令和８年度・令和９年度
AI を活用した光化学スモッグ予測事業業務委託
調達仕様書
（公募用）

千葉県環境生活部大気保全課

目次

1 調達案件の概要

1.1. 調達案件名

AI を活用した光化学スモッグ予測事業業務委託

1.2. 調達の背景

千葉県では、大気汚染防止法に基づき大気汚染の状況を監視し、県民の健康や生活環境への被害を防止する取り組みを行っています。特に、大気の汚染が著しくなり、人の健康や生活環境に係る被害が生じる恐れがある場合には、注意報を発令して県民に周知するとともに、事業者に対してばい煙などの排出量を減少させる措置を求めています。

オキシダント濃度が高濃度（0.120ppm 以上）となり、それが継続すると認められる場合には光化学スモッグ注意報が発令されます。この注意報が発令された場合、学校では屋外での体育活動等が中止されるほか、企業においては県からの要請に基づき燃料使用量等を 30 分以内に 20%以上削減する必要があり、生産活動に制約が加わることとなります。このように光化学スモッグ注意報の発令は、県民生活や企業活動に影響を与えるものであり、特に夏季（4 月～10 月）の日中において、県職員が平日・休日を問わず常時監視を行う必要がある状況です。ただし、注意報の発令は年間で 10 日程度に留まるため、監視業務の効率化が課題となっています。

そこで、本調達では、過去の気象データやオキシダント濃度データなどを AI に学習させ、高精度で予測するシステムを導入することで、複数の効果が期待されています。具体的には、注意報発令の予測精度が向上することで、企業においては生産活動をより計画的に行えるようになり、県民の生活も急な計画変更が減少することで快適性が向上します。また、県職員による常時監視業務の負担も軽減されることが見込まれています。

1.3. 調達目的及び期待する効果

本調達の目的は、過去の気象データやオキシダント濃度を AI に学習させることで、光化学スモッグ注意報の予測精度を向上させ、県民生活や事業者活動への影響を最小限に抑えつつ、県職員の監視業務の負担を軽減することです。

予測精度の評価に応じて再学習やパラメータ調整を行うことで、継続的な改善を図り、注意報発令のタイミングを高精度に予測することで、企業が計画的に生産活動を行えるようになるほか、県民生活の急な計画変更が減少します。

1.4. 業務・情報システムの概要

本事業に係るシステム概要は下図のとおり。

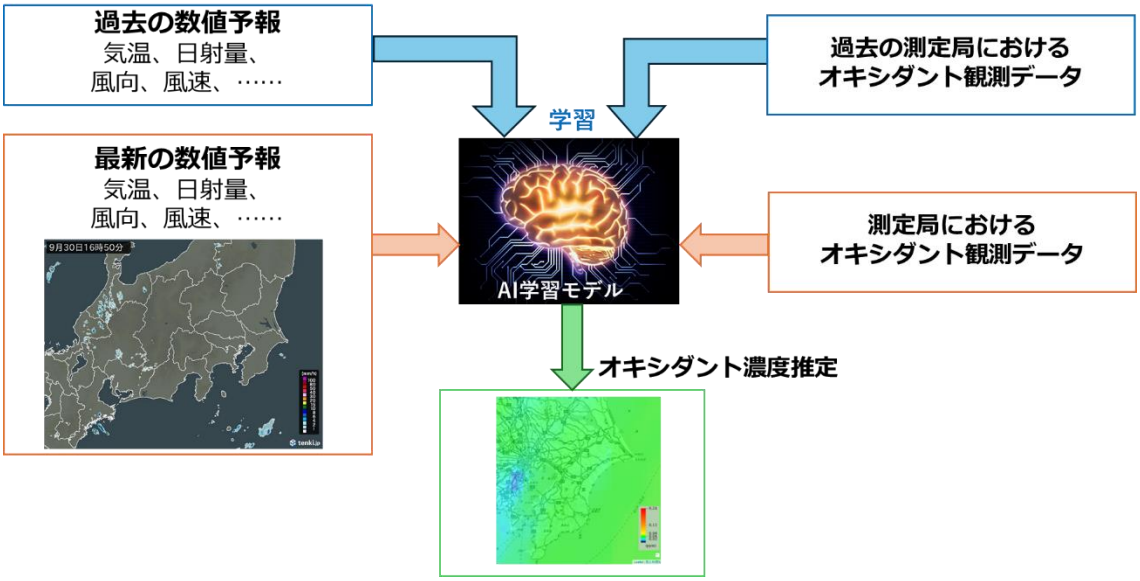

図１　AI を活用した光化学スモッグ予測のシステム概要

1.5. 契約期間

契約日から令和１０年２月２９日まで

1.6. 作業スケジュール

本業務は、令和８年度及び令和９年度の約２か年をシステム構築期間とし、令和１０年３月１日からの本格運用※を目指す。スケジュールの詳細は要求水準書「1.3 業務規模・スケジュール」参照。

※千葉県大気汚染緊急時対策実施要綱では、光化学スモッグ注意報の発令期間は 4 月から１０月までと定めているが、発令期間前の１か月間を準備期間とし、当該システムは、３月からの本格運用とする予定である。

