森林クラウドシステムに関わる
情報セキュリティガイドライン

－ Ver.6.0 －

令和３年３月

森林 GIS フォーラム　標準仕様分科会

目次

コラム：

1. ガイドラインの概要と目的

1-1. ガイドラインの概要

本ガイドラインは、「林野庁補助事業　森林情報高度利活用技術開発事業のうち森林クラウドシステム標準化事業」の取組みにおいて、森林クラウドシステムに関わる情報セキュリティについて検討をおこなった成果をガイドラインとしてまとめたものである。

本ガイドラインは、森林クラウドシステムの導入・構築・利用において、森林システム及び森林情報に起因して求められるセキュリティ対策を、クラウド利用者への導入指針として取りまとめた「セキュリティ要件編」、及び本事業で検討を行った、森林クラウドシステムを含めた森林情報の高度な利活用を行う上で明らかとなった課題とその対応策について、参考となるよう取りまとめた「利活用事例編」からなる。

森林クラウドシステムとは、クラウド環境で標準化した森林情報システムを構築し森林・林業に従事する都道府県、市町村、林業事業体が森林情報の高度利活用を目的としている。

森林クラウドシステムにおける情報セキュリティを検討するにあたって、森林・林業の特徴となる行政(都道府県、市町村等)が保有する森林情報を民間事業者(林業事業体、森林所有者等)が共有・利用するため森林クラウドシステム提供事業者に対する信頼性の確保が重要であるとともに、森林情報には個人情報(森林所有者情報)が含まれていることから利用者である都道府県、市町村、林業事業体(森林所有者を含む)等の業務遂行における安全性の確保が必要である。

平成 25 年度・26 年度は、森林クラウドシステム提供事業者(以下、クラウド事業者という)と都道府県、市町村、林業事業体等を対象に情報セキュリティに係る検討を実施し、その成果を情報セキュリティガイドライン(案)として公表した。

以下の図 1　情報セキュリティガイドラインの範囲に示す。

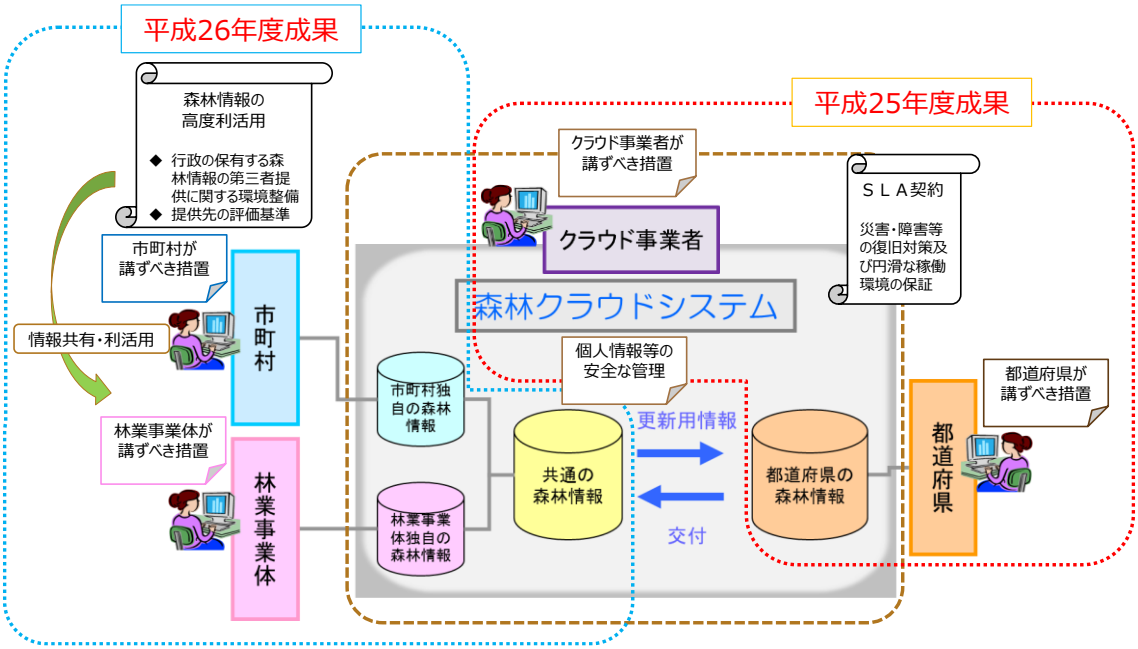


図 1　情報セキュリティガイドラインの範囲

平成 27 年度の情報セキュリティガイドラインは、複数のクラウド事業者がユーザ ID とパスワードを連携する、森林クラウド・トラストフレームワークに関する検討成果を基に、平成 26 年度に公表した情報セキュリティガイドラインの検証・改善を行い取りまとめた。

平成 28 年度の検討では、森林クラウド標準仕様の普及をテーマとして取り組んだ。セキュリティガイドラインについても、森林クラウドの導入時の手引きとして内容の更新と整理を行った。

平成 29 年度は、森林クラウドのさらなる普及を目指し、主に導入現場において留意すべき事項について、コラム形式のコンテンツを追加した。

令和 2 年度の改訂として、新たにセキュリティや個人情報保護対策の実践的手段としてマネジメントシステムの導入についてコンテンツを追加するとともに、巻末資料として個人情報保護法改正に伴う同法の改正ポイントを追加した。また、それに伴い、ガイドラインの構成を見直した。

1-2. ガイドラインの目的

情報通信技術の発展によりあらゆるものがインターネットにつながる時代となった今日、コンピュータ利用環境も大きく変わり始めている「IT を所有する」時代から「IT を利用する」時代にクラウドコンピューティングは、ネットワーク上に存在するコンピュータ資源を活用するための利用技術の発展成果である。

クラウドコンピューティング技術を活用した森林クラウドシステムの実証が平成 25 年度より開始されたことにより、森林情報のシステム化が進んでいない市町村及び森林所有者を含む林業事業体への導入が期待される。

森林クラウドシステムを安全で効果的に利用することができる様にクラウド事業者や森林クラウドシステムの利用者(以下、クラウド利用者という)が講ずべき情報セキュリティ対策とクラウド事業者、クラウド利用者間でサービス内容、範囲、品質等に関する保証基準の共通認識であるサービスレベルの合意を得る SLA（Service level Agreement）契約の締結が、森林クラウドシステムの普及のために重要となる。

本ガイドラインは、これらの観点から、新たに森林クラウドシステムの導入・構築・運用をする際に考慮すべき点・参照すべき情報を把握するとともに、森林クラウドシステムを含めた森林情報を利活用する際に必要となる手続き及びセキュリティ対策について取りまとめたものである。

1-3. ガイドラインの対象者

本ガイドラインの対象者として、森林クラウドシステムの「導入・運用」「構築」「利用」を行う者を対象としている。

■森林クラウドシステムの導入・運用を行う者（都道府県・市町村）

森林クラウドシステムの導入・調達について検討を行う者、多くの場合では都道府県・市町村の林務担当者及びシステム担当者

■森林クラウドシステムの構築を行う者（クラウド事業者）

このガイドラインでは森林クラウドシステムの導入及び構築を対象としており、自治体と直接的にやり取りを行うシステム事業者を指し、直接的に森林システムを構築・提供しないインフラ環境やプラットフォーム環境を提供する事業者については対象外とする。

本ガイドラインでは、それらの環境を利用した森林クラウドシステムサービスを提供する者、もしくはそれらの提供者が一体となり、クラウド利用者に森林クラウドシステムサービスを提供する者を対象とする。

■森林クラウドシステムの利用を行う者（都道府県・市町村・林業事業体等の外部事業者）

外部事業者とは、森林計画作成や各種届出の申請など、自治体の林務に関して情報利用・連携・システムを利用する事業者を指しており、自治体の情報公開制度や Web での情報公開などのシステムについてはこのガイドラインの対象外とする。

2. 用語の定義

2-1. クラウドコンピューティング

ネットワーク、サーバ、ストレージ、アプリケーション、サービスなどの構成可能なコンピューティングリソースの共用プールに対して、便利かつオンデマンドにアクセスでき最小の管理労力またはサービスプロバイダ間の相互動作によって迅速に提供できるという、モデルのひとつである。（アメリカ国立標準技術研究所より）

2-2. ファイアウォール

組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。また
そのようなシステムが組みこまれたコンピュータ。

2-3. SLA（Service level Agreement）

サービスプロバイダや通信事業者が利用者に対して、一定以上のサービスの品質を保証する制度または契約。通信速度や利用可能時間などを定量的に指標化し、ある水準を下回った場合には、利用料金を減額することなどが規定される。サービス品質保証契約。

2-4. GIS（Geographic Information System：地理情報システム）

地理的位置を手がかりに、位置に関する情報を持ったデータ（空間データ）を総合的に管理・加工し、視覚的に表示し、高度な分析や迅速な判断を可能にする技術である。

2-5. BCM（Business Continuity Management)

包括的・統合的な事業継続のためのマネジメントのこと。

2-6. ディザスタリカバリ（disaster recovery）

建物単体での火災などの小規模なものから風水害、地震などの自然災害や不正侵入、テロなどの人為的なものなど比較的大きなものまで原因、規模にかかわらず広範囲であり、このような災害に対する予防・復旧の対策のこと。

2-7. 森林簿

都道府県が地域森林計画を樹立するために作成する基礎資料であり、森林の所在、面積、地況、林況等が記載されている。特に樹種、林齢等を正確に把握する事が必要であることから、5 年ごとに空中写真の撮影や造林実績の資料収集等を行ったうえで、森林簿の内容を修正している。

2-8. 森林計画図

森林法第５条の規定に基づいてたてられる地域森林計画の図面として、対象となる森林の区域を林班界及び小班界等により示すものであり、縮尺 1/5000 で作成される。森林計画図は、所有権、所有界、面積等土地に関する諸権利及び立木竹の評価について証明する資料としては使用できない。

2-9. 森林経営計画

「森林所有者」又は「森林の経営の委託を受けた者」が、自らが森林の経営を行う一体的なまとまりのある森林を対象として、森林の施業及び保護について作成する 5 年を 1 期とする計画である。 一体的なまとまりを持った森林において、計画に基づいた効率的な森林の施業と適切な森林の保護を通じて、森林の持つ多様な機能を十分に発揮させることを目的としている。

2-10. 林地所有者台帳

森林の土地の所有者となった旨の届出が義務付けられ森林所有者情報等を把握するために市町村が更新、管理している台帳

2-11. 地籍調査

主に市町村が主体となって、一筆（※）ごとの土地の所有者、地番、地目を調査し、境界の位置と面積を測量する調査である。 「地籍」とは、いわば「土地に関する戸籍」のことである。

地籍調査が行われることにより、その成果は登記所にも送られ、登記簿の記載が修正され、地図が更新される。 また、固定資産税算出の際の基礎情報となるなど、市町村における様々な行政事務の基礎資料として活用される。 なお、地籍調査は、国土調査法に基づく「国土調査」の１つとして実施される。

※ 土地の所有権等を公示するために、人為的に分けた区画のこと。土地は「筆」（ひつ）という単位でカウントされる。

2-12. 森林クラウド・トラストフレームワーク

複数のクラウド事業者がそれぞれ ID 連携を行うことによって、ひとつのユーザ ID で安全に利用できる枠組みのこと。

2-13. ID プロバイダ

ID 連携及び、アクセス権限・制御、不正アクセスの監視等の機能を有する事業者のこと。

3. 森林クラウドシステム事業者が講ずべき措置

森林クラウドシステムの構築にあたり森林クラウドシステム事業者が講ずべきセキュリティ対策について、クラウドシステム一般で求められるセキュリティ要件と、森林クラウドシステムに求められるセキュリティ要件に分けられる。

クラウドシステム構築におけるセキュリティ要件については、昨今では自治体向けクラウド・ASP の導入が進んでおり、関係各所からガイドライン・指針などが出されている。ここでは、クラウドシステム環境、データ管理環境、システム利用環境、森林システム構築におけるセキュリティ要件に整理した。

3-1. クラウドシステム環境におけるセキュリティ要件

クラウドシステム環境におけるセキュリティ要件を「技術的」、「物理的」、「組織的」に区分した。

3-1-1. 技術的セキュリティ対策

クラウドシステムの開発・導入・保守について、外部からの脅威に対して今ある最新の技術を効果的に導入しセキュリティ対策を施すことが必要である。

- ✓ 多重化などハードウェアの障害対策
- ✓ 開発環境・運用環境の分離
- ✓ 開発・導入に関する情報の機密性確保と適切な管理
- ✓ 不正プログラム対策ソフトウェアの導入と最新の状態の維持管理
- ✓ ソフトウェアのセキュリティパッチの適用
- ✓ ファイアウォール等外部からの不正アクセスの防止策の導入
- ✓ サーバ等システムの脆弱性判定とその対策
- ✓ 通信時の暗号化措置
- ✓ 脆弱性に関する情報の収集及びソフトウェアの更新
- ✓ 上記に限らず、適宜、ソフトウェアセキュリティに関する関連情報や脆弱性及び不正プログラム等に関する情報を参照しリスク管理を行うことが必要である。

3-1-2. 物理的セキュリティ対策

物理的・環境的な施設建物やサーバ機器等の可用性・安全性の確保に対する対策が必要である。

- ✓ 施設建物の耐震、免震構造であること
- ✓ 利用するサーバの設置場所が国内であること
- ✓ 非常用電源装置等の対策が施されていること

- ✓ サーバルームに消化設備等が装備されていること
- ✓ 物理的な入退管理がされている、従業員であっても関係者以外の入退が制限されていること
- ✓ 破壊侵入の防止、防犯監視等の対策がなされていること
- ✓ マルチテナントなど他のサービスと設備を共有する場合には、そのリスクを検討し、利用者へ説明を行う。またそのリスクを最小にするよう努めること。

3-1-3. 組織的セキュリティ対策

クラウド事業者は、開発・運営にあたり法令等を遵守した社内体制の整備と教育の実施を行う。また、森林クラウドシステム利用者の承認とアクセス制御を適切に行うことが求められる。

- ✓ 法令、規範の遵守
- ✓ システム開発・運営における責任者の明確化など、運用体制に関する規定の整備
- ✓ 開発・運営に関して外部委託を行う際の、外部委託事業者で委託内容に応じたセキュリティ対策が行われていることの確認
- ✓ ユーザ ID、アクセス権限等の適切な管理
- ✓ セキュリティインシデントやシステム障害などの事故対応計画の策定と周知

3-2. データ管理環境におけるセキュリティ要件

データ管理環境におけるセキュリティ要件では「データバックアップ」、「データ保管場所・期間」、「ディザスタリカバリ」に対策を区分した。

3-2-1. バックアップ対策

- ✓ データバックアップの適切なインターバルと実施タイミングの設定
- ✓ バックアップデータの適切な世代管理設定
- ✓ バックアップデータの多重化
- ✓ 定期的なバックアップ環境の確認と復元手順の確認

3-2-2. データの保管場所・保管期間

- ✓ 規程・契約等で定められた保管期間の厳守
- ✓ データの保管場所を国内とする
- ✓ 漏えい・流出時の予防対策として暗号化等の技術的措置
- ✓ 記録媒体等機器廃棄の際の、復元不可能な状態での情報の消去

