

森林整備保全事業の調査、測量、設計及び計画業務における
受発注者間の情報共有システム実施要領

1 総則

(1) 目的

森林整備保全事業の調査、測量、設計及び計画業務における情報共有システムの活用は、業務における「受発注者間のコミュニケーションの円滑化」、「受発注者の事務負担の軽減」等を図り、業務の適正な履行を確保することを目的とする。

(2) 用語の定義

本要領で用いる用語のうち、「森林整備保全事業調査、測量、設計及び計画業務標準仕様書」（平成29年3月30日付け28林整計第380号林野庁長官通知）に定義する用語以外についての定義は以下のとおりとする。

① 情報共有システム

情報通信技術を活用し、受発注者間など異なる組織間で情報を交換・共有することによって業務効率化を実現するシステムをいう。

② 情報共有システムのサービス提供者

インターネットを介して情報共有システムのサービスを提供している民間事業者等をいう。

③ 利用者

情報共有システムを使用して業務帳票の「協議」、「承諾」等の処理を行う受発注者及び保存された電子データの閲覧を行う受発注者をいう。

④ 承認者

発議された業務関係種類について承認する者をいう。

⑤ 閲覧者

発議された業務関係書類について閲覧する者をいう。

⑥ 差し戻し

発議された業務関係書類が承認できない場合に、書類を発議者または前の承認者にその理由とともに返却することをいう。

(3) 情報共有システムの機能と要件

情報共有システムは、別表1の機能と要件を満たすものでなければならない。

(4) 情報共有システムの利用上の留意点

① 情報共有システムの契約

ア 受注者は、本業務で使用する情報共有システムを選定し、監督職員と協議し承諾を得なければならない。

イ 情報共有システムのサービス提供者との契約は、受注者が行うものとし、契約締結後は、契約を証する写しを監督職員に提出するものとする。

ウ 情報共有システムのサービス提供者との契約は、既に本システムを導入している国土

交通省が公表している「情報共有システム提供者における機能要件の対応状況（導入担当者向け）」を参考資料として利用するものとする。

情報共有システム提供者における機能要件の対応状況【国土交通省ホームページ URL】

http://www.cals-ed.go.jp/jouhoukyouyuu_taiou/

② 関係者への利用権限の付与、利用の習慣化

利用者は2-(2)による登録を経て、アカウント（ID、パスワード）を得た時点から利用権限を付与されたものとする。アカウントを得た利用者は、情報共有システムの利用に努めるものとする。

③ アカウント管理の徹底

アカウントが第三者に渡ると、業務関係書類の漏えいや、改ざん等の恐れがあるため、利用者は、アカウントの管理を徹底するものとする。なお、パスワードは、利用者ごとに設定するものとする。

(5) 受注者と情報共有システムのサービス提供者との契約内容

受注者と情報共有システムのサービス提供者との契約については、次の内容を含めた契約を行うものとする。

① サービス提供者は、情報共有システムに関する障害を適正に処理、解決できる体制及びヘルプデスク等を通じて問合せ及び要望に応える体制を整えること。

② サービス提供者は、善良なる管理者の注意をもってしても防御し得ない不正アクセス等により、情報漏えい、データ破壊、システム停止などがあつた場合、速やかに受注者に連絡を行い、適正な処理を行うこと。

③ ②の場合において、サービス提供者に重大な管理瑕疵があると発注者若しくは受注者が判断した場合、又は復旧若しくは処理対応が不適切な場合には、受注者は、サービス提供者と協議の上、情報共有システムの利用契約を解除することができること。

④ サービス提供者が定める約款等より、本実施要領が優先すること。

(6) 費用

情報共有システムの利用に係る費用は、以下のとおりとする。

① 情報共有システムの利用に係る費用（登録料及び使用料）は、直接経費に含まれる。

② 情報共有システムの操作に係る研修（発注者も含まれる場合に限る）や緊急時の対応等に費用が生じた場合は、別途監督職員と協議するものとする。

2 準備

(1) 情報共有システム利用環境

情報共有システムの利用環境及びセキュリティ要件は、別表2及び別表3によるものとする。また、受注者は、以下の確認等を行うものとする。

① 通信回線の確認

受注者は、担当部署等におけるADSLや光ファイバ、高速モバイル回線等の通信速度及び実効速度等について確認し、利用できる体制を整えるものとする。なお、環境を整えることが不可能な場合は、監督職員と協議するものとする。

② 対応パソコン・OS等の確認

受注者は、使用する端末（パソコンのOSやCPU、ハードディスク容量、メモリ容量、ディスプレイ解像度等）について確認し、利用できる体制を整え、担当部署等で使用する端末の形式・型番を監督職員に報告するものとする。