1.7 グリーン購入法の適用

本調達は、「国等による環境物品等の調達の推進等に関する法律」（グリーン購入法）に従った調達をすること。

なお、判断基準については、千葉県で準拠している「環境物品等の調達の推進に関する基本方針」及び千葉県で定めている最新の「環境配慮物品調達方針」に準じること。

2 調達範囲

2.1 調達範囲

本事業は、AI を活用した光化学スモッグ予測事業業務委託に係るシステム設計、開発業務及び付帯する業務（データ収集、前処理、予測処理、結果出力、既存システムとの連携等）を行うものとする。

県民向けの情報提供は既存の別システムにより実施予定であり、本システムは当該システムへのデータ連携（API 等）を行うものとする。

独自提案の追加により、県が想定する調達範囲を拡張して業務を行う場合には、県と協議の上、契約時に調達範囲を決定すること。

3 情報システムに求める要件

設計、開発の実施に当たっては、「別添　要求水準書」（以下「要求水準書」という。）の各要件（機能要件、非機能要件、業務実施体制等）を満たすこと。

本仕様書は業務の進め方、成果物、体制、スケジュール等の実施方法を定める。

4 作業の実施内容に関する事項

4.1 業務計画書等の作成

受託者は契約締結後速やかに業務計画書を作成し、県の承認を得ること。

計画書に修正が必要となった場合は、受託者は速やかに県に報告し、協議の上で修正内容を合意し、更新履歴を残し共有すること。

4.2 作業管理

⑴ 設計・開発工程及びシステム構築期間中の運用・保守工程の作業管理

ア　作業管理の基本方針

受託者は、県が承認した「業務計画書」に基づき、設計・開発工程及び運用・保守工程の作業管理を適切に実施すること。

イ　管理の実施内容

以下の管理活動を、計画的かつ確実に実施すること。

(ｱ) 進捗管理

(ｲ) 品質管理

(ｳ) リスク管理

(ｴ) 課題管理

(ｵ) 構成管理

ウ　運用・保守工程の管理

運用・保守の管理方針は受託者が提案し、県と協議して確定する。

なお、「千葉県情報セキュリティ対策基準（契約締結時における最新版のもの)」を遵守すること。

⑵ コミュニケーション方法

受託者は、コミュニケーションツールを活用して、県との会議及び情報共有を円滑に行うこと。コミュニケーション手段についても双方協議で決定する。

4.3 要件定義

⑴ 要求水準書の確認と調整

ア　要求水準書の確認

受託者は、設計・開発の実施に先立ち、要求水準書の内容を十分に確認すること。

設計・開発に重大な影響を与える不整合、不足、矛盾が無いかを確認すること。

イ　要求水準書の調整すべき事項の特定等

要求水準書の内容を確認し、技術的実現性・運用上の制約・外部連携の観点から要求水準書の内容に不整合などが想定される場合、要求水準書の内容について、調整が必要な事項を特定し、県に報告すること。

ウ　要件調整のプロセス

イの報告後、影響（費用・納期・品質・運用）を整理した上での調整案を示し、県の了解を得た上で、調整内容を確定すること。

また、要件調整の内容・決定事項は要件調整台帳等に記録すること（調整項目、決定事項、影響、当該箇所等）。

⑵ 要求水準書の追加修正と承認

独自提案により要求水準書の内容に追加修正を行う場合は、随時、県及び関係者と協議し、協議結果を反映した要求水準書の修正案を提示し、県の了解を得た上で確定すること。

上記の協議で想定している修正内容とは、費用・納期・品質・運用に影響する重要な変更が該当する。

なお、重要な変更以外の軽微な変更は、事前に県へ報告の上、記録した内容を、定例会議等で共有すること。修正に関する協議・報告内容は、要件調整台帳等で記録すること。

⑶ 要求水準書の管理

要求水準書は、版数及び変更概要が分かるように管理を徹底すること。

要求水準書の修正版を作成する際は、変更履歴を要求水準書に記載し、修正

前後の内容を比較できる形式で保存すること。

4.4 設計

⑴ 設計の基本方針

受託者は、要求水準書の要件を満たすための基本設計及び詳細設計（運　用設計を含む）を実施し、成果物について県の承認を得ること。

設計内容は、第三者（県や本システム関係事業者等）が容易に理解できる形式で作成し、用語の定義や表記の統一に特に配慮すること。

⑵ 基本設計及び詳細設計（アプリケーション）

ア　基本設計

アプリケーションの基本設計では、システム全体図、データの流れと機能構成、機能・画面・帳票一覧、画面遷移図、データ一覧等を考慮して設計を行い、「基本設計書（アプリケーション）」を取りまとめ、県の承認を得ること。

基本設計書には、要求水準書の各要件が網羅されていることを容易に確認できる資料を添付すること。

イ　詳細設計

基本設計書（アプリケーション）に基づき、機能設計、スキーマ定義、コード定義、ジョブネット定義等を考慮して詳細設計を行い、「詳細設計書（アプリケーション）」を取りまとめ、県の承認を得ること。