3-2-3. ディザスタリカバリの対策

災害などによる被害からの回復措置、あるいは被害を最小限の抑えるための予防措置を

行う必要がある。「システムを災害から守る」のみならず、各種の障害は必ず起こりえるものと想定し、いかに効率よく迅速に復旧するかという点から災害対策を捉える。システム停止による利益の損失を最小限に抑える事を目的とする。

- ✓ 多地点でのバックアップデータの分散保管
- ✓ データおよびソフトウェアのポータビリティの確保
- ✓ 連絡先・報告事項を含む災害等緊急時の対応計画の策定

3-3. システム利用環境におけるセキュリティ要件

システム利用環境におけるセキュリティ要件では「アプリケーション管理」、「運用管理」、「ユーザ管理」に対策を区分した。

3-3-1. アプリケーション管理

クラウド事業者は安全かつ安定したサービス提供に努めなければならない。

- ✓ ソフトウェア、アプリケーションの定期的な脆弱性診断と対策の実施
- ✓ ソフトウェア、アプリケーションの変更履歴の管理
- ✓ 各種ログ、障害記録などの取得及び管理

3-3-2. 運用管理

サーバやネットワークからの不正アクセスや攻撃に対応する監視機能の整備を行い利用者に必要な情報の通知が迅速に実行できる体制整備が望ましい。

- ✓ セキュリティインシデントの通知、監視
- ✓ サーバ、ネットワークの監視
- ✓ 不正アクセスや不正使用の検知と記録の実施
- ✓ サービスの停止、障害時等の通知
- ✓ 利用者への相談窓口の設置
- ✓ SLA に基づくパフォーマンス監視

3-3-3. ユーザ管理

ユーザ ID およびアクセス権限の設定および通知を行い、利用者からの決定または変更通知に迅速に対応できる体制を整備する。

- ✓ サービス利用契約と SLA に基づく管理体制
- ✓ 利用者の特定と認証、利用者 ID およびアクセス権限等の通知
- ✓ 定期点検、障害対応等によるサービス停止の通知

3-4. 森林システム構築におけるセキュリティ要件

森林システムの構築では、一般的なバックオフィス業務システムのクラウド化とは異な

ったセキュリティ要件があり、それらに対してセキュリティ対策を講ずる必要がある。
森林クラウドシステムの構築・導入は多くの場合自治体を対象としており、森林システムの特徴的なセキュリティ要件は、森林システムでの情報の取り扱い、森林システムに特有の利用形態・利用環境、自治体向けクラウドシステム構築におけるセキュリティ要件に分けられる。

3-4-1. 森林システムでの情報の取り扱い

森林システムで取り扱う情報には利用に制限が付されるものがあり、その根拠となる法令・規則に従って取り扱う必要がある。

- ✓ 伐採届、所有者変更届など林務に関する庁内情報の利用
- ✓ 民間事業者が作成した空中写真・地図など、他社が著作権を有する情報
- ✓ 森林簿、森林計画図など、森林情報取扱要領の対象となる情報
- ✓ 個人情報保護条例の対象となる情報
- ✓ 測量法における、基本測量成果の複製・使用

3-4-2. 森林システムを用いた情報連携

多くの都道府県で森林システムを用いて庁内外との情報の連携が行われており、システム及びデータへのアクセス管理を適切に行うなどのセキュリティ対策が求められる。

- ✓ 庁内の統合型 GIS や台帳管理システム等との情報連携の際に、森林情報の閲覧・編集などのアクセス権限を適切に設定・管理する。
- ✓ 庁内の他のデータベース等との突合処理について、予め定められたタイミングで適切に行う
- ✓ 本庁と支局など出先機関との間での情報連携・共有の際に、アクセス権限を適切に設定・管理すると共に、業務に必要な情報を選択的に取り扱う等ネットワークへの負荷を考慮する
- ✓ 都道府県・市町村間など外部自治体での情報連携の事例情報の共有・提供の際に、外部自治体が取り扱ってよい森林情報のみを閲覧・編集するようアクセス権限を適切に設定する
- ✓ 林業事業体・森林組合など外部事業者・団体への森林情報の提供を行う際に、取り扱ってよい森林情報のみを閲覧・編集するようアクセス権限を適切に設定する、提供・公開用データベースを森林システムから分離するなど、外部からアクセス可能な情報を適切に管理する
- ✓ WebGIS を含む Web 上で森林情報を一般に公開・提供する際には、Web 公開用の森林情報データベースを森林システムから分離したものとする

3-4-3. 利用者と利用形態

森林システムは、台帳管理や計画作成など複数の目的に対応したシステムとなっており、利用者ごとに必要となる機能・情報が異なる事例がある。導入先自治体の業務、利用形態を調査、検討することが求められる。

- ✓ 利用者の違いに応じた適切なアクセス管理、例えば、外部利用者に対して、ネットワーク・サーバーを分離した環境とする、データのアクセス・編集権限を適切に設定する、不必要な権限を付与しない
- ✓ 利用者の違いに応じた適切なユーザ管理を行う。林業事業体など、特定の端末を複数人で用いる環境では、アカウントの共有を避ける、アカウントと利用者の紐づけを行う、アカウントを共有する場合には台帳等のシステム外に利用履歴を残す等、利用者を特定できるよう記録を残す
- ✓ 異なる自治体でクラウドシステムを共用する際に、各自治体のセキュリティポリシーや規定とクラウドシステムのセキュリティ対策に齟齬が無いことを確認する
- ✓ 外部情報との突合、情報公開のための処理など、定期的に行われる外部との情報連携については、処理を行う期間・タイミングを定め、適切に監視を行う、例外的な持出し・持ち込みを防ぐ
- ✓ 利用環境の違いに対応したユーザ管理およびアクセス管理、例えば、出先機関の特定業務にのみ機能・情報を制限したシステムとする、閲覧・印刷のみ可能とするなど
- ✓ 市町村・林業事業体など、共有の電子メールアドレスを利用している環境では、ユーザ ID・パスワードの通知の際に電子メールを利用せず、郵便などによる通知を行うことで、ID・パスワードの開示先を把握することが望ましい
- ✓ 事業者が、複数の自治体と事業連携を行う場合など複数の森林クラウドシステムへのアクセス権限が必要となる際には、人的ミスやパスワードの使いまわしを避けるため、シングルサインオンなどの技術を用いるなど利用者の負荷軽減を行うことが望ましい

3-4-4. ・自治体向けシステムのセキュリティ対策

自治体向けクラウドシステムの場合では、特に自治体向けのセキュリティ対策を検討する必要がある。自治体向けシステムでは、自治体独自のセキュリティ基準により、より厳しいセキュリティ対策が求められる可能性がある。また、自治体によっては、ネットワーク環境や利用する端末について制約が発生する可能性がある。

- ✓ 導入先自治体における情報セキュリティ基本方針・情報セキュリティ対策基準等に基づき適切な取り扱いを行う
- ✓ 取扱う個人情報を特定し、個人情報保護条例・個人情報保護条例施行規則等に基づき適切な取り扱いを行う
- ✓ 森林クラウドシステムで利用するネットワーク環境や利用する端末について、回線

帯域や外部情報へのアクセスなど、業務に求められる機能を実現できるものかを検証する

3-4-5. 新たな自治体情報セキュリティ対策の抜本的強化について

平成 29 年 7 月から開始されるマイナンバー本格利用と情報提供ネットワークに備え、平成 27 年 12 月に総行情第 77 号「新たな自治体情報セキュリティ対策の抜本的強化について」により総務大臣より全自治体に対してセキュリティ対策の通知があった。

この中では、自治体の情報システムを「①マイナンバー利用事務系」「②LGWAN 接続系」「③インターネット接続系」の三つに整理し、それぞれに以下の対策が示されている。

① マイナンバー利用事務系においては、 原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民（個人）情報の流出を徹底して防ぐこと。
② マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、財務会計など LGWAN を活用する業務用システムと、Web 閲覧やインターネットメールなどのシステムと の通信経路を分割すること。なお、両システム間で通信する場合には、ウィルスの感染のない無害化通信を図ること（LGWAN 接続系とインターネット接続系の分割）。
③ インターネット接続系においては、都道府県と市区町村が協力して インターネット接続口を集約した上で、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を講じること。

これらの森林クラウドシステムへの影響について、以下にまとめた。

① マイナンバー利用事務系について

森林システムを利用する業務で取扱う情報のうち、マイナンバーに関連する情報として林地台帳等での地方税情報の庁内利用が該当する。

地方税情報における課税台帳の所有者情報を、林地台帳の整備等林務で利用する際には、課税台帳を管理する課税管理システムではマイナンバーを直接的に取り扱うことはないこと、また林地台帳へ提供する情報は所有者情報及び地番情報であることから、林地台帳の取り扱いはマイナンバー利用事務系に該当せず、またマイナンバーを取り扱うことはないと考えられる。

しかし、課税台帳から林地台帳の所有者情報を転記する際には課税管理システムを用いて所有者情報を得ることになり、この処理に関するシステムを構築する際には、課税台帳から転記する所有者情報のみを抽出する、ネットワークの分離を行うなど、マイナンバー利用事務系と林地台帳を取り扱うシステムを完全に分離した取り扱いを検討する必要があると考えられる。

② LGWAN 接続系について

総務大臣通知では、LGWAN 接続系とはマイナンバーによる情報連携に活用される LGWAN 回線・端末を指しており、LGWAN 接続系とインターネット接続系の分離について「自治体情報セキュリティ強化対策事業実施要領」を参照することが求められているが、具体的な手法は指定されておらず、自治体の現状のネットワーク環境や業務を踏まえた効果的な対策を取る必要がある。

森林システムの特徴として、国土地理院や民間事業者の提供する API を用いて外部から地図などを取得する場合や、森林組合などの外部事業者が森林システムを利用する場合など、利用者や利用目的によって LGWAN ではなくインターネット接続を必要とする可能性がある。また、出先機関などで LGWAN 回線環境にネットワーク帯域などの制約があり、航空写真などの大きなデータを利用することができない可能性がある。導入検討を行う際には、機能・性能に制限が発生する可能性、事前に求める機能要件、使用する端末数、などを業務に基づき明確にする必要がある

これらを踏まえ、LGWAN 接続系で行われている庁内情報の利用や手続き業務と、森林クラウドシステムでそれらと連携する利用目的や取り扱う情報をあらかじめ特定し、森林クラウドシステムで LGWAN 接続を行う場合のコストなど課題を踏まえ、自治体内部の情報セキュリティに関する規定に基づき判断を行う必要がある。

③ インターネット接続系について

インターネット接続系について、インターネット接続を都道府県に集約することで、リスクとなる無害化通信などセキュリティ対策が必要となる箇所を減らし、リスクの低減と市区町村のセキュリティ対策コストを低減することが求められている。

セキュリティクラウドの構築検討では、インターネット接続系の指すものとして、E メール送受信、Web 閲覧、OS・セキュリティ対策ソフトなどのアップデートデータ受信などが想定されており、WebGIS などの高度な利用については個別検討が求められている。

森林クラウドシステムの導入には、LGWAN 接続系で取扱う内部向け森林システムと別にインターネット接続による外部授業者向けシステムを構築し、無害化処理を行うことで情報連携を行う方法、また逆に特定の LGWAN 接続系から分離したインターネット接続端末を森林クラウドシステム専用端末とする方法などが考えられる。いずれの手法にしても LGWAN 接続系とインターネット接続系で一部重複した整備が必要となるため、森林クラウドシステムの利用目的・利用端末数を明らかにし、導入コストを踏まえた導入検討が必要になる。

4. 森林クラウドシステム利用者が講ずべき措置（都道府県・市町村・林業事業体等）

森林・林業事業に携わる者が森林クラウドシステムを利用する際に講ずべき対策について、森林クラウドシステム構築・導入、管理・運用、利用の段階に整理した。

4-1. 森林クラウドシステム構築・導入

森林クラウドシステムの構築・導入の際には、森林クラウドシステムの利用者・利用形態と、利用する情報と用途を特定する必要がある。

4-1-1. 利用者と利用形態の特定

森林クラウドシステムの利用者・利用形態を特定し、必要となるアクセス管理・ユーザ管理方法を検討する。利用者と利用形態の検討事項として以下が挙げられる。

→クラウド調達のガイドライン参照

- ✓ 森林クラウドの利用者：行政機関（国・都道府県・市区町村）、民間事業者・森林組合等外部組織
- ✓ 利用する環境：庁内・庁外の違い、LGWAN 接続による自治体の利用、IP-VPN や専用線などを用いた外部からの利用、モバイル回線を用いた現地での利用
- ✓ 利用する端末：他の業務で利用する PC、森林システム専用端末、複数人で共有する端末、タブレット等モバイル機器

4-1-2. 利用する情報と用途の特定

利用する情報と用途を特定し、森林情報の閲覧・編集について業務に応じた権限を設定する必要がある。

- ✓ 各種森林計画の策定など計画業務
- ✓ 政策立案のための調査検討
- ✓ 森林資源情報の整備・管理
- ✓ 伐採届、林地開発など行政手続き
- ✓ 集約化・林地取得の検討

4-2. 森林クラウドシステムにおける SLA の合意

3. 森林クラウドシステム事業者が講ずべき措置については、森林システムを構築・提供する事業者として留意すべき点をまとめたものである。それらの具体的な実施、サービスの実現に用いるインフラ、クラウド環境やシステムの管理運用方法と品質については、別途、利用者との間で要件と責任分界点を明確にし、SLA（Service level Agreement）を結ぶことが望ましい。

【都道府県・市町村・林業事業体】

SLA（Service level Agreement）とは、クラウド事業者とクラウド利用者(都道府県、市町村、林業事業体が対象となる)との間で、森林クラウドシステムが提供するサービスの契約を締結する際に、提供するサービスの範囲・内容及び前提となる諸事項を踏まえた上で、サービスの品質に対する要求水準を規定するとともに、規定した内容が適正に実現されるための運営ルールを両者の合意として文書化したものであり、森林クラウドシステムを導入する時は、SLA の合意契約を締結する事が望ましい。
SLA の構成要素を表 1 に示す。

表 1　SLA の構成要素

SLAの構成要素	解　説
サービスメニュー	SLAの対象となるサービスの種別と各サービスの機能要件のことです。 サービスの範囲などもここに含めることになるので、できるだけ具体的な記述が求められます。
サービス要件	サービスメニューごとに規定される定量的又は定性的要件で、後の評価やパフォーマンス設定の前提となる要件になります。
SLA評価項目	サービスメニューに対応する品質を定量的に設定・評価する項目で、提供されているサービスについて評価する項目となるので、できるだけ測定が可能なものにする必要があります。
SLA設定値	SLA評価項目の具体的な値のことです。これには、保証値と目標値の二つがあります。保証値は、いわば守らなくてはいけない値です。一方で目標値は、あくまで目標であり、必ずしも守らなければならないものではありません。
報告要件	報告の周期や方法のほか、SLA測定方法についてもここで定義することが望ましいといえます。
ペナルティ	対象とするサービスメニューやサービス要件、SLA設定値等が達成されなかったときの影響度や未達の度合いなどによって、考慮すればよいかと思います。
その他	免責やSLAに関し委託元と委託先の義務についても記述されると望ましいでしょう。

