まれるため。
B.1.1.4	オンラインリクエスト件数	（備考） 【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民記録システムの転入・転出処理などがある。	（備考） 【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民記録システムの転入・転出処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	クラウドサービスでオートスケール機能等を利用することで、各リソースの拡張性の確保が見込まれるため。
B.1.1.5	バッチ処理件数	（備考） 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。	（備考） 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。	クラウドサービスでオートスケール機能等を利用することで、各リソースの拡張性の確保が見込まれるため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.1.1.1	運用時間（平日）	（選択時の条件） [-] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合 （レベル） レベル2：定時外も頻繁に利用（1日12時間程度利用） レベル3：24時間利用 レベル4： （備考） 【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。 定時：	（選択時の条件） [-] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、頻繁ではないが計画された稼動延長がある場合 （レベル） レベル2：繁忙期は定時外も頻繁に利用（1日12時間程度利用） レベル3：定時外も頻繁に利用（1日12時間程度利用） レベル4：24時間利用 （備考） 【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。	繁忙期に運用時間が異なることが想定されるため。 クラウドサービス利用における注意事項の追加。
C.1.1.2	運用時間（休日等）	（備考）	（備考） 【注意事項】 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。	クラウドサービス利用における注意事項の追加。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.4.3.1	マニュアル準備レベル	（選択時の条件） 運用をユーザが実施することを想定。 通常運用に必要なオペレーションのみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合 （備考） 【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。	（選択時の条件） 運用をユーザが実施することを想定。 [-]通常運用に必要なオペレーションのみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合 （備考） 【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。 なお、クラウドサービス上でのメンテナンス（一部サービスの提供終了や廃棄を含む）への対応に関するマニュアルについても想定される。	クラウドサービスのメンテナンス等に必要な手順書が漏れることがないよう、注意喚起するため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.4.5.1	外部システムとの接続有無	（メトリクス説明） 情報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。 （選択レベル） レベル1：庁内の外部システムと接続する （選択時の条件） 庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [-] データのやり取りを行う他システムが存在しない場合 [+] 庁外の外部システムに接続して、データのやり取りを行う場合 （レベル） レベル0：外部システムと接続しない レベル1：庁内の外部システムと接続する レベル2：庁外の外部システムと接続する	（メトリクス説明） 情報システムの運用に影響する他システムや外部システム（団体が管理に関わらないシステム）との接続の有無に関する項目。 （選択レベル） レベル1：他システムと接続する （選択時の条件） 庁内基幹系システムとして、住基と税などのように連携する他システムが存在することを想定。 [-] データのやり取りを行う他システムが存在しない場合 [+] 外部システムに接続して、データのやり取りを行う場合 （レベル） レベル0：他システムや外部システムと接続しない レベル1：他システムと接続する レベル2：外部システムと接続する	明確化のため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.4.5.1	外部システムとの接続有無	（備考） 【注意事項】 接続する場合には、そのインターフェース（接続ネットワーク・通信方式・データ形式等）について確認すること。	（備考） 【注意事項】 庁外の民間クラウド等で稼動する場合でも、内部ネットワークで接続する場合は庁内のシステムと位置づけること。 また、接続する場合には、そのインターフェース（接続ネットワーク・通信方式・データ形式等）について確認すること。	明確化のため。
D.4.1.1	移行データ量	（選択時の条件） 10TB（テラバイト）未満のデータを移行する必要がある。 [-] 1TB未満の場合 [+] 10TB以上の場合	（選択時の条件） 移行前システムのデータを抽出したうえで、移行対象データを決定する必要がある。	選択レベルと選択時の条件の整合化のため。