詳細設計書には、基本設計書との対応表を含め、設計内容の整合性が確認できるようにすること。

ウ　外部インタフェース仕様書の作成

外部システムと連携するために必要な仕様を定義し、「外部インタフェース仕様書」を作成し、県の承認を得ること。外部インタフェース仕様書には、連携概要、送受信データ項目・形式、通信・認証方式、エラーハンドリング、セキュリティ要件、運用上の留意事項を含めること。

エ　UI 要件

職員端末は要求水準書「2.6 システム構成・機器構成」に記載のスペックを前提とする。

UI/可視化は職員業務に支障がない応答性を確保すること。応答性の評価方法は受託者提案とする。

⑶ 基本設計及び詳細設計（システム方式）

ア　基本設計

要求水準書の内容を確認し、「基本設計書（システム方式）」を作成し、県の承認を得ること。

基本設計書には非機能要件の設計、システム設計、業務継続設計を含むこと。

イ　詳細設計

基本設計書（システム方式）を踏まえ、詳細設計結果を記載した「詳細設計書（システム方式）」を作成し、県の承認を得ること。

詳細設計書には、非機能要件の実現方法、システム設定の詳細、業務継続の詳細設計を含むこと。

ウ　環境定義

構成・設定が再現できる資料を作成すること。環境構築手順は、手順書または IaC 等の再現手段のいずれかで提示すること。

⑷ 設計における留意事項

ア　ライフサイクルコストの考慮

設計段階で、運用・保守におけるコスト最適化を考慮した構成とすること。

イ　モニタリング性の確保

モデルの運用中における性能劣化（モデルドリフト）や入力データの分布変化（データドリフト）の検知を目的としたモニタリング機構の実装は任意提案とする。

4.5 開発・テスト

⑴ 開発手法

ア　柔軟な開発手法の採用

従来のウォーターフォール型開発に限定せず、スパイラル型、アジャイル型等、柔軟な対応が可能な開発手法を採用すること。

開発手法は受託者提案とし、必要に応じ県と協議のうえで決定すること。

イ　開発ツールの整備

受託者は、開発・テスト・運用に必要なツールを整備すること。使用するツールの選定及び運用方法は受託者提案とし、必要に応じて県と協議して決定すること。

⑵ 開発の実施

ア　開発作業の進行

受託者は、業務計画書に基づき、基本設計・詳細設計に従って開発作業を実施すること。進捗状況や課題を定期的に県へ報告すること。

イ　成果物の整備

開発により作成された実行ファイル、設定ファイル、スクリプト等は、実行可能な状態で整理し、納品時に提出すること。実行に必要な最小限の手順及び依存関係情報を含めること。

⑶ テスト計画と管理

ア　テスト計画の策定

受託者は、設計内容及び要求水準書に基づき、受入に必要な範囲でテスト計画を作成し、県と協議の上で確定すること。

テスト項目は、導入を計画している AI 特有のものを含めること。

イ　テストの実施と報告

テスト計画書に基づき、テストを実施し、結果を「テスト結果報告書」として整理すること。報告内容は、受入判断に必要な範囲（合否、主要不具合、KPI 結果等）とする。

ウ　不具合対応

テスト中に発見された不具合については、原因分析を行い、修正・再テストを実施すること。対応内容は記録し、重大な不具合については県に報告すること。

⑷ テストの実施

ア　中間テストの実施

本業務は２年間の構築期間を予定しており、１年目終了時点（令和９年１月末を目安）に中間テストを実施する。中間テストは、構築済みの予測モデル及びシステム機能について、過去の実測データを用いて性能・品質を評価し、KPI の達成状況を確認する。

(ｱ) 評価対象

・実装済みの主要機能
・モデルの予測精度、操作性等

(ｲ) 評価方法

・令和６～７年度の実測データ及び気象データを用いた再現評価
・評価結果は「テスト結果報告書（中間テスト編）」として整理し、県に提出する

イ　運用テストの実施

本格運用前に、実運用を想定した運用テストを実施する。運用テストでは、予測処理のタイムライン、通知機能、障害時の対応フロー、モデルの継続的な性能評価等について確認を行い、安定した運用が可能であることを検証する。