（出典：総務省　自治体 CIO 育成研修）

SLA を設定する対象の判断基準は以下 4 つにあると考えられる。
① 委託するサービスの重要性はどの程度のものか
② SLA の内容を文書化できるか
③ SLA を設定した場合の測定が可能であるか
④ SLA を設定した場合、その内容を達成できる環境があるか
SLA を設定する対象の例を表 2 に示すが、あくまで例であるため、上記判断基準をもとに森林クラウドシステムの利用者で考慮することが望ましい。

表 2　SLA を設定する対象例

対象	項目	内容
セキュリティ	ファイアウォール	不正アクセスを検出するまでの時間 不正アクセス検出後、通知までの時間
	ウイルス対策	パターンファイル更新までの時間 ウイルススキャンにかかる時間
	情報提供	最新セキュリティ情報を提供する間隔 最新セキュリティ情報を提供する件数
サポートデスク	ヘルプデスク	受付時間 解決率 電話がつながらない確率、時間 コールバックまでの時間
保守	障害対策	対応時間 復旧時間 原因判明率 原因究明までの時間
アプリケーション	アプリケーションの稼働	サービス提供時間 処理完了までの時間 帳票出力までの時間 稼働率 同時接続可能数 バックアップに要する時間 バックアップタイミング リストアに要する時間 アプリケーション変更に要する時間
ネットワーク	ネットワーク管理	回線の種類 稼働率 伝送遅延時間 トラフィック管理
データセンター	中央監視	ID・パスワードの変更に要する時間 公的認証の取得状況 ログ収集の間隔 閾値の監視間隔
ストレージ	データ管理	世代管理 ディスク負荷率 容量の監視間隔 データベースバージョンアップの方法 バックアップ媒体と保管世代数 バックアップタイミング バックアップの保存期間 データリカバリの復旧時間

（出典：総務省　自治体 CIO 育成研修）

相互間で SLA を設定する対象の決定後は、指標の設定をおこなう。
指標は、具体的な数値とすることが望ましいが、場合によっては「あり/なし」で判断することになると思われる。

SLA の導入に関するメリットとデメリットについて以下の通り整理する。

4-2-1. 導入のメリット

- ✓ サービスレベルの質が向上できる、SLAを設定することで、提供されるサービレベルが明確になり、それを継続的に見直すことで、質の向上が可能となる。
- ✓ サービス全体の水準が統一化できSLAを設定・検証し、それを展開することで、都道府県や市町村、森林組合、その他林業事業体で同じサービスの水準が決定できる。
- ✓ サービスが提供されない場合の保険となり、SLAが未達の場合は、場合によってペナルティが与えられる。

4-2-2. 導入のデメリット

- ✓ 管理するための確認事項やSLAを運用するための様々な確認事項があり、計画段階でも管理・考慮するべきことが多くなる。
- ✓ 管理するためのコスト増加や確認事項の増加は、結果的にコストに跳ね返ってくる。
- ✓ 森林クラウドシステム事業者もSLA策定など作業内容が増えるため、コスト増を要求することが一般的である。

4-3. 森林クラウドシステムに関するセキュリティポリシー・規定の策定

森林クラウドシステムの導入・運用の際に、森林クラウドシステム管理・運用者には，森林クラウドサービスに関連する新しい規程や管理策を策定し、既存の情報管理規程や情報セキュリティ基本方針と合致しているかをレビューすることが求められる。

管理・運用者は，クラウドサービスが情報セキュリティ基本方針に合致しない場合、原因を調査し、必要に応じて双方を是正することが望ましい。また、クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検することが望ましい。

森林クラウドシステムに関するセキュリティポリシー・規定に盛り込む具体的な内容については、総務省「地方公共団体における情報セキュリティポリシーガイドライン」[1]などを参照の上、情報管理者と調整の上作成することが必要である。

4-3-1. 端末・記録媒体の管理

森林クラウドシステムの導入・運用では、クラウドシステム利用端末及び森林情報を記録した媒体の管理を適切に執り行う必要がある。具体的には、以下に挙げる項目を含めた、クラウドシステムの利用端末の利用管理、及び森林情報の取り扱い管理を行う必要がある。

- ✓ ID・パスワードの管理
- ✓ 情報および端末の利用履歴の管理
- ✓ 職員等利用者の教育

[1] https://www.soumu.go.jp/denshijiti/jyouhou_policy/

- ✓ アクセス制御
- ✓ 事故報告体制の構築

4-4. データ管理環境におけるセキュリティ要件

森林クラウドシステムでは、データ管理環境におけるセキュリティ要件はクラウド事業者が対応している。データ管理について、利用者はクラウド管理者が定めた規定を順守すること、森林情報取扱規定、個人情報取扱指針など、取り扱う情報に応じた規定を順守しが求められる。また不要な複製を避けることでリスクを低減することが望ましい。

4-5. 森林クラウドシステム管理・運用におけるセキュリティ要件

森林クラウドシステム管理・運用におけるセキュリティ要件を「物理的」「組織的」「データ管理」「ユーザ管理」の観点から区分した。

4-5-1. 物理的セキュリティ対策

【都道府県・市町村・林業事業体】

- ✓ クライアント端末の破壊、防犯等の対策を施すことが望ましい。
- ✓ 台帳などによる端末の持出し管理を行うことが望ましい。

4-5-2. 組織的セキュリティ対策

【都道府県】

- ✓ 法令(個人情報保護条例を含む)・規範等の遵守および遵守状況の監督
- ✓ 森林クラウドシステム利用管理責任者を任命し、利用者 ID やアクセス権限等の認証および利用者の管理をおこなうこと。
- ✓ 運用規定・利用規定を定め、担当者への周知・教育を実施する。
- ✓ 適宜、システム利用環境と運用規程とが実務に合っているかを精査し、必要に応じて規程等の見直し、教育を実施する
- ✓ SLA の契約等、サービス内容、範囲等を森林クラウド事業者と合意していることが望ましい。
- ✓ 電子媒体の利用制限および保管場所等の手続きを明確にしておくことが望ましい。

【市町村】

- ✓ 法令(個人情報保護条例を含む)・規範等の遵守および遵守状況の監督
- ✓ 適宜、システム利用環境と運用規程とが実務に合っているかを精査し、必要に応じて規程等の見直し、教育を実施する。
- ✓ 森林クラウドシステム利用管理責任者を任命し、利用者 ID やアクセス権限等の認証および利用者の管理をおこなうこと。
- ✓ SLA の契約等、サービス内容、範囲等を森林クラウド事業者と合意していることが

望ましい。

- ✓ 電子媒体の利用制限および保管場所等の手続きを明確にしておくことが望ましい。

【林業事業体】

- ✓ 法令(個人情報保護法を含む)・規範等の遵守および遵守状況の監督
- ✓ 運用規定・利用規定を定め、担当者への周知・教育を実施する。
- ✓ 適宜、システム利用環境と運用規程とが実務に合っているかを精査し、必要に応じて規程等の見直し、教育を実施する
- ✓ 森林クラウドシステム利用管理責任者を任命し、利用者 ID やアクセス権限等の認証および利用者の管理をおこなうこと。
- ✓ SLA の契約等、サービス内容、範囲等を森林クラウド事業者と合意していることが望ましい。

4-5-3. データ管理

【都道府県】

- ✓ 都道府県は市町村や林業事業体に対して森林情報を電子媒体にて提供する場合があるため、万一の紛失や盗難等の対策にデータの暗号化またはファイルパスワード等の設定が必要である。
- ✓ 契約に基づくサービスレベルが利用実態と合っているか定期的に評価見直しをおこなうことが望ましい。
- ✓ クラウド事業者から通知されるアクセスログを適宜確認することが望ましい。

【市町村】

- ✓ 市町村は契約に基づくサービスレベルが利用実態と合っているか定期的に評価・見直しを実施することが望ましい。
- ✓ 都道府県、林業事業体に提供する手段が電子媒体である場合は、データの暗号化を施すか、又はパスワードの設定を施すようにする。
- ✓ クラウド事業者から定期的に提供されるアクセスログ・リストの確認を実施することが望ましい。(異常なアクセス回数やダウンロード・プリント等の確認)

【林業事業体】

- ✓ 林業事業体は契約に基づくサービスレベルが利用実態と合っているか定期的に評価・見直しを実施することが望ましい。
- ✓ クラウド事業者から定期的に提供されるアクセスログ・リストの確認を実施することが望ましい。(異常なアクセス回数やダウンロード・プリント等の確認)

4-5-4. ユーザ管理

【都道府県】

- ✓ 職員の人事異動や退職等による利用者登録やアクセス権限の追加・失効の認証手

続きやクラウド事業者への速やかな通知と担当者への認証通知を実施すること。利用者登録やアクセス権限の追加・失効等の手順を下図 1 に示す。

- ✓ 森林クラウドシステムの運用を確立するためには、クラウド事業者と都道府県間の利用者登録、アクセス権限等の情報が双方同一情報であること、常に最新であり、正確でなくてはならない。
- ✓ 外部からのアクセスを許可した場合、共有の電子メールアドレスを利用している環境に対して、ユーザ ID・パスワードの通知の際に電子メールを利用せず、郵便などによる通知を行うことで、ID・パスワードの開示先を把握することが望ましい

【市町村】

- ✓ 職員／従業者等の配属・人事異動・退職等でシステムのアクセス権限の追加・削除等が発生した場合は速やかに内部手続き完了の上、クラウド事業者に通知しなければならない。
- ✓ 森林クラウドシステム利用に係るアクセス権限の追加・変更が発生した場合は遅滞なく担当者に通知しなければならない。
- ✓ 市町村のシステム管理責任者は林業事業体にアクセス権限を与え「ID・パスワード」を通知する場合は郵送もしくは直接手渡し等とし、電子メールでの通知は禁止とする。

【林業事業体】

- ✓ 職員／従業者等の配属・人事異動・退職等でシステムのアクセス権限の追加・削除等が発生した場合は速やかに内部手続き完了の上、クラウド事業者に通知しなければならない。
- ✓ 森林クラウドシステム利用に係るアクセス権限の追加・変更が発生した場合は遅滞なく担当者に通知しなければならない。

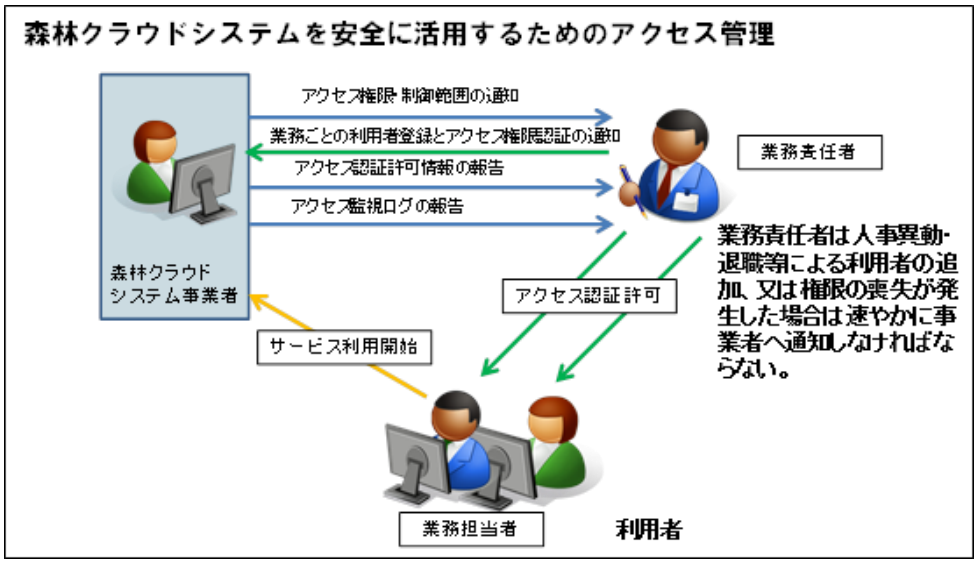


図 2　利用者登録とアクセス権限の認証フロー例

4-6. 参照すべき基準・ガイドライン等

- 経済産業省・独立行政法人情報処理推進機構（IPA）「情報システム調達のための技術参照モデル（ＴＲＭ）平成 25 年度版　自治体編」及び「クラウドサービス編」
  https://www.ipa.go.jp/osc/trm/
- 独立行政法人情報処理推進機構（IPA）「安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～」
  https://www.ipa.go.jp/security/vuln/websitecheck.html
- 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
  https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html
- 総務省「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」
  https://www.soumu.go.jp/denshijiti/jyouhou_policy/
- 総務省「地方公共団体における ASP･SaaS 導入活用ガイドライン」
  https://www.soumu.go.jp/denshijiti/asp_saas.html
- 総務省「平成 27 年度地方公共団体情報セキュリティ強化対策費補助金の第 1 回交付決定」及び総行情第 77 号「新たな自治体情報セキュリティ対策の抜本的強化について」
  https://www.soumu.go.jp/main_content/000402431.pdf
- 独立行政法人情報処理推進機構（IPA）「企業（組織）における最低限の情報セキュリティ対策のしおり」
  https://www.ipa.go.jp/security/antivirus/shiori.html

コラム

SLA を明確にするためのヒント

情報システムの導入・運用において、SLA（Service Level Agreement）の考え方を導入することの重要性は「4-2. 森林クラウドシステムにおける SLA の合意」で記した通りである。SLA については、主に基幹系の情報システムにおいては馴染み深いものであり、インターネット・サービス・プロバイダ（ISP）などの事業者では、あらかじめ SLA 要件をサービス利用規約に記載しているようなケースも多い。

森林クラウドシステムのような特定の業務を行うための業務システムにおいて SLA を締結し、情報システムを導入することはまだ一般的ではないかもしれない。しかし、これまでのように業務を行う事務所や事業所にサーバ（ハードウェア）を設置するのではなく、特にクラウドサービスを利用する場合などにおいては、SLA を締結することの重要性は大きく異なる。

SLA と言うと特別なことに感じられるかもしれないが、要は以下のポイントを明確化し、サービスを提供する事業者と、サービスを導入する利用者間で合意を得ることに尽きる。

【SLA 締結のポイント】

- 機能要件の明確化
  （機能の必要性）
  - その機能は、情報システムを導入予定の業務において必須のものか？

  （機能実現の確実性）
  - 導入予定の業務を支援する情報システムとして、その機能が機能しない場合に代替の方法によって業務が遂行できるか？
- 運用要件の明確化
  （運用のレベル）
  - そのシステムは、24 時間/365 日の運用が要求されるか？
  - メンテナンスのために利用が不可能となる時間はどの程度許容されるか？
  - システムを利用できない期間の代替手段はあるか？

情報システムを新たに導入・もしくは情報システムのリプレイスを行う場合は、上記のポイントを可能な限り明確にすることで、運用後のトラブルやサービス提供側と利用者側の誤解を回避することができ、円滑なシステムの運用の実現が可能となる。

5. 森林クラウドシステム利用におけるセキュリティ対策

システム利用環境におけるセキュリティでは利用者が森林クラウドシステムをクライアント端末で利用する際に考慮すべき点について区分した。

5-1. アプリケーション管理

森林クラウド事業者が安全かつ、安定したサービスを提供するための対策が講じられていることと、都道府県森林クラウド利用者は既にあるソフトウェアを利用することから管理策の対象から外すこととする。