A.3.2.1	保管場所分散度（外部保管データ）	（選択レベル） 遠隔地1カ所 （レベル） レベル3：2ヶ所（遠隔地） レベル4： （備考） ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。	（選択レベル） 遠隔地1ヶ所 （レベル） レベル3：2ヶ所（近隣の別な建物と遠隔地） レベル4：2ヶ所（遠隔地） （備考） ここで遠隔地とは、主系サーバ等の設置場所と同時被災の恐れがない遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。 A.3.2.2（保管方法（外部保管データ））と合わせて考慮し、整合するようにレベルを選択すること。	A.3.2.1（保管場所分散度）とA.3.2.2（保管方法）の関係性の整合化を行い明確化するため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
A.3.2.2	保管方法（外部保管データ）	（選択レベル） レベル1：同一システム設置場所内の別ストレージへのバックアップ （選択時の条件） 媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合 （レベル） レベル0：媒体による保管 レベル1：同一システム設置場所内の別ストレージへのバックアップ レベル2：DRサイトへのリモートバックアップ （備考）	（選択レベル） レベル2：ネットワーク経由でストレージへのリモートバックアップを含む （選択時の条件） A.3.2.1と同じ拠点へのリモートバックアップを想定。 [-]媒体での外部保管のみによる運用を許容できる場合 （レベル） レベル0：外部保管しない レベル1：媒体による外部保管のみ レベル2：ネットワーク経由でストレージへのリモートバックアップを含む （備考） 【注意事項】 A.3.2.1（保管場所分散度(外部保管データ)）と合わせて考慮し、整合するようにレベルを選択すること。	A.3.2.1（保管場所分散度）とA.3.2.2（保管方法）の関係性の整合化を行い明確化するため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.1.3.1	監視情報	（選択レベル） レベル4：リソース監視を行う （レベル） レベル0：監視を行わない レベル1：死活監視を行う レベル2：エラー監視を行う レベル3：エラー監視（トレース情報を含む）を行う レベル4：リソース監視を行う レベル5：パフォーマンス監視を行う	（選択レベル） レベル4：レベル3に加えてリソース監視を行う （レベル） レベル0：監視を行わない レベル1：死活監視を行う レベル2：レベル1に加えてエラー監視を行う レベル3：レベル2に加えてエラー監視（トレース情報を含む）を行う レベル4：レベル3に加えてリソース監視を行う レベル5：レベル4に加えてパフォーマンス監視を行う	下のレベルの内容に加えて当該レベルを実施することを明確化するため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.5.9.1	定期報告会実施頻度	（備考） 【注意事項】 障害発生時に実施される不定期の報告会は含まない。	（備考） 【注意事項】 業務ごとの定期報告会の頻度を指す。 また、障害発生時に実施される不定期の報告会は含まない。	明確化のため。
C.6.3.1 （新規）	インシデント管理の実施有無		（メトリクス説明） インシデントの管理を実施するかどうかを確認する。 （選択レベル） レベル1：既存のインシデント管理のプロセスに従う （選択時の条件） [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	運用管理業務に対する要求レベルを漏れなく定義できるようにするため。
C.6.4.1 （新規）	問題管理の実施有無		（メトリクス説明） インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。 （選択レベル） レベル1：既存の問題管理のプロセスに従う （選択時の条件） [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	運用管理業務に対する要求レベルを漏れなく定義できるようにするため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.6.5.1 （新規）	構成管理の実施有無		（メトリクス説明） リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。 （選択レベル） レベル1：既存の構成管理のプロセスに従う （選択時の条件） [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	運用管理業務に対する要求レベルを漏れなく定義できるようにするため。
C.6.6.1 （新規）	変更管理の実施有無		（メトリクス説明） ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。 （選択レベル） レベル1：既存の変更管理のプロセスに従う （選択時の条件） [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	運用管理業務に対する要求レベルを漏れなく定義できるようにするため。

非機能要件の標準の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.6.7.1 （新規）	リリース管理の実施有無		（メトリクス説明） 承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。 （選択レベル） レベル1：既存のリリース管理のプロセスに従う （選択時の条件） [-]運用管理契約を行わない場合 [＋]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	運用管理業務に対する要求レベルを漏れなく定義できるようにするため。
E.3.1.2	Webアプリケーション診断実施の有無	（メトリクス） Web診断実施の有無 （メトリクス説明） Web診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のこと。 （選択時の条件） [-] 内部犯を想定する必要がない場合、Webアプリケーションを用いない場合	（メトリクス） Webアプリケーション診断実施の有無 （メトリクス説明） Webアプリケーション診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のこと。 （選択時の条件） [-] 内部犯を想定する必要がない場合、インターネットに接続したWebアプリケーションを用いない場合	インターネット上に公開しないWebアプリケーションは対策効果が見込まれないため。