ウ　テストの自動化

テストの自動化は任意とする。受託者が自動化を行う場合は、対象範囲や方法を提案すること。

4.6 受入テスト支援

が実施する受入テストに対する受託者の支援内容及び範囲は、県が作成する受入テスト計画の確定時に県と協議の上で決定する。

⑴ 受入テスト計画への支援

ア　計画作成の支援

受託者は、県が受入テストの「テスト計画書」を作成する際に、必要な情報提供や助言を行うこと。

受託者は、以下の内容に関して支援を行う。

・テスト環境の仕様：受入テストで使用する環境の構成や設定情報

・テスト項目の提案：県から依頼があった場合に限り実施する

イ　テスト計画書の内容確認

受託者は県が作成した受入テスト計画書について、技術的観点から不明点の解消に協力する。内容の最終確定は県が行う。

⑵ 受入テスト実施の支援

ア　テスト環境整備の支援

受託者は、受入テストがスムーズに実施できるように以下を実施する。

（ｱ）テスト環境の準備

（ｲ）テスト結果等（テスト環境の仕様、テスト項目、テストデータなどを含む）の提供

イ　受入テスト中の技術支援

受託者は、受入テスト実施中、県からの技術的問い合わせに対応する。

障害対応は受託者の責に期す不具合に限り原因調査及び修正方針を提示

する。この場合、再テストの実施方法は県と協議の上で決定する。

⑶ 受入テスト後のテスト結果

ア　受託者が提供するテスト結果等

県が実施した受入テストの結果の判断に必要な範囲で、以下及び県が求めるテスト結果等を提供する。既存成果物（環境定義、環境構築手順、試験結果等）で代替できる場合は新規作成は不要とする。

(ｱ) テスト環境構築手順書

テスト環境の構築手順を記載した文書

(ｲ) テストデータ

受入テストで使用するデータ一式

イ　テスト結果の確認支援

受託者は、県が行う合否判断に必要な範囲で、テスト結果の解釈（原因の切り分け等）に協力する。

ウ　その他留意事項

受託者が提供するテスト結果のうち、証跡（ログ、スクリーンショット等）は重大機能・重大不具合に関するものに限り提供し、その他は結果一覧等で代替できるものとする。

4.7 引継ぎ

受託者は、県が必要と認める範囲で、運用・保守に必要な情報及び成果物の引継ぎを実施すること。

引継ぎ対象・基準・スケジュール等は県と協議して柔軟に運用する。

引継ぎ成果物は既存資産の活用・電子化・簡素化も可能とする。

必要に応じて、県職員や本格運用後の当該システムに係る保守点検会社に説明会を実施すること。

詳細は要求水準書「4.5 引継ぎに関する事項」参照。

4.8 教育に関する事項

受託者は、県職員が運用開始に必要な範囲で、本システムの操作・運用に関する教育（説明）を実施すること。

詳細は要求水準書「4.6 教育要件」参照。

4.9 会議開催

受託者は、県と業務の進捗状況、課題、成果物の現状を把握するため、定例会議及び必要に応じて臨時会議を開催すること。

詳細は要求水準書「4.2 県との連携・報告」参照。

4.10 データ管理方法

受託者は、別添「別記 データ保護及び管理に関する特記仕様書」に従い、本システムで取り扱うデータについて、保護及び管理を行うこと。

データ管理にあたっては、情報セキュリティ、バックアップ、アクセス制御、改ざん防止等に十分配慮し、県と協議のうえ管理体制を確定すること。

詳細は要求水準書「3.9 セキュリティ要件」参照。

4.11 業務完了報告書の作成

受託者は、年度ごとに以下の内容を含む「業務完了報告書」を作成し、県の承認を得ること。

なお、令和８年度実施分の「業務完了報告書」については、業務の進捗状況を考慮して作成すること。

「業務完了報告書」の提出期限は、令和８年度実施分は令和９年３月１７日までに、令和９年度実施分は令和１０年２月１５日までとする。

詳細は要求水準書「4.4 検査・確認」参照。

(1) 当該年度に実施した業務内容の概要

(2) 品質目標、品質評価基準、成果物の品質評価結果
(3) 実施した各工程の開始・終了日、計画との差異がある場合の理由
(4) 次年度に向けた技術的課題、対応方針、スケジュール等（８年度のみ）
(5) 運用テスト期間中に実施した監視の記録（稼働状況や予測精度等）、監視によって検出された異常、問題の年数及びこれらの問題に対する対応内容（再学習、閾値調整等）（９年度のみ）
(6) 業務の目的や達成すべき目標、評価基準、完了基準の達成状況及びその証拠（９年度のみ）
(7) サービス提供状況及び成果物の評価を踏まえた、受託者による本業務に対する総括（９年度のみ）
(8) その他必要な事項

4.12 成果物の作成及び提出

(1) 成果物一覧

成果物の一覧、提出時期、提出形式について、要求水準書「4.3 成果物一覧」に従うこと。提出スケジュールの調整が必要な場合は、県と協議のうえ業務計画書に反映すること。

(2) 成果物の納品方法

ア　成果物は、原則として日本語で作成すること。ただし、英字での表記が一般的な文言については、英字のままで差し支えない。
イ　情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。
ウ　電子データで納品する場合は、納品後、県において改変が可能となるよう、Microsoft Office 形式や図表等の元データも併せて納品すること。なお、業務効率化のために、ツールから出力される結果を成果物にしている場合は、県と協議の上でそれを納品することも可能である。
エ　成果物の作成に当たって、特別なツールを利用する場合は、県の承認を得ること。
オ　成果物が外部に不正に利用されたり、納品過程において改ざんされたりす

ることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

カ　電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

キ　受託者が保有する特許などを用いる場合には、成果物にその旨を明記すること。

ク　受託者は、要求水準書「4.3 成果物一覧」に指定された期限に向けて成果物の草案を準備し、内容について県と協議のうえ初版を期限内に納品し県の承認を得ること。

ケ　成果物については、必要に応じて更新し、県の承認を得て最終版とした上で、契約満了日までに成果物一式を納品すること。

4.13 契約金額の内訳書の提出

受託者は、契約後、本業務に係る契約金額の内訳書を別紙１により、提出すること。

内訳書には、以下の区分・項目ごとに年度別の費用を明記すること。

【区分及び項目例】

1. 初期構築費（１年目・２年目）
   - ・システム設計・開発費
   - ・パッケージソフト導入・改造費（自社/他社製の場合はシステム設計概要書を提出）
   - ・クラウド初期導入・設定費
   - ・成果物作成費（設計書、マニュアル等）
   - ・その他（通信費、データ購入費等）
2. 運用・保守費（１年目、２年目、３年目（見込））
   - ・クラウド利用料

・パッケージ使用料
・システム運用・保守費用
・障害対応・バックアップ・再学習等
・教育・引継ぎ費用

3. 年度別内訳
・1 年目費用（構築＋運用）
・2 年目費用（構築＋運用）
・3 年目以降の運用費用（年度あたりの見込まれる金額を記載）

将来拡張費用の区分は不要とする。

契約金額の明細提出の義務化はしないが、主要項目ごとに価格を明記すること。

内訳書の提出は、契約締結時及び年度更新・協議時にも、県が必要と認めた場合に再提出を求めることがある。

4.14 その他

受託者は、本業務に関し、県庁内関係部署及びシステム運用に関する関係者等から説明要請や質問等があった場合は、資料作成、回答等の対応支援を行うこと。

4.15 検査の実施

(1) 県は、年度ごとに受託者から提出された業務完了報告書及び納品物に基づき、検査を実施する。

(2) 令和８年度実施分の検査では契約書、仕様書、要求水準書に基づき、以下の観点から成果物の確認を行う。

ア　業務内容の履行状況

イ　成果物の品質、精度等の妥当性

ウ　中間テストの結果を踏まえた技術的課題等の妥当性

(4) 令和９年度実施分の検査では、契約書、仕様書、要求水準書に基づき、以下の観点から成果物の確認を行う。

ア　業務内容の履行状況

イ　成果物の品質、精度、再現性の妥当性

ウ　運用テスト及び受入テストの結果等の妥当性

(5) 検査の結果、修正が必要と判断された場合、受託者は速やかに対応し、再提出を行うこと。

(6) 検査に合格した時点で、年度ごとの業務は完了とみなされ、令和９年度の実施分の検査後は、検収手続きに移行する。

5 作業の実施体制・方法に関する事項

5.1 作業実施体制と役割

本業務における実施体制と役割、各役割に従事する実施者の氏名は業務計画書に記載し、提出すること。

作業要員が長期不在となる場合は、迅速に代替要員を加えること。詳細は、要求水準書「4.1 業務実施要件」参照。

5.2 作業要員に求める資格等の要件

情報セキュリティ責任者は、次のいずれかに該当すること。

ア　情報システムコントロール協会（ISACA）が認定する公認情報システム監査人（CISA）の資格保有者

イ　情報システムコントロール協会（ISACA）が認定する公認情報セキュリティマネージャ（CISM）の資格保有者

ウ　International Information Systems Security Certification Consortium が 認定するセキュリティプロフェッショナル認証資格(CISSP)の資格保有者

エ　情報セキュリティマネジメント試験合格者

オ　情報セキュリティに関する実務経験が３年以上ある者

カ　上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者。

5.3 作業場所

⑴ 設計・開発業務

設計・開発及びテスト等の作業場所は、受託者の責任において用意すること。その際は、必要に応じて県職員が現地確認を実施することができるものとする。

6 成果物に関する事項

6.1 知的財産権の帰属

本業務により作成される成果物（プログラム、設計書、ドキュメント、データ等を含むがこれに限らない）に関する知的財産権（著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条までに定めるすべての権利を含む。）は、以下の各号に定める場合を除き、すべて県に帰属するものとする。

⑴ 受託者が著作権を有するもの（本業務の契約前に著作権を有するものに限る。）であって、その全部又は一部を成果物として提供する場合には、県は業務における利用目的の範囲内でこれを改変し使用することができるものとする。

⑵ 納入する成果物に第三者が権利を有する著作物（以下「既存著作物」という。）が含まれる場合には、受託者は当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行なうものとする。この場合において、受託者は当該既存著作物の使用及び内容に関し、事前に県の承認を得ることとし、既存著作物が含まれる成果物については、当該使用許諾契約の範囲内で使用するものとする。

上記⑵の場合において，第三者との間に著作権に係る権利侵害の紛争が生じたときは、当該紛争の原因が専ら県の責に帰す場合を除き，受託者の責任及び負担により一切を処理するものとする。県は、係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力を講ずる。

6.2 検収

⑴ 本業務の受託者は、成果物等について、納品期日までに県に内容の説明を実施し、検収を受けること。

⑵ 検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行うこと。また、変更点について県に説明を行った上で、指定された日時までに再度納品すること。