5-1-1. 技術的セキュリティ対策

【都道府県（運用者)】

- ✓ クライアント端末の OS(例えば､Windows)のセキュリティパッチを適宜実施する、またサポートがなされている OS を利用すること
- ✓ ウィルス対策ソフト等が常に最新版に更新されていること
- ✓ クライアント端末に導入されている、または導入しようとするアプリケーションの管理をすることが望ましい

【都道府県・市町村（利用者)】

- ✓ クライアント端末の OS（例えば、Windows）のパッチ対応を適宜実施すること
- ✓ ウィルス対策ソフト等が常に最新版に更新されていること
- ✓ クライアント端末に導入されている、または導入しようとするアプリケーション(市販ソフトや無償アプリ等)の管理をすることが望ましい。
- ✓ 外部からのアクセスを許可した場合、共有の電子メールアドレスを利用している環境に対して、ユーザ ID・パスワードの通知の際に電子メールを利用せず、郵便などによる通知を行うことで、ID・パスワードの開示先を把握することが望ましい

【林業事業体】

- ✓ クライアント端末の OS（例えば、Windows）のパッチ対応を適宜実施すること
- ✓ ウィルス対策ソフト等が常に最新版に更新されていること

5-1-2. データ保管場所・期間の対策

【都道府県・市町村・林業事業体】

- ✓ 災害復旧対策は森林クラウド事業者が担っているがバックアップデータが多く存在することはより安全性が担保できるため､クラウド利用者側も適宜､バックアップを実施することが望ましい。

【都道府県】

- ✓ 市町村、林業事業体に提供する情報の保管と提供後の削除
- ✓ 森林簿や計画図の更新に合わせた保管・削除の期間・タイミングを明確にする。

【市町村】

- ✓ 都道府県から提供された情報の保管と利用後の削除
- ✓ 林業事業体から受領した情報の保管と利用後の削除

【林業事業体】

- ✓ 都道府県・市町村から受領した情報の保管と利用後の削除
- ✓ 不用意な情報の複製を行わない

5-2. 参照すべきガイドライン等

・ IPA 対策のしおりシリーズ

https://www.ipa.go.jp/security/antivirus/shiori.html

コラム

適切なセキュリティ対策を実施するためのヒント

新たに情報システムを導入する場合、担当者や情報システム部門の頭を常に悩ませるのが「情報セキュリティ対策」のレベルである。本ガイドラインにおいても、セキュリティ対策の重要性やポイントを列挙しているが、必ずしも全てのセキュリティ対策が必須というわけではない点に注意が必要である。

【ルール面の留意点】

そもそも、情報セキュリティ対策は、脅威を特定し、その脅威を排除するため・もしくは被害を最小限に抑えるために必要なリスク管理を行うことが重要である。ほとんどの場合は、各自治体において「情報セキュリティ規程」もしくはそれに準ずる何らかのルールが存在するはずであるから、導入先の自治体のルールを守ることが大原則となる。

組織における情報セキュリティ規程は、どのような情報システムでも適用できるよう、一般的かつ抽象的に書かれているか、逆に導入済みの特定の情報システムにおけるセキュリティ要件をもとに決められているようなケースでは、内容に偏りがあるような場合もある。森林クラウドシステムを導入する際は、導入先の組織における情報セキュリティ規程の内容をあらかじめ確認し、必要に応じて既存の情報セキュリティ規程の改訂をも考慮すべきである。したがって、組織内の情報システム部門担当者も巻き込んだ導入プロジェクトを実施することが望ましい。特に、クラウド形態の情報システムの導入が初めてというようなケースでは、既存の C/S 形式の情報システムの運用形態とは大きく異なるシステムとなるため、情報システム部門の理解を得ながら進めることは効果的である。

【技術面の留意点】

勿論、運用上の人員確保や情報システム構築時の予算規模が潤沢であれば、万全なセキュリティ対策を施すことでセキュリティリスクを最小限に抑えることが可能であるが、そのようなケースは稀である。したがって、実際にはセキュリティ対策に優先順位をつけ、よりプライオリティの高い対象に対してセキュリティ対策を施すこととなる。また、高度なセキュリティ対策を導入することで、情報システムのパフォーマンスが低下する場合もあるという点にも注意が必要である。

セキュリティ対策の対象を明確化し、優先順位をつけ、コスト面やパフォーマンス面での効果のバランスも考慮したセキュリティ対策を取捨選択することが、導入後の運用まで見据えたセキュリティ対策として有効かつ効果的なアプローチである。

6. 森林クラウドシステムに係る個人情報

森林クラウドシステムで有する個人情報の扱いを森林クラウド事業者と森林クラウド利用者に区分した。また、森林クラウドシステムでは自治体の持つ個人情報を含んだ森林情報を森林クラウド事業者の管理するクラウド環境へ預けることになる。また、森林クラウドを通じた森林情報の第三者提供を行うことで、森林情報のより高度な利活用が考えられる。そこで、個人情報の第三者提供における制度・手続きについて検討を行った。

6-1. 森林クラウドシステムにおける個人情報の該当性

① 森林クラウドシステムにおける個人データ

- ✓ 森林簿

  森林簿には森林所有者名及び大字、字、地番、「在村・不在村」が存在する。

- ✓ 森林計画図

  地図上に地番が標記されている場合がある。

- ✓ 林地所有者情報

  所有者名、住所、連絡先、土地取得日、地番、面積等

- ✓ 地籍調査情報(地籍簿、地籍図)

  所有者名、地番、面積、

都道府県は森林簿、森林計画図を個人情報ファイルとし、市町村はそれ以外に林地所有者台帳、地籍調査情報を個人情報ファイルとしている。

又、一部の都道府県、市町村によっては、所有者名、地番以外にも、「大字、字、林相」も個人情報の扱いとしているところがある。

② 森林計画図の個人情報の該当性

「地理空間情報の活用における個人情報の取扱いに関するガイドライン（地理空間情報活用推進会議平成 22 年 9 月）」3.1 地理空間情報における個人情報保護の考え方（1）地理空間情報に係る個人情報該当性では、地番や住居番号等の特定の土地や建物の所在を示す地理空間情報に関しては、一般に何人も閲覧等が可能な不動産登記情報や市販の住宅地図と照合することにより特定の個人を識別することができる傾向にある。

そのため、地番や住居番号等の特定の土地や建物の所在を示す地理空間情報であって、他の情報と照合することで特定の個人が識別できることから基本的に個人情報に該当すると位置づけている。

6-1-1. 対象となるクラウド利用者の個人情報保護に関する法令等

クラウド利用者は地方公共団体(都道府県・市町村)と民間事業者(林業事業体)が対象となることから遵守する法令・規範等がそれぞれ異なる。

① 都道府県、市町村

個人情報保護法（基本法)、個人情報保護条例、規範等

② 林業事業体

個人情報保護法、農林水産分野における個人情報保護に関するガイドライン等

6-1-2. クラウド利用者が講ずべき個人情報保護に関する体制

【都道府県・市町村】

- ✓ 個人情報保護条例及び内部規程の遵守
- ✓ システム管理責任者は、個人情報を適切に取扱うためにその業務に合わせたアクセス権限を与えなければならない。
- ✓ 実施機関は担当者が個人情報保護に関する知識等を一定のレベルに保つため定期的な教育を実施することが望ましい。
- ✓ 実施機関は法令・規範等の遵守状況を定期的に確認するため、個人情報保護、及び情報セキュリティに関する内部監査を実施する必要がある。

【林業事業体】

- ✓ 個人情報保護法及び農林水産分野における個人情報保護に関するガイドラインの遵守
- ✓ 法令を遵守するための個人情報管理規程の作成とその遵守
- ✓ システム管理責任者は、個人情報を適切に取扱うためにその業務に合わせたアクセス権限を与えなければならない。
- ✓ 事業者は担当者が個人情報保護に関する知識等を一定のレベルに保つため定期的な教育を実施することが望ましい。
- ✓ 事業者は法令・規範等の遵守状況を定期的に確認するため、個人情報保護、及び情報セキュリティに関する内部監査を実施する必要がある。

6-2. クラウド事業者の個人情報保護

森林クラウドシステムを提供する事業者（提供しようとする事業者）は、システム内での個人データの処理や保管等、利用者が個人データを利用するための安全性を確保しなければならない。

又、クラウド事業者はこの事業のために自ら取得している個人情報の安全性を確保しなければならない。

【クラウド事業者がこの事業で取得・利用している個人情報】

- ✓ クラウド利用者名、電話番号、メールアドレス、ID・パスワード、アクセス履歴、

【利用者が管理・利用している個人情報】

① 森林簿データ

・ 森林簿には森林所有者名及び大字、字、地番、「在所・不在所」が存在する。

② 森林計画図データ

・ 地図上に地番が標記されている場合がある

自治体によっては、地番を個人情報としている。

- ✓ 地籍調査データ
- ✓ 地籍簿、地籍図には、所有者名、地番、面積、図面上の位置

※林地所有者情報は、正しい所有者等を特定するために利用するものでシステム上では「森林簿データ」に反映される。

ただし、「市町村が利用者」の場合は過去の所有者も必要な時があるのでクラウド上で管理する場合があるので留意しなければならない。

6-2-1. クラウド事業者が講ずべき個人情報保護に関する体制

クラウド事業者は、自社が提供するシステム、又はサービスにおいて個人情報保護の重要性を認識し、以下の体制を整備しなければならない。

- ✓ 法令・規範等の遵守
- ✓ 個人情報保護方針の策定と公表
- ✓ 個人情報保護規定の策定および体制整備
- ✓ 相談・問合せ担当窓口の設置公表
- ✓ 目的外利用の禁止
- ✓ 第三者提供の禁止
- ✓ 運用管理担当者とシステム開発担当者とアクセスの権限を分ける
- ✓ 事故、障害等による漏えい事故発生の体制が整備されていること。
- ※ 個人情報の保護に関する体制が整備されていることを証明する ISMS、プライバシーマーク、ASP・SaaS 認証等の第三者認証の取得制度を有効に利用することも検討する

6-3. 森林クラウドシステムでの個人情報保護と利活用

クラウド利用者は法令・規範等を遵守し、個人情報の安全、且つ適切な取扱いをしなければならない。

6-3-1. 森林クラウドシステムにおける個人情報の利用

森林クラウドシステムは、地方自治体の保有する森林情報及び森林所有者情報を施業主体者である林業事業体と情報共有・利用することで森林整備に関する政策が達成できる環境を目指し整備している。森林・林業事業では個人情報を提供するのは、都道府県、市町村であり、利用する主体者は林業事業体となる。

例えば、森林経営計画を達成するためには、周辺の森林を一括して施業し森林・林業に関する業務の効率化を図る必要がある。　また、林業事業体は森林所有者に森林経営の提案をおこなうため、所有名、連絡先等の個人情報が必要となる。しかし、市町村では林業事業体への「第三者提供」が実現しているのは僅かである。

行政での個人情報を含む森林情報の公開・提供における留意点について、以下に第三者提供及びオープンデータ化の事例として以下にまとめる。なお、林地台帳制度に基づく「林地台帳・林地台帳地図」の公表・提供については、林野庁の定める「林地台帳整備マニュアル」及び「林地台帳運用マニュアル」に基づき実施することとなる。

6-3-2. 都道府県・市町村が保有する森林情報の第三者提供

森林情報の第三者提供を行う上で、第三者提供を行うための法的な根拠について調査を行った。森林法、及び地方自治体(1763 団体)の個人情報保護条例の調査から、いずれの地方自治体でも一定の条件で第三者提供が可能であることが確認できた。(詳細は平成 26 年度　森林情報高度利活用技術開発事業～森林クラウドシステム標準化事業～の報告書を参照)

【森林法の抜粋（一部該当箇所のみ)】

(農林水産大臣等の援助)

第 191 条　農林水産大臣及び都道府県知事は、全国森林計画及び地域森林計画の達成並びに市町村森林整備計画及び森林経営計画の作成及びこれらの達成のために必要な助言、指導、資金の融通のあっせんその他の援助を行うように努めるものとする。

2　市町村は森林の経営の受託又は委託に必要な情報の提供、助言又は、あっせんを行うとともに、市町村森林整備計画の達成並びに森林経営計画の作成及びその達成のために必要な助言､指導その他の援助を行うように努めるものとする。

(施業の集約化等の事業の推進)

第 191 条

5　国及び地方公共団体は、効率的な森林の経営を可能とするためには森林の施業の集約化等の事業の推進が重要であることに鑑み、これらの事業を担うことができる森林組合等の主体の育成、当該事業への支援その他の必要な措置を講ずるよう努めるものとする。

【某市の個人情報保護条例の抜粋（一部該当箇所のみ)】

第 7 条(利用及び提供の制限)

実施機関は、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

2　前項の規定にかかわらず、実施機関は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。

ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによっ

て、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。
(1) 本人の同意のあるとき、又は本人に提供するとき。
(2) 法令等に定めのあるとき。
(3) 個人の生命、身体又は財産の安全を確保するため、緊急かつやむを得ないと認められるとき。
(4) 出版、報道等により公にされているもので提供することが適当であると認められるとき。
(5) 実施機関の内部で利用し、又は他の実施機関、国、独立行政法人等、他の地方公共団体若しくは地方独立行政法人に提供する場合で、事務に必要な限度で使用し、かつ、使用することに相当の理由があると認められるとき。
(6) 前各号に掲げる場合のほか、審査会の意見を聴いた上で、公益上の必要その他の相当の理由があると実施機関が認めて利用し、又は提供するとき。

第8条 (オンライン結合による提供の制限)
実施機関は、オンライン結合(通信回線を用いて実施機関が管理する電子計算機と実施機関以外のものが管理する電子計算機を結合し、実施機関の管理する保有個人情報を実施機関以外のものが随時入手し得る状態にする方法をいう。以下同じ。)により保有個人情報を提供するときは、個人の権利利益を不当に侵害することがないように努め、法令等に基づく場合を除き、あらかじめ審査会の意見を聴かなければならない。
2 実施機関は、前項の規定により審査会の意見を聴いたオンライン結合による保有個人情報の提供の内容を変更するときは、あらかじめ審査会の意見を聴かなければならない。

第9条 (保有個人情報の提供を受ける者に対する措置要求)
実施機関は、実施機関以外のものに対して保有個人情報を提供する場合において、必要があると認めるときは、提供を受けるものに対し、提供に係る個人情報について、その利用の目的若しくは方法の制限その他必要な制限を付し、又はその漏えいの防止その他の個人情報の適切な管理のために必要な措置を講じることを求めなければならない。

第10条 (安全確保の措置)
実施機関は、保有個人情報の管理にあたっては、個人情報の漏えい、滅失及びき損の防止その他の保有個人情報の適正な管理のために必要な措置を講じなければならない。
2 実施機関は、個人情報を取り扱う事務の利用目的に照らし、保有の必要がない又は保有の必要のなくなった保有個人情報を確実に、かつ、速やかに廃棄し、又は消去しなければならない。ただし、歴史的若しくは文化的な資料又は学術研究用の資料として保存されるものについては、この限りでない。