③ 対応ウェブブラウザの確認

受注者は、使用するウェブブラウザについて確認し、利用できる体制を整えるものとする。

④ セキュリティの確認

受注者は、情報共有システムに係るデータの保管やサイバー攻撃、不正アクセス等に対するセキュリティ対策及び要件について、サービス提供者に確認し、監督職員に報告するものとする。

(2) 利用者の決定

受発注者は、契約した情報共有システムの操作手順に従い、利用者の役職・氏名・メールアドレス等の情報を登録するものとする。

3 情報共有システムの利用

(1) 情報共有システムで扱う業務関係書類

別表4の業務書類のうち、利用頻度を踏まえ、監督職員と協議して定めるものとする。

(2) 個人情報等の扱い

個人情報等が含まれる機密性の高い資料等は、情報共有システム内で取り扱ってはならない。

(3) 情報共有システムで扱う業務関係書類の処理

情報共有システムで扱う業務関係書類については、掲示板機能、発議書作成機能及びワークフロー機能により処理するものとする。なお、情報共有システムで扱う業務関係書類については、森林整備保全事業調査、測量、設計及び計画業務標準仕様書で定義する「書面」として認めるものとする。

(4) 情報共有システムで扱う業務書類の整理

受注者は、情報共有システムで扱う業務関係書類について、受発注者が閲覧・検索を容易にできるよう種別毎にフォルダ分けを行い整理するものとする。

(5) 担当部署等での使用

① 担当部署等で使用する端末は、受注者のセキュリティ対策を施したものとし、2-(1)-②により監督職員に報告した端末とする。

② 担当部署等で端末を使用する場合は、保管方法や事務所等の施錠方法を定め、盗難対策を徹底させるとともに、休日、夜間は持ち出し可能な場所に端末を保管したままにしないものとする。また、端末を移動させる場合は、利用者の手元から離さないようにしなけれ

ばならない。

(6) データバックアップ体制

受注者は、サービス提供者が行うデータバックアップとは別に、情報共有システムで取り扱うデータのバックアップを行わなければならない。なお、バックアップ体制として、バックアップ担当者氏名、頻度、媒体、媒体保管場所を監督職員に報告するものとする。

(7) 業務完成後のデータの取扱い

受注者は、サービス提供者との契約が終了するまでに、情報共有システム上の全てのデータが消去される時期についてサービス提供者に確認し、監督職員に報告するものとする。

(8) 情報共有システムで扱わない業務関係書類の取扱い

情報共有システムで扱わない業務関係書類については、従来どおり紙により提出するものとする。

4 検査における業務関係書類の取扱い

情報共有システムで扱う業務関係書類の検査（業務完成検査・既済部分検査・中間技術検査）は、パソコンやプロジェクター等を用い電子データ（以下「電子検査」という。）で行うことができるものとする。なお、電子検査を行う際に必要となるパソコンやプロジェクター等の機材については、受注者が準備するものとする。

また、情報共有システムで扱わない業務関係書類の検査は、従来どおり紙により行うものとする。

「森林整備保全事業の調査、測量、設計及び計画業務における受発注者間の情報共有システム実施要領」の機能と要件

	機能	要件
1	業務基本情報管理機能	(1)システムへの直接入力で業務基本情報を登録できる。 (2)登録した業務基本情報を修正、削除、参照できる。 (3)登録した業務基本情報を発議書類作成機能等で利用できる。 (4)業務実績情報システム（テクリス）ファイルの登録内容を取り込み、業務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、担当する複数又は全ての業務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、担当する複数又は全ての業務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、担当する業務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)業務関係書類を作成、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)業務基本情報が、業務関係書類の入力フォームに反映できる。 (4)以前作成した業務関係書類の記載内容を利用して、新たに別の業務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)一時保存した発議資料を修正、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、担当する複数又は全ての業務の発議書類の承認履歴及び現在の承認状況等を一覧できる。 (6)一覧には、業務名、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、並び替えできる。 (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