7 その他特記事項

(1) 本システムで使用する機器やソフトウェア（ミドルウェア、ライブラリ）等を調達する際は、不正侵入の経路となるバックドアや脆弱性が含まれていないことを確認し、システム稼働中にメーカーサポートを受けられる安全なプロダクトを選定すること。
(2) 本業務においてライセンスの取得を要するソフトウェア等を利用する場合は、受注者の負担で必要数のライセンスを用意すること。
(3) 本業務において、県は新たな機器、通信回線等は用意しない。受注者の負担で必要な機器、通信回線等を調達すること。
(4) 本仕様書に定めのない事項は、双方で協議の上、定めることとする。
(5) 受託者からの提案事項についても、仕様に含めるものとする。
(6) 委託金の支払いについては原則として、年度ごとに清算払いとする。

8 附属文書

別記　データの保護及び管理に関する特記仕様書
別添１　要求水準書
別紙１　見積金額内訳書

別紙１

契約金額内訳書

（単位：円　税込み額）

項目		１年目	２年目	３年目(見込)※1
初期構築費	要件定義・基本設計			
	詳細設計・開発費			
	パッケージ改造費（該当時）			
	クラウド初期導入費			
	成果物作成費			
運用・保守費	クラウド利用料			
	パッケージ使用料（該当時）※2			
	システム運用・保守費			
	障害対応・バックアップ			
	教育費用			
	通信費			
	情報購入費			
	改修等開発費			
合計				

※１　３年目以降の単年度当たりの運用・保守費

※２　パッケージソフトを導入（又は改造して導入する場合も含む）する場合、契約後にシステム設計概要書を提出すること。

別記　データ保護及び管理に関する特記仕様書

第１　目的

本契約において取り扱う各種データについて、適正なデータ保護・管理方策及び情報システムのセキュリティ方策ついて明確にすることを目的とする。

第２　適用範囲

本契約を履行するに当たり、出版、報道等により公にされている情報を除き、千葉県（以下「発注者」という。）が交付若しくは使用を許可し、又は契約の相手方（以下「受注者」という。）が作成若しくは出力したものであって用紙に出力されたものを含む全ての情報（以下「電子データ等」という。）を対象とする。

第３　対象とする脅威

本書において対象とする脅威は、次に掲げる情報セキュリティが侵害された又はそのおそれがある場合とする。

（１）不正プログラムへの感染（受注者におけるものを含む。）

（２）サービス不能攻撃によるシステムの停止（受注者におけるものを含む。）

（３）情報システムへの不正アクセス（受注者におけるものを含む。）

（４）書面又は外部記録媒体の盗難又は紛失（受注者におけるものを含む。）

（５）機密情報の漏えい・改ざん（受注者におけるものを含む。）

（６）異常処理等、予期せぬ長時間のシステム停止（受注者におけるものを含む。）

（７）発注者が受注者に提供した又は受注者にアクセスを認めた発注者の電子データ等の目的外利用又は漏えい

（８）アクセスを許可していない発注者の電子データ等への受注者によるアクセス

（９）意図しない不正な変更等（受注者におけるものを含む。）

第４ 本契約を履行する者が遵守すべき事項

受注者は、本契約の履行に関して、以下の項目を遵守すること。

４．１ 業務開始前の遵守事項

受注者は、以下の（1）から（6）までの各項目に定める事項及び契約内容を一部再委託する場合は（7）に定める事項を取りまとめた「データ管理計画書」を作成し、業務開始前までに発注者の承認を得ること。

なお、行政手続き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（平成 25 年法律第 27 号）による個人番号及び特定個人情報（以下「特定個人情報等」という。）を取扱う業務の場合は、他の電子データ等と明確に区分して管理することとし、特定個人情報の適正な取扱いに関するガイドラインに基づく安全管理措置について、「データ管理計画書」の各事項へ、追加で記載すること。

（1）データ取扱者等の指定

受注者は、電子データ等を取り扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等を明確に管理するため、特定個人情報等を取り扱う者（以下「特定個人情報ファイル取扱者」という。）及び特定個人情報ファイル取扱者を統括する者（以下「特定個人情報ファイル取扱責任者」という。）についても併せて指定し、「データ取扱者等名簿」に記載すること。

なお、データ取扱者、データ取扱責任者、特定個人情報ファイル取扱者及び特定個人情報ファイル取扱責任者（以下「データ取扱者等」という。）は、守秘義務等のデータの取扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

（2）データ取扱者等への教育・周知計画

受注者は、データ取扱者等を対象とした、本契約での電子データ等の取扱いや漏えい防止等の教育及び周知に関する「データ取扱者等への教育・周知計画」を作成すること。

（３）電子データ等の取扱いにおける情報セキュリティ確保の措置計画

受注者は、本契約に係る電子データ等の取扱いに関し、電子データ等の保存、運搬、複製及び破棄並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画」を作成すること。「データ取扱計画」には、以下に示す措置を含めること。

（ア）本契約の作業に係る電子データ等を取り扱うサーバ、パソコン、モバイル端末について、アクセス制御及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