市町村は森林法及び林野庁長官通知をもって市町村の個人情報保護条例にある「利用及び提供の制限」の例外措置が適用できると考えられる。

(5)　実施機関の内部で利用し、又は他の実施機関、国、独立行政法人等、他の地方公共団体若しくは地方独立行政法人に提供する場合で、事務に必要な限度で使用し、かつ、使用することに相当の理由があると認められるとき。

(6)　前各号に掲げる場合のほか、審査会の意見を聴いた上で、公益上の必要その他の相当の理由があると実施機関が認めて利用し、又は提供するとき。上記の条件にあてはめて実施機関内部の利用及び第三者提供の承認を得ることが望ましい。

承認手順例および第三者提供先の評価基準と評価手順例を図 3　第三者提供の例外措置と提供先の評価に関する承認手順に示す。

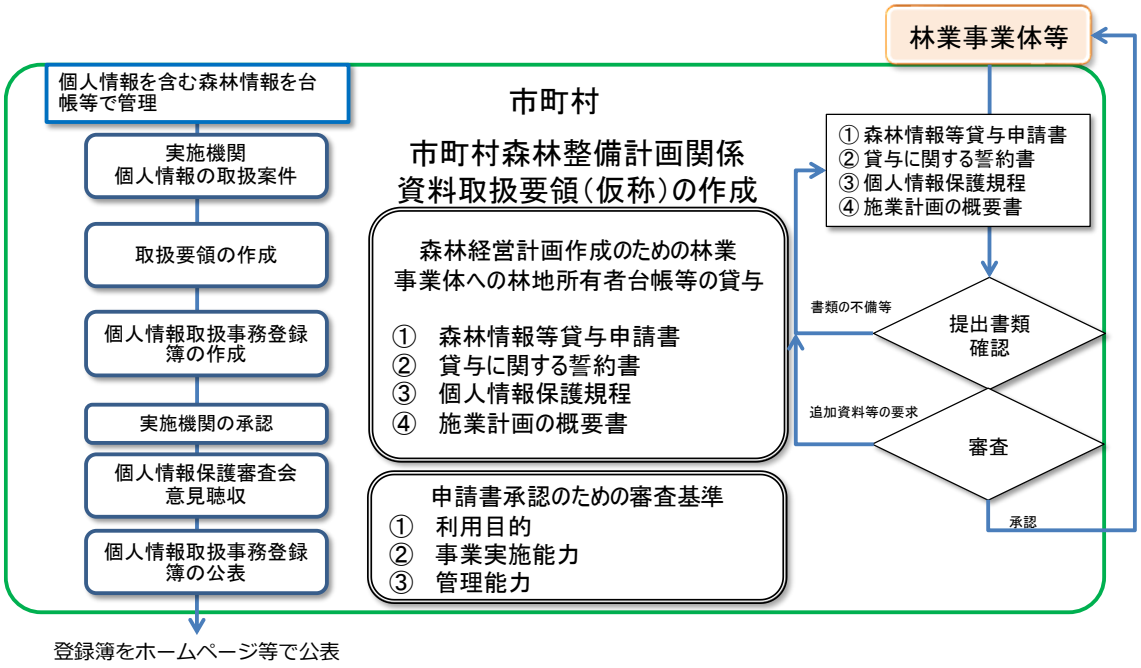


図 3　第三者提供の例外措置と提供先の評価に関する承認手順

【第三者提供に関する手順】

① 実施機関の内部利用に関する承認を得る
② 所有者情報を含む森林情報の取扱要領の作成
③ 第三者提供先の評価基準作成
④ 森林情報の第三者提供に関する案件の伺作成・提出
⑤ 個人情報保護審議会の意見を聴いた上で実施機関長が承認

【第三者提供先の評価基準と評価手順】

(林業事業体の提出書類)

- ✓ 林地所有者台帳等貸与申請書
- ✓ 誓約書
- ✓ 個人情報保護規程
- ✓ 施業計画の概要書

(評価基準)

- ✓ 書類審査
- ✓ 利用目的
- ✓ 事業実施能力
- ✓ 管理能力

コラム

個人情報保護に過剰反応しないためのヒント

個人情報保護法が施行されたのは平成 17 年（※行政機関向けの「行政機関個人情報保護法」も同じ）であり、以後社会的にも「個人情報とは保護すべきものである（保護されなければならない）」という認識が浸透してきた。しかしながら、個人情報保護法の浸透が必ずしも正しく進んできたわけではない、という点についても注意深く考慮する必要があるだろう。

たとえば、代表的な例として、学校の緊急連絡網（クラスごとの電話番号のリスト）が作成されなくなったことなどが挙げられるが、緊急連絡網を作成すること、それを関係者に配布すること事態は法規制上全く問題がなく、まさしく過剰反応の一例であると言えよう。

緊急連絡網の事例は代表的なものであるが、行政の行う業務においても、類似するようなケースが生じていないだろうか？個人情報保護法は事業者法であり、地方自治体には行政機関個人情報保護法が適用されるが、両者にはそれほど大きな違いはなく、あるとすればマイナンバーの取扱い程度であろう。両者とも、取り扱う個人情報には大きな差はない。差があるとすれば、行政機関の場合は取り扱う個人情報の量や場面が圧倒的に多いという点くらいである。また、事業者が収集する個人情報は事業者が行うビジネス上必要であるという点に対し、行政機関が収集し、取り扱う個人情報は「法令で定められた行政業務を行うため」という点が大きく異なる点である。

森林管理等の業務で個人情報を取り扱うようなケースであっても、それは同様である。森林管理等で個人情報を取り扱う必要があるのであれば、各自治体が定める個人情報保護条例に基づき、適切に取り扱うだけである。利用目的の明確化の原則や目的外利用の禁止の原則の遵守は勿論重要であるが、組織の内部で取り扱う情報の機密性という視点から見れば、個人情報と同等もしくはより厳しい管理下に置かれるべき情報は少なくない。例えば、企業で言えば取引先との機密保持契約に含まれる情報は外部には絶対に漏らすはずはなく、法令遵守に関係なく厳重に管理されるはずである。

このことは、個人情報を取り扱う上でも非常に重要なヒントとなる。法令遵守は勿論当たり前のことであるが、「なぜ、その情報を厳重に管理しなければならないのか」ということを考えれば、自ずとその管理方法やセキュリティ対策は決定するはずである。その情報が保護すべき対象である理由を理解することは、対象のデータが個人情報であるか否か、ということとは関係なく、適切な保護の方法を導き出すには有効なアプローチである。

【実践編】

7. マネジメントシステムの導入

本ガイドラインに書かれている情報セキュリティ対策や個人情報保護対策は、全て一般的な原則をもとに森林クラウドシステムに応用したものである。これらの原則を、より実践に近づけるための一つの手法として、情報セキュリティや個人情報保護を組織の中でルール化し、運用する「マネジメントシステム」という方法がある。

7-1. マネジメントシステムとは

マネジメントシステムの多くは、ISO（国際標準化機構）やJIS（日本産業規格）において「規格」として発行されている。たとえば、ISO 9001（品質マネジメントシステム）やISO 14001（環境マネジメントシステム）などは、国内でも多くの企業が実践しているマネジメントシステムの代表例である。

マネジメントシステムは、組織が目的を達成するために様々な内部規定を決め、それをそのとおりに運用するための管理体系である。ここには、規程や手順、それらを実際に運用するための責任や権限の体系も含まれる。

（参考：ISO 9001 における「マネジメントシステム」の定義）

方針、目標及びその目標を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素。

さらに、マネジメントシステムの特徴として一般的によく知られているのが、いわゆる「PDCA サイクル」と呼ばれる継続的改善手法である。

Plan（計画）	組織が設定した目標を達成するために、実施計画を作成する。
Do（実行）	実施計画に基づき、計画や規程通りに業務を実行する。
Check（評価）	実行した/実行中の業務が、計画や規程通りに行われた/行われているのかを評価する。
Action（改善）	評価結果をもとに、不備の有無を確認し、必要に応じて是正処置を行い、実施計画にフィードバックする。

7-2. マネジメント規格の概要

マネジメント規格とは、上記の ISO 9001 での定義の通りであり、ここで言う「方針」「目標」などが情報セキュリティであれば、情報セキュリティ対策のためのマネジメントシステム構築ができることになる。その際に参考になるのが、要求事項やガイドライン等を示したマネジメントシステム規格である。マネジメントシステム規格は殆どの場合以下の構成で書かれている。

（参考）一般的なマネジメント規格の目次構成（JIS Q 9001 の例）

1. 適用範囲	7. 支援
2. 引用規格	8. 運用
3. 用語及び定義	9. パフォーマンス評価
4. 組織の状況	10. 改善
5. リーダーシップ	附属書
6. 計画	参考文献

1. 適用範囲、2. 引用規格、3. 用語及び定義

これらの項目は、通常どのISO規格やJIS規格でも書かれている一般的なものである。

1. 適用範囲：
   当該規格の適用範囲が定義される。適用範囲とは、規格が規定している対象や制限の範囲のことであり、規格を参照する特定の読者などを想定している場合もある。その他、特定の事業分野、業界や製品等が限定される場合もある。
2. 引用規格：
   他の規格を引用する部分がある場合は、ここにその規格が列挙される。
3. 用語及び定義：
   「マネジメントシステム」のように、規格で取扱う一般的ではない用語について定義がされている。

4. 組織の状況

マネジメントシステムを構築・運用しようとする組織に対する要求事項が規定されている。マネジメントシステムを構築・運用する組織はこのようなことを実施しなければならない、ということが書かれている。

5. リーダーシップ

組織がマネジメントシステムを構築・運用するにあたり、組織を統率する人物やマネジメントする人物に対する役割や権限について規定されている。

6. 計画

マネジメントシステムを構築・運用するにあたり、自らが運用するマネジメントシステムをどのように設計し、どのような実行計画のもとに運用すべきかが規定されている。

7. 支援

マネジメントシステムを構築・運用するために必要な様々な資源（人的リソースや必要となる資材、技術などのすべて）について、それらをどのように採用し、維持するかについて書かれている。

8. 運用

構築したマネジメントシステムを継続的に運用するために必要な事項について規定されている。

9. パフォーマンス評価

マネジメントシステムの運用状況を自己評価するための手法について規定されている。具体的には、内部監査等に関する要求事項が書かれている。

10. 改善

パフォーマンス評価の結果、規格の要求事項を満たしていなかった場合、どのようにそれを改善し、マネジメントシステムを継続的に運用すべきかが規定されている。

附属書及び参考文献

多くの場合、規格には「附属書」が付属しており、本文を補足する内容が規定されていたり、参考となる情報が示されている。

7-3. 情報セキュリティマネジメントシステム（ISMS）

情報セキュリティ分野に特化したマネジメントシステムとしては、情報セキュリティマネジメントシステム（Information Security Management System：以下、ISMS）が知られている。ISMS は、ISO/IEC 27001 として ISO 規格が発行され、それを日本語化したものが JIS Q 27001 として発行されている（ISO 規格、JIS 規格ともに内容は同一であるため、以下 JIS Q 27001 と表記）。JIS Q 27001 では、組織が ISMS を構築・運用するための「要求事項」が規定されており、同規格の要求事項を満たすことで、組織内に適切な ISMS を構築・運用することができる。

JIS Q 27001 が要求しているのは、本ガイドラインでも書かれている情報セキュリティの一般的な原則について、組織内でそれらを実践するために必要となる具体的な方策であり、それらを継続的に運用するための事項である。

JIS Q 27001 には、上記 7-2. で示した内容のほか、情報セキュリティ特有の内容として、附属書が追加されている。附属書では、具体的なセキュリティ対策のための管理策が示されている。

【JIS Q 27001 附属書 A（規定）管理目的及び管理策】

項番	管理策	目的	管理策数
A.5 情報セキュリティのための方針群			
A.5.1	情報セキュリティのための経営陣の方向性	情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため。	2
A.6 情報セキュリティのための組織			

項番	管理策	目的	管理策数
A.6.1	内部組織	組織内で情報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため。	5
A.6.2	モバイル機器及びテレワーキング	モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。	2
A.7 人的資源のセキュリティ			
A.7.1	雇用前	従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため。	2
A.7.2	雇用期間中	従業員及び契約相手が，情報セキュリティの責任を認識し，かつ，その責任を遂行することを確実にするため。	3
A.7.3	雇用の終了及び変更	雇用の終了又は変更のプロセスの一部として，組織の利益を保護するため。	1
A.8 資産の管理			
A.8.1	資産に対する責任	組織の資産を特定し，適切な保護の責任を定めるため。	4
A.8.2	情報分類	組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするため。	3
A.8.3	媒体の取扱い	媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため。	3
A.9 アクセス制御			
A.9.1	アクセス制御に対する業務上の要求事項	情報及び情報処理施設へのアクセスを制限するため。	2
A.9.2	利用者アクセスの管理	システム及びサービスへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。	6
A.9.3	利用者の責任	利用者に対して，自らの秘密認証情報を保護する責任をもたせるため。	1
A.9.4	システム及びアプリケーションのアクセス制御	システム及びアプリケーションへの，認可されていないアクセスを防止するため。	5
A.10 暗号			
A.10.1	暗号による管理策	情報の機密性，真正性及び／又は完全性を保護するために，暗号の適切かつ有効な利用を確実にするため。	2
A.11 物理的及び環境的セキュリティ			

項番	管理策	目的	管理策数
A.11.1	セキュリティを保つべき領域	組織の情報及び情報処理施設に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。	6
A.11.2	装置	資産の損失，損傷，盗難又は劣化，及び組織の業務に対する妨害を防止するため。	9
A.12 運用のセキュリティ			
A.12.1	運用の手順及び責任	情報処理設備の正確かつセキュリティを保った運用を確実にするため。	4
A.12.2	マルウェアからの保護	情報及び情報処理施設がマルウェアから保護されることを確実にするため。	1
A.12.3	バックアップ	データの消失から保護するため。	1
A.12.4	ログ取得及び監視	イベントを記録し，証拠を作成するため。	4
A.12.5	運用ソフトウェアの管理	運用システムの完全性を確実にするため。	1
A.12.6	技術的ぜい弱性管理	技術的ぜい弱性の悪用を防止するため。	2
A.12.7	情報システムの監査に対する考慮事項	運用システムに対する監査活動の影響を最小限にするため。	1
A.13 通信のセキュリティ			
A.13.1	ネットワークセキュリティ管理	ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。	3
A.13.2	情報の転送	組織の内部及び外部に転送した情報のセキュリティを維持するため。	4
A.14 システムの取得，開発及び保守			
A.14.1	情報システムのセキュリティ要求事項	ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。	3
A.14.2	開発及びサポートプロセスにおけるセキュリティ	情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため。	9
A.14.3	試験データ	試験に用いるデータの保護を確実にするため。	1
A.15 供給者関係			
A.15.1	供給者関係における情報セキュリティ	供給者がアクセスできる組織の資産の保護を確実にするため。	3

