農林水産省 情報共有システム機能要件対応表

企業名：株式会社建設総合サービス
情報共有システム名：電納ASPer（デンノウエスパー）

工事の情報共有システム活用要領の機能と要件　　2019年10月時点

	機　能	要　　件	システムの実装範囲
1	工事基本情報管理機能	(1)システムへの直接入力で工事基本情報を登録できる。 (2)登録した工事基本情報を修正、削除、参照できる。 (3)登録した工事基本情報を発議書類作成機能等で利用できる。 (4)工事実績情報システム（コリンズ）ファイルの登録内容を取り込み、工事基本情報として利用できる。	○
2	掲示板機能	(1)受発注者間で交換・共有する情報（以下、「記事等」という。）を登録・削除・閲覧できる。 (2)記事等には、タイトル、登録者名、登録日時等を管理できる。 (3)記事等に対して、返信コメントを登録できる。 (4)記事等には、書類、図面、写真等の電子ファイルを添付できる。 (5)記事等には、閲覧可能な利用者の範囲を設定できる。 (6)同一システムを利用する監督職員が、担当する複数または全ての工事で登録された記事等をツリー構造等で一覧表示できる。 (7)同一システムを利用する監督職員が、担当する複数または全ての工事で記事等を一括して登録、修正、削除できる。 (8)ログイン時に、担当する工事に関する未読の記事等のタイトル一覧を表示できる。 (9)記事等のタイトル、登録者名、登録日時から、記事等を検索できる。	○
3	発議書類作成機能	(1)工事関係書類（別表４の様式31、33、37）を作成、修正、削除できる。 (2)作成時に必須項目に未記入があった場合は、エラーメッセージを表示できる。 (3)工事基本情報が、工事関係書類の入力フォームに反映できる。 (4)以前作成した工事関係書類の記載内容を利用して、新たに別の工事関係書類の作成ができる。 (5)作成中の発議書類は、一時保存することができる。 (6)一時保存した発議書類を修正・削除できる。 (7)発議書類には、書類、図面、写真等の電子ファイルを添付できる。	○
4	ワークフロー機能	(1)システム内で電子により決裁処理ができる。 (2)回答予定日を設定できる。 (3)中間処理・回答日、最終処理・回答日を設定できる。 (4)発議書類の承認履歴、現在の承認状況等を一覧表示により確認できる。 (5)同一システムを利用する監督職員が、担当する複数または全ての工事の発議書類の承認履歴及び現在の承認状況等を一覧表示できる。 (6)一覧には、工事名、タイトル、承認・閲覧状況等を表示できる。 (7)一覧表示した情報を絞り込み表示、並べ替えできる。 (8)承認者及び閲覧者（以下、「承認者等」という。）の選択及びワークフローの順番が設定できる。	

		(9)発議者は発議書類に対する説明等のコメントを付与することができ、承認者等がコメントを確認することができる。 (10)発議者は、承認者等に対し電子メールで発議を通知することができる。 (11)承認者は、発議文書に対し承認、差し戻しを行うことができる。 (12)差し戻しは、発議書類の発議者または前の承認者に対して行うことができる。 (13)承認者は、処理・回答内容欄を含む工事関係書類について、処理・回答内容を入力できる。 (14)承認者は、発議書類に対する所見等をコメントとして登録でき、発議者及び他の承認者等が確認できる。 (15)承認者は、発議者に対し電子メールで承認、差し戻しを通知することができる。 (16)決裁中の工事関係書類が差し戻し等により修正等となった場合には、修正日や修正内容等が履歴として表示できる。 (17)単純な書類の入力ミス等に対応できるように、決裁が完了した工事関係書類については、発議日や最終処置・回答日を修正することができる。 (18)発議書類の承認履歴を電子データ等で出力できる。	○
5	書類管理機能	(1)工事関係書類をフォルダ分けして、体系的に管理できる。（フォルダ分けは、別表４－１、４－２に基づきに分類する。） (2)工事書類は、フォルダを指定して登録できる。 (3)フォルダは適宜追加、修正、削除することができる。 (4)工事関係書類は、分類、日付等により検索、並べ替えし、一覧表示できる。 (5)工事関係書類を閲覧できる。 (6)ファイルを指定してファイル出力できる。 (7)工事関係書類を一覧表としてExcel、CSV 等の形式でファイル取得でき、資料として活用できる。	○
6	工事関係書類出力機能	(1)登録した工事関係書類は、外部媒体にフォルダ構成、ファイル名を保持したまま、一部または全部をファイル出力できる。	○
7	スケジュール管理機能	(1)個人の予定を登録、修正、削除、参照できる。 (2)同一システムを利用する監督職員が、担当する複数または全ての工事について、それらの工事を担当する複数または全利用者の予定を１画面に統合して参照できる。 (3)同一システムを利用する監督職員が、担当する複数の工事で予定を一括して登録、修正、削除できる。	○
8	システム管理機能	(1)利用者ごとにＩＤ、パスワード、メールアドレス、使用できる機能及び権限等を登録、変更、削除することができる。 (2)複数の工事を担当する監督職員は、同一のＩＤ、パスワードによりログインすることができる。	○