（イ）機密性２以上の電子データ等の取扱いは、発注者又は受注者のいずれかの管理下にない情報システム等（データ取扱者等の個人所有物であるパソコン及びモバイル端末を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（ウ）電子データ等名称、データ取扱者名、授受方法、使用目的、使用場所、保管場所、保管方法、返却方法、授受日時、返却日時、特定個人情報等の有無等を記録する「データ管理簿」を整備すること。

（エ）機密性２以上の電子データ等の保存に、発注者又は受注者のいずれかの管理下にない情報システム等又は電磁的記録媒体（データ取扱者等が私的に契約しているサービス及びデータ取扱者等の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（オ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者の作業に立ち会うなど適切な管理を行うこと。

（カ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者が作業を終了し作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

（キ）機密性２以上の電子データ等を電子メールにて送信する場合には、暗号化を行うこと。

（４）外部設置における情報セキュリティ確保の措置計画

受注者は、発注者が指定する場所以外に情報システム機器を設置（外部設置）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、部外者

の侵入等の意図的な情報漏えい等を防止する措置を記載した「外部設置における情報セキュリティ措置計画」を作成すること。「外部設置における情報セキュリティ措置計画」には以下に示す措置を含めること。

（ア）情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、受注者の管理下にあり、部外者の立入りが制限された場所において行うこと。

（イ）電子データ等を取り扱うパソコン、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないパソコン、モバイル端末等を用いた作業を制限すること。

（ウ）入退室記録、作業記録等を蓄積し、不正の検知、原因特定に有効な管理機能を備えること。

（５）外部接続における情報セキュリティ確保の措置計画

受注者は、発注者が指定するネットワーク以外のネットワークへ接続（以下「外部接続」という。）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、外部のネットワークからの侵入や改ざんを防御する措置を記載した「外部接続におけるセキュリティ措置計画」を作成すること。「外部接続におけるセキュリティ措置計画」には、以下に示す措置を含めること。

（ア）外部接続箇所にファイアウォールを設置し、不要な通信の遮断を行うこと。

（イ）外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断を行うこと。

（ウ）外部接続箇所で不正な通信を検出した場合、発注者へ通報を行うこと。

（６）情報セキュリティが侵害された又はそのおそれがある場合における対処手順

受注者は、本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、発生した場合の対処手順を記載した「情報セキュリティ侵害時対処手順」を作成すること。「情報セキュリティ侵害時対処手順」には、以下に示す対処を含めること。

（ア）作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、発注者に、口頭にてその旨第一報を入れること。発注者への第一報は、

情報セキュリティインシデントの発生を認知してから１時間以内に行うこと。

（イ）当該第一報が行われた後、発生した日時、場所、発生した事由、関係するデータ取扱者等を明らかにし、平日の午前９時から午後５時の間は１時間以内に、それ以外の時間帯は３時間以内に発注者に報告すること。また、当該報告の内容を記載した書面を遅延なく発注者に提出すること。

（ウ）発注者の指示に基づき、対応措置を実施すること。

（エ）発注者が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、発注者に提出すること。

（オ）再発を防止するための措置内容を策定し、発注者の承認を得た後、速やかにその措置を実施すること。

（７）再委託における情報セキュリティの確保の措置計画

受注者は、本契約内容について一部再委託（更に順次行われる再委託を含む。）する場合、受注者が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先において確保させる必要があり、再委託先における情報セキュリティの十分な確保を受注者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するため、「再委託における情報セキュリティ措置計画」を作成すること。なお、特定個人情報等を取扱う業務を再委託したときは、発注者が行う再委託先の管理状況等の確認について、受注者は必要な協力を行うこと。

４．２　業務実施中における遵守事項

（１）「データ管理計画書」に基づく情報セキュリティ確保

「データ管理計画書」に記載した、データ取扱者等への教育・周知、電子データ等の取扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

（２）データ管理簿への記録

受注者は、データ取扱者等が電子データ等を取り扱う場合、「データ管理簿」に記録し、データ取扱責任者に確認させること。また、特定個人情報等を扱う業務の場合、特定個人情報ファイル取扱責任者に併せて確認させること。

（３）「データ管理計画書」の変更

（ア）受注者は、本契約に基づく請負作業中に、次の事項について作業開始前に提出した「データ管理計画書」の内容と異なる措置を実施する場合は、事前に「データ管理計画書」の変更について発注者に提出し、承認を得ること。また、承認された変更の内容を記録し保存すること。

・データ取扱者等の異動を行う場合

・データ取扱者等に対する教育・周知の計画を変更する場合

・電子データ等の取扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合

・再委託先及び再委託先の情報セキュリティ対策を変更する場合

（イ）一時的に「データ管理計画書」とは異なる措置を実施する場合は、原則として事前にその旨を発注者へ提出し、承認を得ること。ただし、情報セキュリティが侵害された又はそのおそれがある場合など緊急を要する場合等の場合、受注者は、実施内容について事後速やかに発注者へ報告すること。