項番	管理策	目的	管理策数
A.15.2	供給者のサービス提供の管理	供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため。	2
A.16 情報セキュリティインシデント管理			
A.16.1	情報セキュリティインシデントの管理及びその改善	セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取組みを確実にするため。	7
A.17 事業継続マネジメントにおける情報セキュリティの側面			
A.17.1	情報セキュリティ継続	情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければならない。	3
A.17.2	冗長性	情報処理施設の可用性を確実にするため。	1
A.18 順守			
A.18.1	法的及び契約上の要求事項の順守	情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。	5
A.18.2	情報セキュリティのレビュー	組織の方針及び手順に従って情報セキュリティが実施され，運用されることを確実にするため。	3

7-4. 個人情報保護マネジメントシステム

上記のISMS同様､個人情報保護に特化したマネジメントシステムも存在し､JIS Q 15001に要求事項が規定されている。ISMS（JIS Q 27001）とは異なり、JIS Q 15001 はISO規格を日本語化したものではなく、日本産業規格（JIS）のみが存在している。特徴としては、日本の個人情報保護法に沿って作成されており、同法を遵守しつつ、適切な個人情報保護を実践できる点である。

JIS Q 27001と同じく、JIS Q 15001 も一般的なマネジメントシステム規格と同じ構成となっており、個人情報保護特有の内容として、以下の附属書を有している。

【JIS Q 15001 附属書A（規定）管理目的及び管理策】

項番	管理策	目的	管理策数
A.3.1	一般	個人情報保護マネジメントシステムの運用を行うため。	1
A.3.2	個人情報保護方針	個人情報保護の理念を明確にし，公表するため。	2

項番	管理策	目的	管理策数
A.3.3	計画	個人情報の取扱いに関する計画を策定するため。	7
A.3.4	実施及び運用	運用段階において個人情報の取扱いを行うため。	24
A.3.5	文書化した情報	文書化した情報を作成・維持するため。	3
A.3.6	苦情及び相談への対応	苦情及び相談に対応するため。	1
A.3.7	パフォーマンス評価	パフォーマンス評価を実施するため。	3
A.3.8	是正処置	是正処置を実施するため。	1

【JIS Q 15001 附属書 B（参考）管理策に関する補足】

附属書 A の各々の管理策について、詳細な説明が記載されている。

【JIS Q 15001 附属書 C（参考）安全管理措置に関する管理目的及び管理策】

JIS Q 27001 における附属書 A の管理策と同じ項目としながら、目的を情報セキュリティではなく個人情報保護とした管理策群を規定している。

コラム

マネジメントシステム認証制度の活用

マネジメントシステム規格の多くは、規格の要求事項に適合しているかどうかを第三者が審査し、証明書を発行する「認証制度」が存在する。大手企業の Web サイトやパンフレットなどに「ISO 9001 認証取得」「ISO 14001 認証取得」などと明記しているのを目にすることも少なくないだろう。

マネジメントシステム規格の要求事項には、内部監査を実施し、自らが運用するマネジメントシステムをレビューし、PDCA サイクルにしたがって継続的に改善することが書かれている。したがって、マネジメントシステム規格の要求事項を満たしていれば、認証を取得せずとも、「ISO 規格に準拠したマネジメントシステムを運用しています！」と宣言することは全く問題ない。しかし実際には、取引先や顧客から認証取得の有無を問われたり、取引や調達の要件の一つになっていたりするケースもあり、今や認証取得は組織の能力や価値を示す手段の一つとなっている。

情報システム導入にあたり、情報セキュリティマネジメントシステム（ISMS）を構築・運用することは、情報システムを有効に活用する際の大きな助けとなるだろう。また、森林クラウドシステムではクラウド技術を介して異なる組織間で個人情報を取扱う場面も少なくないと考えられるため、情報セキュリ対策だけではなく、個人情報保護対策も重要なポイントとなる。

情報セキュリティマネジメントシステム、個人情報保護マネジメントシステムには、いずれも認証制度が存在しているため、これらを活用してマネジメントシステムを構築・運用することも、対策の有効な手段の一つと言えるだろう。

■情報セキュリティマネジメントシステム適合性評価制度（ISMS 認証制度）■

JIS Q 27001（ISO/IEC 27001 情報セキュリティマネジメントシステム – 要求事項）に基づき、組織が情報セキュリティマネジメントシステムを構築・運用していることを第三者である認証機関が審査し、認証登録証を発行するしくみ。ISMS 認証制度と呼ぶことも多い。ISO 規格がもとになっていることもあり、国内で取得した ISMS 認証は、国際的に有効である。

国内で ISMS 認証の審査を行う認証機関は 27 機関あり、ISMS 認証取得済みの組織は約 6,300 以上にのぼる（2021 年 2 月現在）。 認証の有効期限は 3 年間であり、認証取得後、3 年毎の更新審査のほか、毎年のサーベイランス審査（維持審査）が行われる。

ISMS 認証には、クラウドサービスに特化した「ISMS クラウドセキュリティ認証」というバリエーションも存在しており、すでに ISMS 認証を取得済みのクラウド事業者が、ISMS に加えてクラウドサービス特有の要求事項を満たしているかを審査する。2021 年 2 月現在、国内で約 200 組織が認証を取得している。

認証の取得単位は、企業全体の場合もあるが、情報システム部門やシステム開発部門など、特に情報セキュリティを重視する部門単位で取得することもある。

■プライバシーマーク制度■

JIS Q 15001（個人情報保護マネジメントシステム – 要求事項）をベースとしつつ、個人情報保護法の遵守状況を含む審査を行い、「プライバシーマーク」を発行する制度である。他のマネジメントシステムの認証制度と同様に、規格で規定されているマネジメントシステムの要求事項を審査するが、他の ISO マネジメントシステム規格とは大きく異なり、日本の個人情報保護法に基づく個人情報保護が実現できているかどうかを審査する点が特徴的である。反面、JIS 規格をベースとした制度になっているため、国内でのみ有効な制度でもある。

2021 年 1 月現在、プライバシーマークの審査を行う審査機関は 19 機関、プライバシーマーク付与事業者は 16,000 社以上にのぼる。マークの有効期限は 2 年間であり、2 年毎の更新審査を受けることでマークの更新が可能である。

【利活用・応用事例編】

8. 森林情報のオープンデータ化

オープンデータとは、特定の利用者・用途に対してのみ限定的に情報を提供するのではなく、権利者を明記するかぎり、誰でも・どんなことにでも使ってよいとする取り組みで、全国の自治体や官庁をはじめとした様々な行政機関で盛んになっている。森林情報についても、いくつかの自治体でオープンデータ化が進められており、それらの事例調査を基に、オープンデータの利点・欠点、具体的な指針についてまとめる。

8-1. オープンデータに先進的に取り組む自治体の傾向

オープンデータに先進的に取り組む自治体として、室蘭市・会津若松市・静岡県・福井県に聞き取り調査を行った。これらの自治体の共通点として以下の三点の傾向が見られた。

① 先進的な GIS の導入・WebGIS の公開を行っている

いずれの自治体でも全庁的に GIS を導入しており、それによって情報の電子化・統合化・共有が進められている他、一部の自治体では市民向けに WebGIS を公開している。これにより、オープンデータとして公開するための情報の電子化が既に全庁的に行われており、他の自治体に比べてオープンデータに取り組みやすい環境だったと言える。またそれに加えて、全庁的に GIS を利用する環境であることから、GIS による情報共有・情報の可視化のメリットを理解しており、オープンデータのメリットである情報共有・利用が理解されやすいと考えられる。

② 自治体内部に情報を集約する体制がある

オープンデータに先進的に取り組む自治体では、オープンデータ所管課はオープンデータの取り組み以前より、全庁での統合型 GIS の導入や行政手続きの電子化の対応や、Web での情報公開を担当するなど、庁内の情報化及び情報公開を担当している傾向が見られた。

これにより、オープンデータ所管課は大きな業務フローを変更することなく他のデータ所管課から情報を預かることができ、先進的にオープンデータへ取り組むことができたと考えられる。

③ 既存の公開情報からオープンデータ化を進めている

オープンデータの取り組みでは、既存の公開情報をオープンデータとすることが一般的である。先進的に取り組む自治体でも同様に、既存の公開情報からオープンデータ化を行っており、取り組みやすいところから始めることで庁内での理解を広めている。

④ オープンデータを全庁的な取り組みとして位置付けている

以上から、オープンデータへの取り組みが上手く機能する条件とは、「これまでと同じ業務でこれまでと同じ公開情報をオープンデータにする」ということになる。しかし、

聞き取り調査では「これまでと同じであれば、なぜオープンデータにする必要があるのか、これまでと何が変わるのか」という意見からオープンデータ化が滞ったという事例があった。現状では、先進的な取り組みを行う自治体では「これまでと変わらないのであれば取り組む」という意識を持つ職員によってボトムアップの取り組みが推進されている傾向がある。今後、他の自治体でオープンデータの取り組みを推進する上では、これらの先進的なオープンデータの取り組み事例から、オープンデータ化のメリットや利活用事例を共有・普及することが重要であると考えられる。

8-2. オープンデータを進める上での自治体の懸念と解決方法

聞き取り調査から出た、オープンデータを積極的に進めることができない懸念点や、オープンデータを進める上で課題となった点をまとめ、それぞれの解決への方策を以下にまとめる。

① オープンデータ対応のコスト

オープンデータは一度公開して完了するものではなく、継続的にデータを公開すること、日々の行政業務の結果がそのまま公開されることが理想である。そのため、負荷やコストを増やして実現するのではなく、普段の行政業務のまま可能な範囲で実施することが重要である。多くの自治体では、オープンデータのために新たな体制を整備する、これまで非公開だった情報を公開とする判断を行うといったことはせず、統計情報や公共データなどの既存の公開情報、かつ広報や統計担当など既存の情報公開フローが整備されているものを、改めてオープンなライセンスを明示することから始める事例が多い。

② オープンデータの需要・メリット

オープンデータの本来の理念としては、需要・メリットの有無にかかわらず、原則公開とすることを掲げている。しかし、自治体聞き取り調査で多く出た意見に、オープンデータを進める際の自治体内部説明では既に公開情報となっているものをオープンデータとすることにどれだけの価値があるのかという問いが多くあり、そのための答えが必要となるというものがあった。

一般的にオープンデータのメリットとして、公共データを利活用したサービスの拡充や、産業の創出が挙げられる。聞き取り調査を行った自治体の中では、これまで自治体が市民のためのサービスを独自に構築していたものを、サービスで利用する情報をオープンデータとして公開することで、サービス事業者はオープンデータをテストデータに用いサービスの実績として宣伝でき、市民は自治体の構築したサービスではなくサービス事業者による使い勝手の良いサービスを用いることができた事例があった。

聞き取り調査ではこれらの公共データを利活用したサービスのメリットに加え、オープンデータとすることで情報公開請求や情報利用の申請手続き業務が軽減されたという意見が多くあった。このことは、オープンデータへの理解が求められるデータ所管課

に対する大きなメリットと言えるだろう。

③　住民からのクレームや訴訟リスクの増加

オープンデータでは、個人情報や個人の権利を侵害する情報は削除したうえで公開する。また、利用規約でデータを利用した際の第三者の権利侵害はデータ利用者が責任を負うことを明記するのが一般的となっている。しかし、自治体の持つデータは物理的な場所に紐づくものが多く、公開によってトラブルにつながる可能性のあるものも少なくない。

聞き取り調査で出た事例としては、ごみ収集場所を地図データとして公開することを検討したが、ごみ収集は町内会など特定の住民のみが定められた場所を利用可能としており、ごみ収集場所を公開した場合には、本来利用してはならない外部の人間によるごみの投棄が発生することが考えられたため、非公開とした。

このような情報の公開・非公開の判断は、オープンデータ所管課ではなく、実際のデータを管理し行政業務に携わるデータ所管課が、公開によるトラブル・公開によるメリットを想定した上で判断することが必要だろう。

④　データ品質が公開に適さない

行政業務の中で使われている情報は、それぞれの目的のために作成・整備されており、他の目的の情報と突き合わせた際に齟齬が発生することは少なくない。しかし、オープンデータの目的には、データの利活用だけでなくデータを公開することで行政の透明性を担保するというものがある。つまり、オープンデータでは、公開のためにデータを加工する必要はなく、実業務の中で使われているデータがそのまま公開されることが重要である。

8-3. 森林クラウド・標準仕様を利用したオープンデータ化の検討

以上の調査で明らかとなったように、プライベートデータでの森林情報の公開・共有、森林情報のオープンデータ化には様々な課題が存在する。

本事業で検討を行った森林クラウド・標準仕様は、これらの課題を解決するために有用であるかを検討した。

①　情報加工・公開・更新のコスト

個人情報を削除する等の公開作業、Web サイト等への公開作業、情報の更新にはコストが発生する。また、図面データの場合ファイルサイズが大きいため、公開インフラのコストが発生することになる。

森林クラウド上で森林情報を管理することで、標準仕様の項目ごとに公開することが可能である。また、実利用する森林クラウド上の情報を公開することで、更新の手間をかけずにリアルタイムの情報を公開することが可能である。

②　都道府県・市町村での情報公開方針の違い

市町村では都道府県の管理する森林情報をベースに申請手続きや現地確認などを行

っている。そのため市町村独自で作成した情報の公開を判断することができない。森林クラウド上では、標準仕様に加えユーザーの目的に応じたレイヤを追加することができるため、市町村が独自に作成した情報だけを公開することが可能である。

③　適さない用途・目的での情報利用

森林情報をオープンデータとした場合、情報の精度や鮮度など林務以外では適さない目的に利用される可能性がある。また、個人情報や財産に関する情報など、森林情報はすべてがオープンデータになるわけではなく、特定の利用者・目的のために限定した情報提供を行う必要がある。森林クラウドでは、利用者ごと・情報項目ごとにアクセス権限を設定することが可能で、これにより特定の目的を持った利用者にのみ情報を公開することができる。そのため、森林クラウド上では、オープンデータとこれまでの制限された公開情報を同じプラットフォーム上で利用することができる。

④　他の情報との不整合・データ形式や粒度の違い

自治体が個別に取り組むオープンデータでは、それぞれが最適な手法で情報を公開しており、自治体によってデータの形式や粒度、項目がバラバラになってしまうことが課題とされている。森林クラウド、及び標準仕様を用いることで複数の自治体から標準化された情報を公開することができ、事業者などの他地域展開が容易になる。

以上のことから、森林情報の公開及びオープンデータ化における課題を解決する上で、森林クラウド・標準仕様を用いることは効果的であると考えられる。

8-4. 森林情報のオープンデータ化のための具体的な指針

8-4-1. オープンデータに関する手引き・指針

オープンデータに関する手引き・指針は、社会的・技術的な定義に関するものや具体的な取り組み事例をまとめたものなど、国内外で多く整備されている。
自治体で今後オープンデータに取り組む際に参考となる手引きをまとめる。

①　社会的・技術的な定義

- オープンデータ・ハンドブック
  http://opendatahandbook.org/guide/ja/
- オープンの定義（Open Definition2.1）
  http://opendefinition.org/od/2.1/ja/

②　導入のための手引き

- 内閣官房　地方公共団体オープンデータ推進ガイドライン
  http://www.kantei.go.jp/jp/singi/it2/densi/kettei/opendate_guideline.pdf
- 内閣官房　オープンデータをはじめよう～地方公共団体のための最初の手引書
  http://www.kantei.go.jp/jp/singi/it2/densi/kettei/opendate_tebikisyo.pdf