		<p>一の順番が設定できる。</p> <p>(9)発議者は発議種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。</p> <p>(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。</p> <p>(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。</p> <p>(12)差し戻しは、発議書類の発議者又は前の承認者に対して行うことができる。</p> <p>(13)承認者は、処理・回答内容欄を含む業務関係書類について、処理・回答内容を入力できる。</p> <p>(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。</p> <p>(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。</p> <p>(16)決裁中の業務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。</p> <p>(17)単純な書類の入力ミス等に対応できるように、決裁が完了した業務関係書類について、発議日や最終処置・回答日を修正することができる。</p> <p>(18)発議書類の承認履歴を電子データ等で出力できる。</p>
5	書類管理機能	<p>(1)業務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に基づき分類する。)</p> <p>(2)業務書類は、フォルダを指定して登録できる。</p> <p>(3)フォルダは適宜追加、修正、削除することができる。</p> <p>(4)業務関係書類は、分類、日付等により検索、並べ替えし、一覧標示できる。</p> <p>(5)業務関係書類を閲覧できる。</p> <p>(6)ファイルを指定してファイルを出力できる。</p> <p>(7)業務関係書類を一覧表として、Excel、CSV等の形式でファイルを取得でき、資料として活用できる。</p>
6	業務関係書類出力機能	<p>(1)登録した業務関係書類は、外部媒体にフォルダ構成、ファイル名を保持したまま、一部又は全部をファイル出力できる。</p>
7	スケジュール管理機能	<p>(1)個人の予定を登録、修正、削除、参照できる。</p> <p>(2)同一システムを利用する監督職員が、担当する複数又は全ての業務について、それらの業務を担当する複数又は全利用者の予定を一画面に統合して参照できる。</p> <p>(3)同一システムを利用する監督職員が、担当する複数の業務で予定を一括して登録、修正、削除できる。</p>
8	システム管理機能	<p>(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、削除できる。</p> <p>(2)複数の業務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。</p>

情報共有システム利用環境（発注者）

項目	条件
1 通信回線	ADSL（1.5Mbps）以上
2 ブラウザ	Google chrome
3 OS	上記ブラウザが表示可能なもの
4 ディスプレイ	1024×768 以上が表示可能なもの

情報共有システムセキュリティ要件

項目	条件
1 アプリケーション、共通の対策	<p>(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。</p> <p>(2)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、通信機器について、定期的にぜい弱性診断を実施し、また、ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ情報等）を定期的に収集し、パッチによる更新を実施できること。</p>
2 暗号化	<p>(1)利用者に ID 及びパスワードを通知する際、その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ず旨を利用者に通知されること。</p> <p>(2)情報共有システムに蓄積する利用者のパスワードは、暗号化が実施されること。</p> <p>(3)利用者からの要請があった場合、直ちに当該 ID によるシステムの利用を停止できること。</p> <p>(4)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。</p> <p>(5)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。</p>
3 アクセス制御	<p>(1)帳票（鑑）並びに帳票（添付）及びその他の添付資料、各保存した履歴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。</p>
4 ネットワーク	<p>(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。</p> <p>(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に必要な対策を実施できること。</p>
5 物理的セキュリティ	<p>(1)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用いた入退室管理が部屋に設置されること。</p> <p>(2)適切に管理された鍵が取り付けられたサーバールームやラックに設置されること。</p>
6 クラウドサービスに係るアクセスログ等の証拠の保存及び提	<p>(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。</p> <p>(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</p>

供	ホーム、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	ぜい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

	<p>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。</p>
15 サービス運営・提供 会社の情報セキュリティ	<p>(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。</p> <p>(2)サービス運営・提供会社は、确实かつ不断に情報セキュリティ確保していることを JIS Q27001 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。</p> <p>(3)JIS Q27001 の資格取得状況は、契約書等を通じて利用者に示すこと。</p>
6 その他	<p>(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（以下、「地震等」という。）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、地震等発生によるデータの破壊等に対応できる体制をとること。</p> <p>(2)運用管理端末について、使用するファイルのウイ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、技術的ぜい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。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。</p> <p>(3)サービスの提供は、日本国の法令が適用されること。</p>

※コンピュータの利用や情報管理、情報システム運用に関して保安（セキュリティ）上の脅威となる事象が発生し、農林水産省のシステム管理者又は情報セキュリティ担当者が必要とする場合は、上記項目に係る手順書、関係書類を可能な範囲で提出すること。

情報共有システムで扱う治山事業の調査、測量、設計及び計画業務における様式一覧

1 「履行管理の様式」(関東森林管理局HP)の様式のうち、下記の様式に適用する。

様式番号	名称	関係条項等
第12号	〇〇〇〇の提出について	標準仕様書
第13号	指示、承諾、協議、確認、検査、立会(報告書・願書)	標準仕様書
第14号	調査等業務打合せ記録簿	標準仕様書
第15号	〇〇〇〇調査業務計画書	標準仕様書
第16号	組織計画表	標準仕様書
第17号	使用機械	標準仕様書
第18号	緊急時等の連絡体制	標準仕様書

2 森林整備保全事業の調査・測量・設計等請負業務監督実施細則(平成27年10月26日付け27 関治第111号)の様式のうち、下記の様式に適用する。

様式番号	名称	関係条項等
監第2号	貸与品(図書等)記録簿	標準仕様書
監第3号	指示・承諾通知書	標準仕様書