別紙２

情報セキュリティの確保に関する基本仕様

Ⅰ　情報セキュリティポリシーの遵守

１　受託者は、情報セキュリティ管理体制を整備していること。

２　受託者は、本業務の従事者に対して、情報セキュリティ対策の教育を実施していること。

Ⅱ　受託者及び業務実施体制に関する情報の提供

１　受託者は、受託者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を本会からの要求に応じて提出すること。

なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（○○国籍の者が△名（又は□％）等）を記載すること。また、この場合であっても、本会からの要求に応じて、可能な限り要員に関する情報を提供すること。

２　受託者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを本会からの要求に応じて提出すること。

（１）ISO/IEC27001 等の国際規格とそれに基づく認証の証明書等

（２）プライバシーマーク又はそれと同等の認証の証明書等

（３）IPA が公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が４に達し、かつ各評価項目の成熟度が２以上であることが確認できる確認書

（４）MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績

Ⅲ　業務の実施における情報セキュリティの確保

１　受託者は、本業務の実施に当たって、以下の措置を講じること。また、以下の措置を講じることを証明する資料を本会からの要求に応じて提出すること。

（１）本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても第三者に開示及び本業務以外の目的で利用しないこと。

（２）本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。

（３）本業務の各工程において、本会の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（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、第三者機関による品質保証体制を証明する書類等を提出すること。）。

（４）本業務において、本会の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入調査等、本会と連携して原因を調査し、排除するための手順及び体制（例えば、システムの操作ログや作業履歴等を記録し、本会から要求された場合には提出するなど）を整備していること。

（５）本業務において、個人情報又は本会における要機密情報を取り扱う場合は、当該情報（複製を含む。以下同じ。）を国内において取り扱うものとし、当該情報の国外への送信・保存や当該情報への国外からのアクセスを行わないこと。

（６）本業務における情報セキュリティ対策の履行状況を定期的に報告すること。

（７）本会が情報セキュリティ監査の実施を必要と判断した場合は、本会又は本会が選定した事業者による立入調査等の情報セキュリティ監査（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 25 条第１項第２号に基づく監査等を含む。以下同じ。）を受け入れること。また、本会からの要求があった場合は、受託者が自ら実施した内部監査及び外部監査の結果を報告すること。

（８）本業務において、要安定情報を取り扱うなど、本会が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。

（９）本業務において、第三者に情報が漏えいするなどの情報セキュリティインシデントが発生した場合は、本会に対し、速やかに電話、口頭等で報告するとともに、報告書を提出すること。また、本会の指示に従い、事態の収拾、被害の拡大防止、復旧、再発防止等に全力を挙げること。なお、これらに要する費用の全ては受託者が負担すること。

（10）情報セキュリティ対策の履行が不十分な場合、本会と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。

２　受託者は、私物（本業務の従事者個人の所有物等、受託者管理外のものをいう。）の機器等を本業務に用いないこと。

３　受託者は、成果物等を電磁的記録媒体により納品する場合には、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、適切に対処するとともに、確認結果（確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等）を成果物等に記載又は添付すること。

４　受託者は、本業務において取り扱われた情報を、本会の指示に従い、本業務上不要となったとき若しくは本業務の終了までに返却又は復元できないよう抹消し、その結果を本会に書面で報告すること。

Ⅳ　情報システムの各工程における情報セキュリティの確保

１　受託者は、本業務において情報システムの運用管理機能又は設計・開発に係る企画・要件定義を行う場合には、以下の措置を実施すること。

（１）情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

ア　情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

イ　情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

(ア) 本会外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能

(イ) 不正プログラム感染や踏み台に利用されること等による本会外への不正な通信を監視する機能

（ウ）本会内通信回線への端末の接続を監視する機能

（エ）端末への外部電磁的記録媒体の挿入を監視する機能

（オ）サーバ装置等の機器の動作を監視する機能

（2）開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

ア　既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

イ　開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

ウ　セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。

エ　ソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を提供すること。

2　受託者は、本業務において情報システムの設計・開発を行う場合には、以下の事項を含む措置を適切に実施すること。

（1）情報システムのセキュリティ要件の適切な実装

（2）情報セキュリティの観点に基づく試験の実施

ア　ソフトウェアの開発及び試験を行う場合は、運用中の情報システムと分離して実施すること。

イ　試験項目及び試験方法を定め、これに基づいて試験を実施すること。

ウ　試験の実施記録を作成し保存すること。

（3）情報システムの開発環境及び開発工程における情報セキュリティ対策

ア　ソースコードが不正に変更されることを防止するため、ソースコードの変更管理、アクセス制御及びバックアップの取得について適切に管理すること。

イ　調達仕様書等に規定されたセキュリティ実装方針に従うこと。

ウ　セキュリティ機能の適切な実装、セキュリティ実装方針に従った実装が行われていることを確認するために、情報システムの設計及びソースコードを精査する範囲及び方法を定め実施すること。