- 地方公共団体情報システム機構　オープンデータ取組ガイド
  https://www.j-lis.go.jp/rdd/opendata/h26_opendataguide.html
- 国土交通省　地方公共団体向け地理空間情報に関する Web ガイドブック
  https://www.mlit.go.jp/kokudoseisaku/gis/gis/webguide/giswg_solsht/1311/

③　日本政府の動向、および国内のオープンデータカタログ

- 電子行政オープンデータに関連する決定等
  https://www.kantei.go.jp/jp/singi/it2/densi/
- データカタログサイト
  https://www.data.go.jp/
- 地理空間情報クリアリングハウス
  http://ckan.gsi.go.jp

④　森林情報のオープンデータ事例

- 静岡県森林情報共有システム
  https://fgis.pref.shizuoka.jp/
- 静岡県　ふじのくにオープンデータカタログ
  https://opendata.pref.shizuoka.jp/
- 北海道　森林計画関係資料
  http://www.pref.hokkaido.lg.jp/sr/srk/OPD.htm

9. 森林クラウド・トラストフレームワーク

森林クラウドの導入検討を行う上で、将来的に都道府県ごとに異なる森林クラウドシステムが導入されると考えられた。その場合には、複数の都道府県で事業を行う林業事業体や木材需要者などの事業者は複数の森林クラウドシステムを利用することになる。その際に、都道府県等クラウド運用者の、ユーザー管理・アクセス管理・ユーザーの本人確認の負荷増大や、複数の森林クラウドシステムを利用する事業者の ID・パスワード管理の煩雑さにより、セキュリティ事故が起きうることが考えられ、その対策としてユーザー認証・ID 連携の仕組みである「森林クラウド・トラストフレームワーク」の検討を行った。

「森林クラウド・トラストフレームワーク」とは、複数のクラウド事業者がユーザ ID とパスワードを連携し、ひとつのユーザ ID とパスワードで様々なクラウドサービスの利用が可能となるためのしくみが必要である。ID 連携トラストフレームワークは、このような複数のユーザ ID とパスワードの管理負担をなくし、異なるクラウドシステムをシームレスに利用可能にするしくみのひとつである。

検討結果については、平成 27 年度「森林クラウド実証システム開発事業」の中で、先行的に実証検証を行った。

ID 連携を可能とした森林クラウドシステムの概念図を以下の図 4　現状のクラウド利用と ID 連携のクラウド利用に示す。

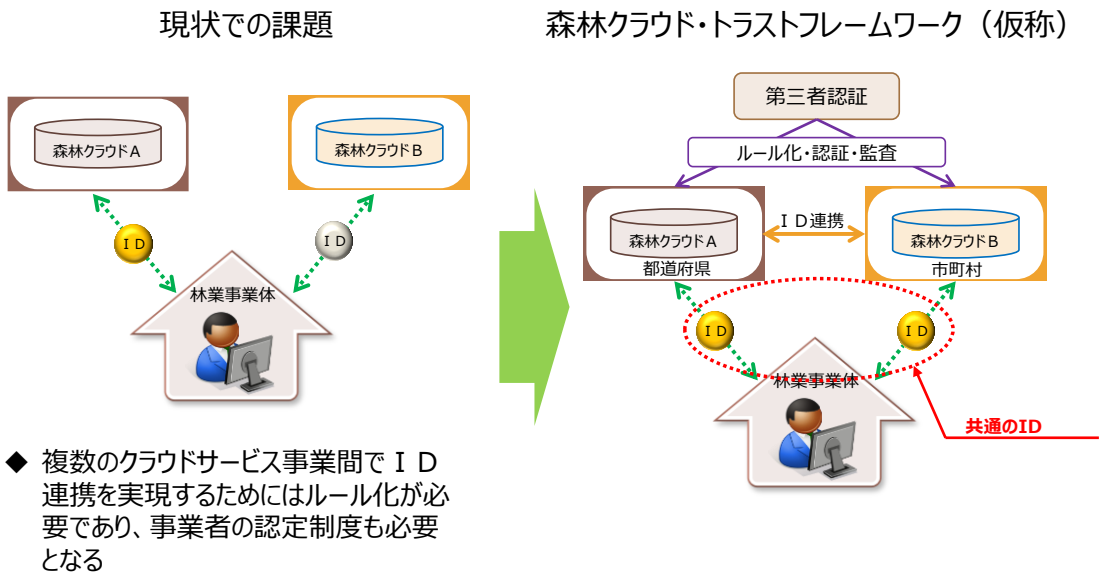


図 4　現状のクラウド利用と ID 連携のクラウド利用

9-1. 森林クラウド・トラストフレームワークの機能

森林クラウド・トラストフレームワークには以下の機能を有する。

(1)　　様々なクラウドシステムと ID 連携を行い安全且つ信頼できる ID プロバイダ機能

(2)　　利用者のアクセス権限及びアクセス制御等の管理機能
(3)　　外部・内部からの異常アクセスの監視機能
(4)　　モバイル端末利用環境のセキュリティ対応機能
(5)　　森林情報とマイナンバー・個人情報等の制御機能（今年度の範囲から外す）

それぞれのクラウド事業者が上記の機能を有するよりも、独立且つ中立的な組織(例えば、クラウド基盤事業者)組織が、ID 連携機能を司る「ID プロバイダ」として機能する方が有効である。

9-2. ID プロバイダの機能

都道府県や市町村、林業事業体がそれぞれ別のクラウド事業者を採用する可能性があるため、ID 連携を可能とする ID プロバイダ機能が必要であること、既存のクラウドサービスを展開している事業者が容易に参加できる環境を整えるために、ID 変換機能を ID プロバイダが有していなければならない。

以下の図 5　ID プロバイダによる ID 連携の概要に示す。

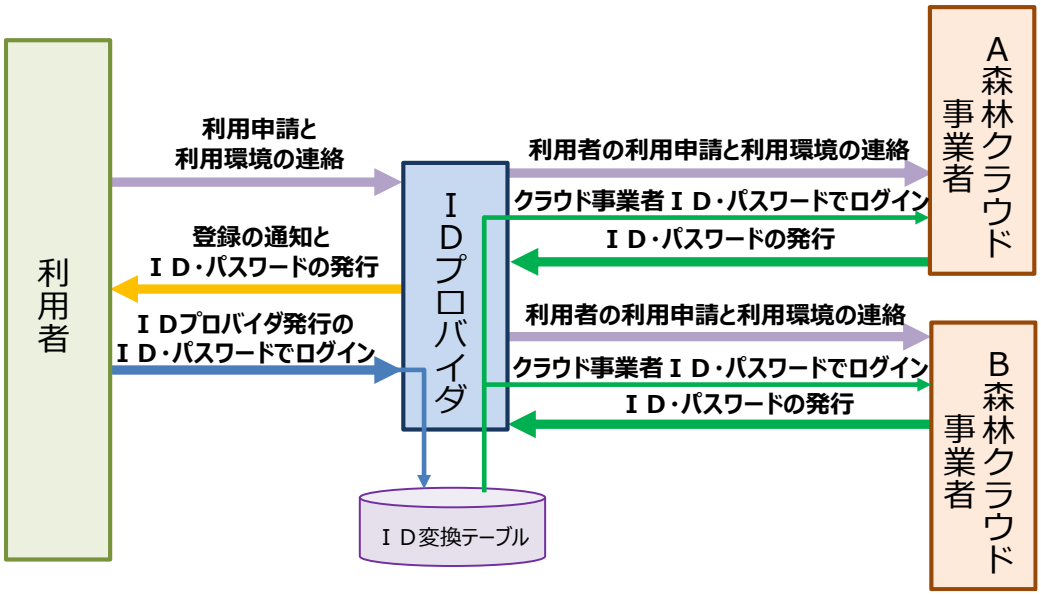


図 5　ID プロバイダによる ID 連携の概要

9-3. 森林クラウド・トラストフレームワークの運用

森林クラウド・トラストフレームワークに参加できる資格があるか、個人情報保護や情報セキュリティの確保に必要な対策が施されているかを評価するための基準が必要である。

- ✓ ID プロバイダは自身の資格要件を満たしていなければならない。
- ✓ クラウド事業者が ID 連携を行うためには、ID プロバイダに登録しなければならない。
- ✓ ID プロバイダは、参加を希望するクラウド事業者に対して資格要件を満たしている

か評価した上で、登録を行い公表することが望ましい。

- ✓ ID プロバイダを担う事業者は、森林クラウドシステム事業において中立的な立場の事業者(例えば、クラウド基盤事業者等)であることが望ましい。
- ✓ クラウド事業者は ID プロバイダから評価を受けその資格要件を満たしていること。
- ✓ 情報セキュリティ・個人情報保護等の規程を策定し、それを遵守していることが求められる。

ID プロバイダの資格要件を評価する組織や機関がないため、ISMS やプライバシーマーク等の第三者認証機関が運営する認証を取得していることが望ましい。

9-4. 森林クラウドシステム利用におけるアクターと役割

森林クラウドシステム利用におけるアクターと役割を以下の表 3 に示す。

表 3　森林クラウドシステム利用におけるアクターと役割

森林クラウドシステム利用におけるアクターと役割					
対象者	利用者		森林クラウド事業者		IDプロバイダ
	都道府県 市町村	森林組合 その他林業事業体 森林所有者	クラウド基盤事業者	サービスプロバイダ	
森林クラウド	ID・パスワード受領 自社利用権限の通知 アクセス許可の通知	ID・パスワード受領 自社利用権限の通知 アクセス権限の受領 自治体へアクセス申請 アクセス許可の受領	基盤利用者登録 ユーザファイル管理 通信トラフィックの監視 不正アクセスの監視	ID・パスワードの通知 利用者の受領・登録 アクセス権限の設定 事業者登録申請 不正アクセスの監視	ID・パスワードの発行 利用者確認・登録 アクセス権限の設定 事業者登録・確認

9-5. ID プロバイダ及びクラウド事業者の資格要件

森林クラウド・トラストフレームワークでは、利用者と対面する ID プロバイダとサービスを提供するクラウド事業者が信頼できる事業者であることを利用者に理解してもらうことが重要である。　そのためには、ID プロバイダ及びクラウド事業者が信頼に足りる評価基準を満たしていなければならない。

ID プロバイダ及びクラウド事業者の資格要件を以下の表 4　ID プロバイダの資格要件及び、表 5　クラウド事業者の資格要件に整理した。

表 4　IDプロバイダの資格要件

資格要件		IDプロバイダ （クラウド基盤事業者等）	備考
①	**組織の成熟度**	組織 法律及び契約の遵守 財務規定 データ保持及び保護 サービスの終了	第三者認証取得事業者である事 (ISMS・Pマーク等)
②	**サービスの定義**	利用規約 サービスの変更通知 利用者との合意 利用者との合意の記録 利用者情報の変更	
③	**情報セキュリティの管理体制**	セキュリティポリシーと手順の文書化 セキュリティポリシーの管理と責任 リスク管理 業務継続計画 品質管理 システム管理 ソフトウェア管理 内部監査・外部監査の実施 監査記録	
④	**情報セキュリティに関する運営基盤**	セキュリティ管理の手法 セキュリティ管理に関する役割の定義 人材リソースの適切性 物理的アクセス制御 論理的アクセス制御	
⑤	**外部サービスの利用**	契約と手続き 契約先の監督	
⑥	**セキュアな通信の確保**	セキュアなリモート通信 認証メッセージの検証 パスワードへのアクセス制御 パスワードの論理的保護	

表 5　クラウド事業者の資格要件

資格要件		森林クラウド事業者 （サービスプロバイダ等）	備考
①	**組織の成熟度**	法的実在性 法令遵守 情報管理能力 委託管理能力 組織管理能力	
②	**サービスの定義**	利用規約 サービスの変更通知 利用者との合意 利用者との合意の記録	
③	**情報セキュリティの管理体制**	セキュリティポリシーと手順の文書化 セキュリティポリシーの管理と責任 リスク管理 業務継続計画 品質管理 システム管理 ソフトウェア管理 内部監査・外部監査の実施 監査記録	
④	**情報セキュリティに関する運営基盤**	セキュリティ管理の手法 セキュリティ管理に関する役割の定義 物理的アクセス制御 論理的アクセス制御	
⑤	**外部サービスの利用**	契約と手続き 契約先の監督	
⑥	**セキュアな通信の確保**	パスワードへのアクセス制御 パスワードの論理的保護	

9-6. クラウド事業者に関する評価・登録の手順

クラウド事業者は登録申請書と資格要件に準じた資料を作成し、ID プロバイダに提出した上で、評価を受け一定の基準を満たしていると判断した場合は、登録認定通知が付与され森林クラウド・トラストフレームワークに登録される。

これらの評価・登録の手順を以下の図 6　評価・登録の手順に示す。

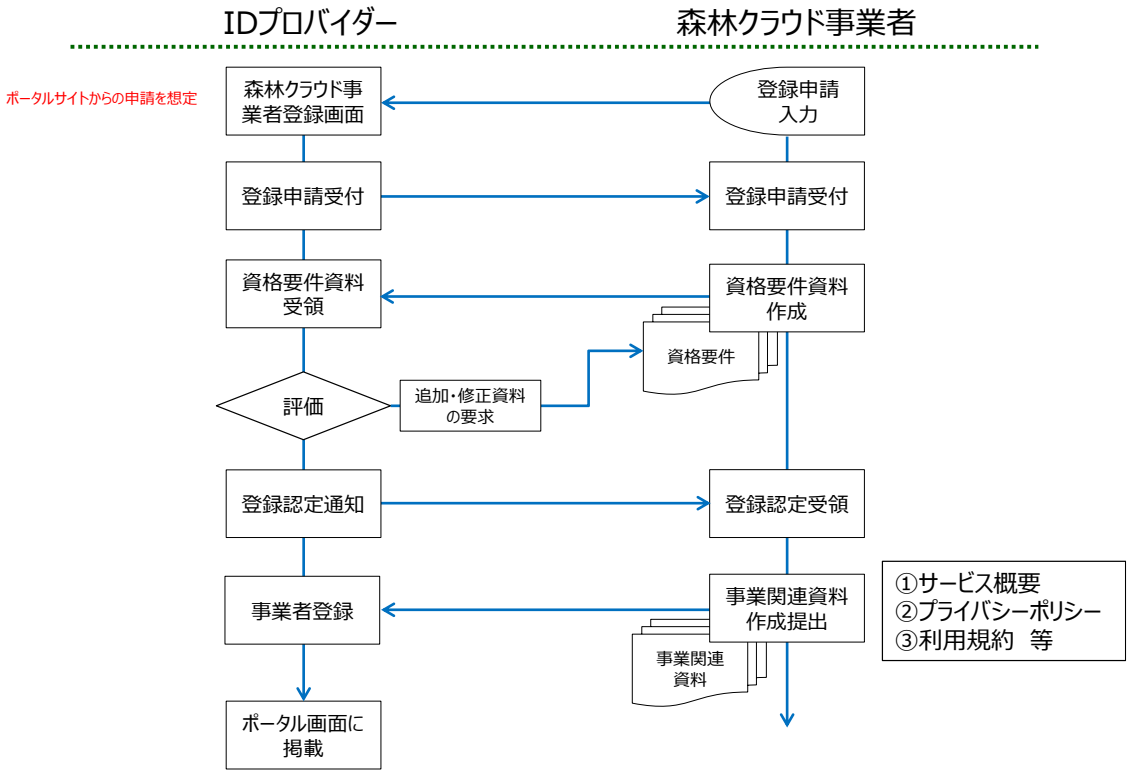


図 6　評価・登録の手順

10. 森林所有者のための分かり易い表示・通知

10-1. 森林所有者への分かり易い表示・通知方法

森林・林業事業における個人情報の取扱いに関して都道府県、市町村及び林業事業体を対象に検討をおこなってきたがここでは、森林所有者に対してプライバシーに配慮した環境整備について整理する。