（４）業務の報告・監査等

（ア）受注者は、発注者へ業務実施中の「データ管理計画書」の遵守状況について定期的に報告すること。

（イ）受注者は、発注者が「データ管理計画書」に係る管理状況について監査を要請した時は、定期・不定期にかかわらず、これを受け入れること。

（ウ）受注者は、「データ管理計画書」の評価、見直しを行うとともに、必要な改善策等について、発注者へ提案すること。

（５）情報セキュリティ対策の履行が不十分であった場合の対応

受注者の本契約に係る作業における情報セキュリティ対策の履行が不十分であると発注者が判断した場合、受注者は発注者と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「データ管理計画書」に反映させること。

４．３ 業務完了時の遵守事項

（１）データ返却等処理

受注者は、本契約に基づく業務が完了したときは、「データ管理簿」に記録されている全てのデータについて、返却、消去、廃棄等の措置を行うものとし、処理の方法、日時、場所、立会者、作業責任者等の事項を記した、「データ返却等計画書」を事前に発注者へ提出し、承認を得た上で処理を実施すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等であることを「データ返却等計画書」に明示すること。

（２）作業後の報告

受注者は、「データ返却等計画書」に基づく処理が終了したときは、その結果を記載した「データ管理簿」を発注者へ提出すること。

（３）情報セキュリティ侵害の被害に関する記録類の引渡し

受注者は、本契約の業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、４．１（６）に基づいて取得し保存している記録類を発注者に引き渡すこと。

４．４ 記憶装置の修理及び廃棄等におけるデータ消去

受注者は、契約により発注者が利用する情報システム機器の修理及び廃棄、リース返却（以下、「廃棄等」という。）の場合、記憶装置から、全ての電子データ等を消去の上、復元不可能な状態にする措置（以下、「抹消措置」という。）を実施すること。

（１）抹消措置計画の作成

受注者は、「データ管理計画書」へ作業予定日時、作業予定場所、実施予定者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者などを記載した「抹消措置作業計画」を追加するとともに、必要に応じてその他の措置内容を変更したうえ、抹消措置実施日（賃貸借契約の場合は賃貸借期間満了日）の３０日前までに発注者に提出し、承認を得ること。

また、賃貸借契約の場合は賃貸借期間満了日から３０日以内に抹消措置実施日を設

定すること。

（２）抹消措置実施方法

ア マイナンバー利用事務系の領域において住民情報を保存する記憶媒体の抹消措置の方法

（ア）当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。なお、対象となる機器について、リース契約による場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行うこと。

（イ）職員が抹消措置の完了まで立ち会いによる確認を行う。ただし、庁舎外で抹消措置を行う場合は、庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の証拠写真が添付された完了証明書により確認できること。

イ 機密性２以上に該当する情報を保存する記憶媒体（上記アに該当するものを除く。）の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。

（イ）庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認できること。

ウ 機密性１に該当する情報を保存する記憶媒体の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態に消去すること。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

エ ＩｏＴ機器を含む特殊用途機器の抹消措置の方法

（ア）デジタル複合機などのＩｏＴ機器を含む特殊用途機器に保存された電子データ等の漏えいの対策について、国際標準に基づくセキュリティ要件と同等以上のセキュリティ要件とその要件に適合した第三者認証（「ＩＴ製品の調達におけるセキュリティ

要件リスト」適合製品など）を取得している機能を有する場合は、当該機能によるデータ消去をもって抹消措置とすることができる。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

（３）抹消措置の報告

受注者は、抹消措置実施日から３０日以内に、作業日時、実施者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者及び全ての記憶装置について抹消措置前後の写真を添付した「抹消措置完了報告書」を発注者へ提出し、承認を得ること。

第５ 情報システムの情報セキュリティ要件

受注者は、本契約により情報システムを導入する場合は、対象となる以下の項目を遵守すること。

５．１ 侵害対策

（１）通信回線対策

（ア）通信経路の分離

不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。

（イ）不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

（ウ）通信のなりすまし防止

情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

（エ）サービス不能化の防止

サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

（２）不正プログラム対策

（ア）不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

（イ）不正プログラム対策の管理

システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該

機能の動作状況及び更新状況を一元管理する機能を備えること。

（３）脆弱性対策

（ア）構築時の脆弱性対策

情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

（イ）運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。

５．２ 不正監視・追跡

（１）ログ管理

（ア）ログの蓄積・管理

情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、発注者が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

（イ）ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

（ウ）時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

（２）不正監視

（ア）侵入検知

不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

（イ）サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

５．３ アクセス・利用制限

（１）主体認証

情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、ＩＤ／パスワードの方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

（２）アカウント管理

（ア）ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

（イ）アクセス権管理

情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

（ウ）管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

５．４ 機密性・完全性の確保

（１）通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。

（２）保存情報の機密性確保

情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

（３）保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

５．５ 情報窃取・侵入対策

（１）情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

（２）侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

５．６ 障害対策（事業継続対応）

（１）システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハード

ウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

（２）システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

５．７　サプライチェーン・リスク対策

（１）受注者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、発注者が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

（２）調達する機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、発注者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

５．８　利用者保護

（１）情報セキュリティ水準低下の防止

情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

（２）プライバシー保護

情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。