資料２－①

地方公共団体の基幹業務システムの標準非機能要件の拡充等について

令和４年７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

標準非機能要件の位置づけ

○　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。

○　標準非機能要件は、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）

標準非機能要件の内容

○ 「標準非機能要件」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」とされている項目の「選択レベル」を基準として、最新の状況等を鑑み修正をしたもの。

※ 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]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②			レベル								備考［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件		－	＊	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※4（業務停止時）	業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	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）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [-] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）により レベルを選定）	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P35	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [-] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P36	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [-] 影響を切り離せる機能がある場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）

標準非機能要件の拡充等の観点

○ 「標準非機能要件」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、現行の標準非機能要件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。あわせて、本セキュリティ検討会での検討状況も踏まえ、選択レベルを見直すとともに、これまで自治体等から寄せられた質問・意見等も勘案したところ。

【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。

標準非機能要件の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
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。
A.3.2.1	保管場所分散度（外部保管データ）	（備考） 【注意事項】 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。	（備考） 【注意事項】 ここで遠隔地とは、主系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。	明確化のため。

標準非機能要件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） 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 （備考）	（選択レベル） 2　DRサイトへのリモートバックアップ （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。 （備考） 【レベル】 レベル1及び2のバックアップとは、リアルタイムにデータバックアップの取得が可能であるものを意味する。また、レベル2のDRサイトとは、システム設置場所（庁舎等の利用場所と必ずしも一致しない）と同時被災の恐れがない遠隔地を意味する。 【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、同水準を示すようにレベルを選択すること。	A.3.2.1（保管場所分散度（外部保管データ））とA.3.2.2（保管方法（外部保管データ））の「遠隔地」と「DRサイト」について、地方公共団体により解釈が異なる可能性があり、整合させるため。

標準非機能要件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、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、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。

標準非機能要件の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
B.1.1.5	バッチ処理件数	（備考） 【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。	（備考） 【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 なお、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。

標準非機能要件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)	（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：	（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。	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） 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。
C.2.3.5	OS等パッチ適用タイミング	（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。	（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）。 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。 また、マイナンバー利用事務系のOSについては最新の修正パッチを常時適用すること。	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、マイナンバー利用事務系のOSについて最新の修正パッチを常時適用することが求められているため。

標準非機能要件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	（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。	（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。

標準非機能要件の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.6.3.1 （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	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	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.6.5.1 （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	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。

標準非機能要件の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
C.6.6.1 （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	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.6.7.1 （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	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。

標準非機能要件の拡充等をする項目

項番	メトリクス	旧	新	見直し理由
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。
E.5.1.1	管理権限を持つ主体の認証	（選択レベル） １　１回	（選択レベル） ３　複数回、異なる方式による認証	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。
E.6.1.1	伝送データの暗号化の有無	（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。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。	（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を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。	内部ネットワークの内容を明確化するため。
E.6.1.2	蓄積データの暗号化の有無	（選択時の条件） [＋]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	（選択時の条件） [＋]物理記録媒体の盗難・紛失の可能性が有る場合、又は、クラウドサービスの仕様により暗号化消去を行う場合（後者については選択レベルを2上げる） （レベル） レベル3　すべてのデータを暗号化	クラウドサービスの仕様によりデータ消去時の物理破壊が困難な場合に、蓄積データを暗号化した上で消去することを求めるため。この場合、選択レベルを２上げ、レベル３を新規に創設する。

標準非機能要件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ない場合	（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を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。 [+]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。