森林経営計画制度及び施業集約化の重要性や必要性について森林所有者(特に零細規模の森林所有者)のほとんどの人は認識していない。

平成 24 年度より施行された森林経営計画制度も地域によっては森林経営計画が提出されている面積が民有林全体の 15%程度に留まっている。[2]

施業集約化が進んでいないのは、森林所有者情報が提供されないためと言われているが他の要因として、森林所有者の理解が得られていないことも影響している。

森林所有者に対して、森林経営計画制度への理解と協力、個人情報の利用に関する同意を得るために都道府県、市町村、林業事業体が一体となって分かり易い表示・通知を実施することが望ましい。

実施するための要件を以下の通り整理した。

① 都道府県に求められる表示・通知内容
- ✓ 森林整備の必要性と施業の協力依頼
- ✓ 森林所有者の責務の説明
- ✓ 個人情報の提供先の表示
- ✓ 提供する個人情報の項目

② 市町村に求められる表示・通知内容
- ✓ 都道府県と共通の内容
- ✓ 市町村独自の森林整備に関する事業・施策の説明

③ 林業事業体に求められる表示・通知内容
- ✓ 森林整備に関する林業事業体の事業説明
- ✓ 施業集約化推進に関する特定受託者の認定を取得していることの説明
- ✓ 森林所有者情報を都道府県、市町村から提供されている理由と目的の説明
- ✓ プライバシーポリシーを作成・公表している

これらが容易に確認できることが重要である。

10-2. 分かり易い表示・通知のポイント

都道府県や市町村の森林・林業事業の政策がそれぞれ異なる特徴があることから表示・通知内容まで規定することはしない。　同様に林業事業体にとっても経営方針がそれぞれ異

[2] 平成 26 年度の市町村・林業事業体への聞き取り調査より森林経営計画の作成状況は市町村有林を除く民有林全体の 15%に留まっている地域がある。

なるため規定しないこととする。

① 文書作成のためのポイント

作成にあたって意味・内容に明確な用語を用い、一貫した言葉遣いで平易かつ簡素に記載されていることが求められる。

- ✓ 一般的に広く用いられる用語を使う。
- ✓ 専門用語を用いる場合は法令や規格標準などで定義された意味・内容になっていること。
- ✓ 同じ意味・内容を示すものとして異なる単語を使わないこと。
- ✓ 同じ単語で複数の異なる意味・内容で使わないこと。

② プライバシーポリシーの作成ポイント

- ✓ プライバシーポリシーには、定められた様式やルールはない。
- ✓ 「できること」「できないこと」をできるだけ明確に示すようにすること。

【プライバシーポリシーの構成（例)】

1. 基本方針
2. 適用範囲
3. 個人情報の取得と利用目的
4. 個人情報の管理
   1) 情報の正確性の確保
   2) 安全管理措置
   3) 従業者の監督
   4) 委託先の監督
   5) 保存期間と廃棄
5. 第三者提供の有無
6. 個人情報の開示・訂正・利用停止等
   1) 個人情報取扱事業者の名称
   2) 保有個人データの訂正等
   3) 保有個人データの利用停止等
   4) 手数料
7. 問い合わせ先
8. 改訂

【巻末付録】

11. 個人情報保護法改正の概要（令和 2 年改正）

個人情報保護法は、平成 27 年改正個人情報保護法に設けられた「いわゆる 3 年ごと見直し」に関する規定（附則第 12 条）に基づき、3 年毎に見直しが行われ、都度改正が行われている。

巻末付録として、令和 2 年に改正された個人情報保護法の改正ポイントを解説する。（以下は、個人情報保護委員会による改正個人情報保護法の概要からの抜粋である）

11-1. 個人の権利の在り方

- 利用停止・消去等の「個人の請求権」について、不正取得等の一部の法違反の場合に加えて、個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和された。
- 保有個人データの開示方法 （※） について、電磁的記録の提供を含め、本人が指示できるようになった。
  ※ 改正以前は、原則として、書面の交付による方法とされていた。
- 個人データの授受に関する第三者提供記録について、本人が開示請求できるようになった。
- ６ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象となった。
- オプトアウト規定 （※）により第三者に提供できる個人データの範囲を限定し、
  ①不正取得された個人データ、
  ②オプトアウト規定により提供された個人データ
  についても対象外となった。
  ※ 本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

11-2. 事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合 （※） に、個人情報保護委員会への報告及び本人への通知が義務化された。
  ※ 一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
- 違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨が明確化された。

11-3. 事業者による自主的な取組を促す仕組みの在り方

- 認定個人情報保護団体制度について、改正法以前の制度 （※） に加え、企業の特定分野(部門)を対象とする団体を認定できるようにした。

※　改正法以前の認定団体は、対象事業者のすべての分野（部門）を対象としていた。

11-4. データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務が緩和された。
- 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認が義務付けられた。

11-5. ペナルティの在り方

- 個人情報保護委員会による命令違反・委員会に対する虚偽報告等の法定刑が引き上げられた。

表 6　改正前後の法定刑の比較

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6 月以下	**1 年**以下	30 万円以下	**100 万円**以下
	法人等	―	―	30 万円以下	**1 億円**以下
個人情報データベース等の不正提供等	行為者	1 年以下	1 年以下	50 万円以下	50 万円以下
	法人等	―	―	50 万円以下	**1 億円**以下
個人情報保護委員会への虚偽報告等	行為者	―	―	30 万円以下	**50 万円**以下
	法人等	―	―	30 万円以下	**50 万円**以下

（個人情報保護委員会の Web サイトより）

11-6. 法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。
- 外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

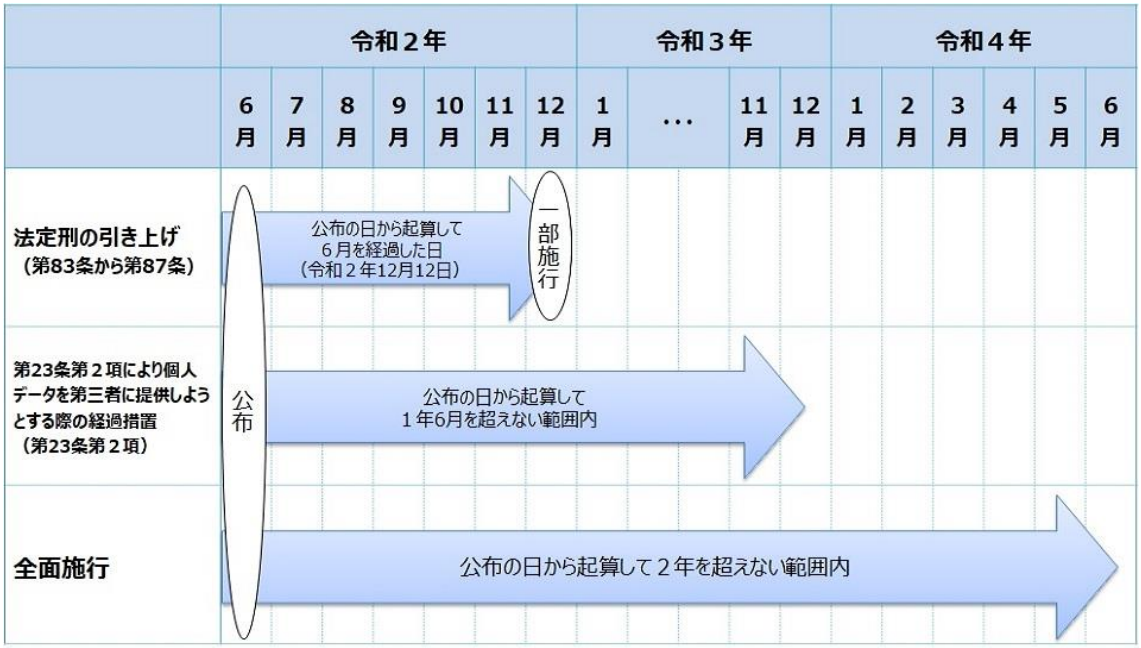
11-7. その他（関連法）

本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

11-8.「個人情報の保護に関する法律等の一部を改正する法律」の施行日について

令和 2 年改正個人情報保護法は、全面施行は「公布の日から起算して 2 年を超えない範囲内」となっているが、一部については既に施行済みである点、令和 3 年中にもさらに一部が施行される予定になっている点についても、注意が必要である。

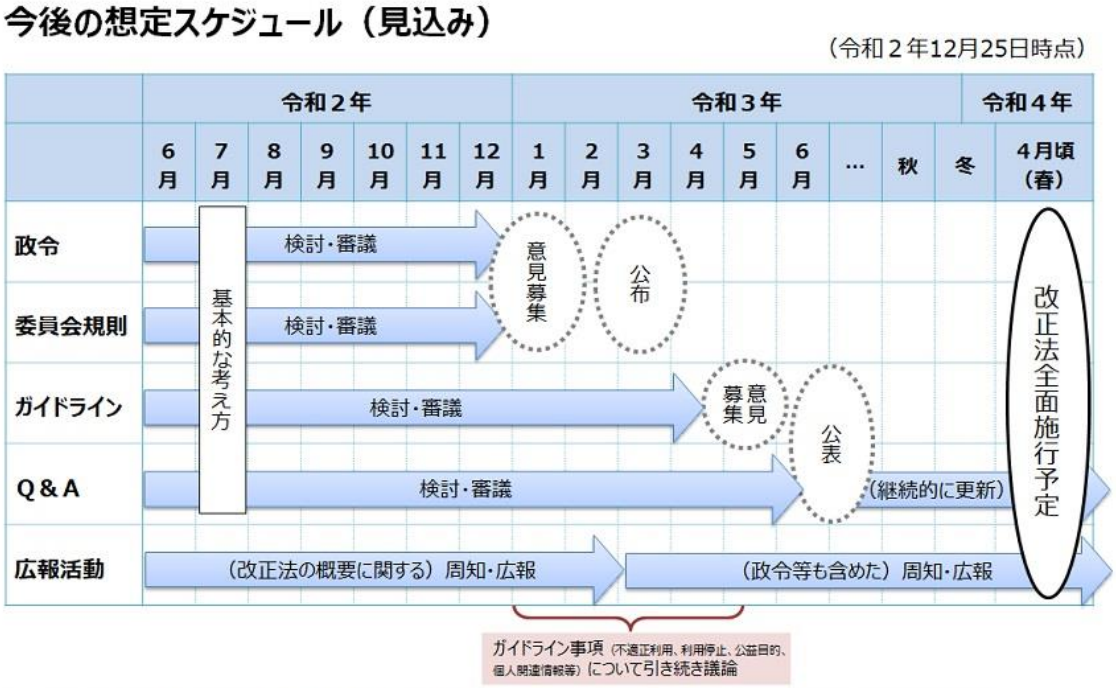
表 7　令和 2 年改正個人情報保護法の施行



（個人情報保護委員会の Web サイトより）

なお、法施行以外にも、改正法を正しく理解し、実施するためのガイドラインの発行や、各種パブリックコメント等の予定がある。

表 8　改正個人情報保護法及の施行及び関連スケジュール



※このほか、個人情報の保護に関する基本方針、認定個人情報保護団体の認定等に関する指針等についての改正も予定。
※上記の表は、第144回個人情報保護委員会（令和２年６月15日）資料１の「改正法の円滑な施行に向けたロードマップ」について、検討状況等を踏まえて修正したものであり、現時点での大まかな見込みのため、今後の状況によって変わり得る。

（個人情報保護委員会の Web サイトより）

12. 参考文献・URL 等

- 個人情報保護法等　個人情報保護委員会
  https://www.ppc.go.jp/personalinfo/
- 個人情報の保護　農林水産省
  https://www.maff.go.jp/j/kanbo/joho/kozin_zyoho/
- 森林計画業務必携　株式会社日本林業調査会
  https://www.j-fic.com/bd/search/title/森林計画業務必携/
- JIS Q 27001　情報セキュリティマネジメントシステム　－　要求事項
  一般財団法人日本規格協会
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+27001%3A2014
- JIS Q 15001　個人情報保護マネジメントシステム　－　要求事項
  一般財団法人日本規格協会
  https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS%20Q%2015001:2017
- 地方公共団体における ASP・SaaS 導入ガイドライン　総務省
  https://cio.go.jp/node/1884
- クラウドサービス利用のための情報セキュリティガイドライン　経済産業省
  https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html
- 地理空間情報の活用における個人情報の扱いに関するガイドライン
  地理空間情報の二次利用促進に関するガイドライン
  地理空間情報活用推進会議
  https://www.gsi.go.jp/chirikukan/guideline.html
- クラウドコンピューティングのためのセキュリティガイダンス（CSA ガイダンス）
  日本クラウドセキュリティアライアンス
  https://www.cloudsecurityalliance.jp/guidance.html

改訂履歴

履歴	版名	日付	適用項目
策定	Ver.1.0	平成 26 年　3 月	都道府県編　(クラウド事業者・都道府県)
改訂	Ver.2.0	平成 27 年　3 月	市町村・林業事業体を追記
改訂	Ver.3.0	平成 28 年　3 月	森林クラウド・トラストフレームワークを追記
改訂	Ver4.0	平成 29 年　3 月	構成の変更及び林地台帳に関する追記
改訂	Ver.5.0	平成 30 年　3 月	コラムを追記
改訂	Ver.6.0	令和 3 年　3 月	実践編を追加 上記に伴い、全体構成を見直し コラムを追加

森林クラウドシステムに係る標準仕様書　Ver. 6.0

平成 25~29 年度　林野庁補助事業
森林情報高度利活用技術開発事業のうち森林クラウドシステム標準化事業
令和 2 年度　　林野庁補助事業
林業イノベーション推進総合対策のうちＩＣＴ生産管理推進対策のうち
レーザ計測による森林資源データの解析・管理の標準化事業

令和 2 年 3 月　発行
一般社団法人　日本森林技術協会
〒102-0085　　東京都千代田区六番町 7 番地
TEL　03 - 3261 - 5497　　FAX　03 - 3261 - 3044　http://www.jafta.or.jp

一般社団法人　日本林野測量協会
〒102-0085　　東京都千代田区六番町 7 番地　日林協会館 2F
TEL　03 - 3261 - 8138　　FAX　03 - 3261 - 8145　　http://rinsokyo.sakura.ne.jp/

問合先
森林 GIS フォーラム事務局　　TEL　029 - 829 - 8314