情報共有システムセキュリティ要件

項　目	条　件	システムの実装範囲
1．アプリケーション、共通の対策	(1)アプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器、ネットワーク稼働状況、障害を監視し、異常を検知できること。 (2)定期的に脆弱性診断を実施し、また、脆弱性に関する情報を定期的に収集し、パッチによる更新を実施できること。	○
2．暗号化	(1)ＩＤ及びパスワードを通知する際、暗号化が実施されること。暗号化ができない場合、ＩＤ発行時に暗号化が行われない旨を利用者に通知されること。 (2)暗号化のアルゴリズムは、「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）」（総務省、経済産業省 平成25年3月1日）に記載されたいずれかのものであること。 (3)情報共有システムと利用者との通信は、SSL3.0/TLS1.0以上で暗号化されること。	○
3．アクセス制御	工事帳票等システム内のデータが不当に消去、改ざんされないように、アクセス制御が実施されること。	○
4．ネットワーク	(1)ファイアウォール、リバースプロキシの導入等により外部及び内部からの不正アクセスを防止することができること。 (2)フィッシング等を防止するため、サーバ証明書の取得等の必要な対策を実施できること。	○
5．物理的セキュリティ	サーバ・ストレージ、情報セキュリティ対策機器等は、重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対して個人認証システムをも用いた入退室管理が実施される部屋に設置されること。	○
6．クラウドサービスに係るアクセスログ等の証跡の保存及び提供	(1)情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定め、監視記録を保存すること。 (2)ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。	○
7．インターネット回線とクラウド基盤の接続点の通信の監視	(1)外部ネットワークを利用した情報交換において、インターネット回線とクラウド基盤の接続点の通信を監視し、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	○
8．クラウドサービスの委託先による情報の管理・保管の実施内容の確認	(1)サービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。 (2)バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等に関する手順書を作成すること。	○
9．クラウドサービス上の脆弱性対策の実施内容の確認	弱性対策の実施内容を確認できること。	○

10. クラウドサービス上の情報に係る復旧時点目標（RPO）等の指標を設定	クラウドサービスの稼働性能を明確化することは、利用者の安心した利用を促進する。そのため、復旧時点目標（RPO）等の指標を、契約書等を通じて利用者に示すこと。	○
11. クラウドサービス上で取り扱う情報の安全性確保	データベースの安全性を確保するためにID、パスワード等でアクセスを制御できること。また、ID、パスワードは厳密に管理すること。	○
12. 利用者の意思によるクラウドサービス上で取り扱う情報の確実な削除・廃棄	(1)契約書に記載された期日に達した際、自動あるいは、手動によりデータを削除すること。 (2)削除したデータは再現できないことを、契約書等を通じて利用者に示すこと。	○
13. 利用者が求める情報開示請求に対する開示項目や範囲の明記	(1)利用者が請求する情報開示請求事項や範囲について、情報を提供すること。 (2)ただし、指定された範囲が情報セキュリティの確保の観点で公開できない場合、その理由を示すことで開示範囲を制限することができる。	○
14. 利用するクラウドサーバの安全性対策	(1)クラウドサービスは、情報セキュリティ監査の観点から各種の認定・認証制度の適用状況等サービス及び当該サービスの信頼性が十分であることが必要である。よって、総合的・客観的に評価できるクラウドサーバにてサービスを提供していること。 (2)クラウドサーバは、安全なデータセンター（IDC）で稼働している必要がある。そこで、データセンター（IDC）の客観的な安全性評価として、JDCC(特定非営利活動法人日本データセンター協会)が制定した、日本国内のデータセンターに求められる信頼性を実現するための指標であるファシリティスタンダードでティア3相当以上の環境下で稼働していることを必須とし、契約書等を通じて利用者に示すこと。	○
15. サービス運営・提供会社の情報セキュリティ	(1)蓄積するデータおよび情報は、機密性、可用性、安全性を確保しなければならない。 (2)サービス運営・提供会社は、確実かつ不断に情報セキュリティ確保していることをJISQ27001の資格取得をもって客観的に評価されていることを示すこと。 (3)JISQ27001の資格取得状況は、契約書等を通じて利用者に示すこと。	○
16. その他	(1)サーバ・ストレージ、情報セキュリティ対策機器等は、地震、火災、雷、停電に対する対策が施された国内の建物に設置すること。またデータのバックアップを行い、地震等発生のよるデータの破壊等に対応できる体制をとること。 (2)運用管理端末について、使用するファイルのウィルスチェックを行う、許可されていないプログラムのインストールを行わせない等セキュリティを考慮する。また、技術的脆弱性に関する情報を定期的に収集し、パッチによる更新を実施できること。 (3)上記を踏まえて、導入する組織が求めるセキュリティ要件を満足できること。 (4)サービスの提供は、日本国の法令が適用されること。	○