エ　オフショア開発を実施する場合、試験データとして実データを使用しないこと。

3　受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、本会に報告し、協議の上、対策を講ずること。

4　受託者は、本業務において情報システムの運用・保守を行う場合には、情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。

（1）情報システムの運用環境に課せられるべき条件の整備
（2）情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
（3）情報システムの保守における情報セキュリティ対策
（4）運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策
（5）利用するソフトウェアのサポート期限等の定期的な情報収集及び報告
（6）情報システムの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポート継続中のバージョンでの動作検証及び当該バージョンで正常に動作させるための情報システムの改修等

5　受託者は、本業務において情報システムの運用・保守を行う場合には、運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。
（1）情報セキュリティに関わる運用保守体制の整備
（2）運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
（3）情報セキュリティインシデント（可能性がある事象を含む。以下同じ。）を認知した際の対処方法の確立

6　受託者は、本業務において情報システムのセキュリティ監視を行う場合には、以下の内容を含む監視手順を定め、適切に監視運用すること。
（1）監視するイベントの種類
（2）監視体制
（3）監視状況の報告手順
（4）情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順
（5）監視運用における情報の取扱い（機密性の確保）

7　受託者は、本業務において運用中の情報システムに脆弱性が存在することを発見した場合には、速やかに本会に報告し、本業務における運用・保守要件に従って脆弱性の対策を行うこと。

8　受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する者との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

9　受託者は、本業務において情報システムの運用・保守を行う場合には、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

10　受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。
（1）情報システム更改時の情報の移行作業における情報セキュリティ対策
（2）情報システム廃棄時の不要な情報の抹消

V　クラウドサービスに関する情報セキュリティの確保

受託者は、本業務において、クラウドサービスを活用する場合には、以下の措置を講じること。また、当該クラウドサービスの活用が本業務の再委託に該当する場合は、当該クラウドサービスに対して、Ⅷの措置を講じること。

1　ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、当該認証の証明書等の写しを本会からの要求に応じて提出すること。

2　クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを本会からの要求に応じて提出すること。

（1）ISO/IEC 27017 又は ISMS クラウドセキュリティ認証制度に基づく認証

（2）セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））

（3）情報セキュリティ監査により対策の有効性が適切であることを証明する報告書（クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 言明書等）

3　クラウドサービスにおいて個人情報又は本会における要機密情報が取り扱われる場合には、当該クラウドサービスのデータセンター（バックアップセンターを含む。）は国内に限ること。

4　クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前（サービス廃止等の１年以上前が望ましい。）に本会へ通知すること。

5　クラウドサービスの契約を終了する場合、クラウドサービス上に保存された本会のデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を本会に書面で報告すること。

6　クラウドサービスに係るアクセスログ等の証跡を保存し、本会からの要求があった場合は提供すること。なお、証跡は１年間以上保存することが望ましい。

7　インターネット回線とクラウド基盤との接続点の通信を監視すること。

8　クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者に外部委託されている場合は、当該クラウドサービス事業者以外の事業者にⅧの措置を講ずること。

9　クラウドサービスにおける脆弱性対策の実施内容を本会が確認できること。

10　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標（RPO）等の指標を提示すること。

なお、本会の要安定情報を取り扱う場合は、データセンターを地理的に離れた複数の地域に設置するなどの災害対策が講じられていること。

11　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

12　クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。

13　本業務において、本会に開示することとしているクラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。

14　本会に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、本会にお

いて、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。

Ⅵ　機器等に関する情報セキュリティの確保

受託者は、本業務において、本会にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等（以下「機器等」という。）を納品、賃貸借等をする場合には、以下の措置を講じること。

1　納入する機器等の製造工程において、本会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本会からの要求に応じて提出すること。

2　機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、本会と受託者が連携して原因を調査・排除できる体制を整備していること。

3　機器等の設置時や保守時に、情報セキュリティの確保に必要なサポートを行うこと。

4　利用マニュアル・ガイダンスが適切に整備された機器等を採用すること。

5　脆弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。

6　ISO/IEC 15408 に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを本会からの要求に応じて提出すること。

7　情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新版を採用するとともに、ソフトウェアの種類、バージョン及びサポート期限について報告すること。なお、サポート期限が事前に公表されていない場合は、情報システムのライフサイクルを踏まえ、販売からの経過年数や後継ソフトウェアの有無等を考慮して選定すること。

8　機器等の納品時に、以下の事項を書面で報告すること。

（1）調達仕様書に指定されているセキュリティ要件の実装状況（セキュリティ要件に係る試験の実施手順及び結果）

（2）機器等に不正プログラムが混入していないこと（最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等）

Ⅶ　管轄裁判所及び準拠法

1　本業務に係る全ての契約（クラウドサービスを含む。以下同じ。）に関して訴訟の必要が生じた場合の管轄裁判所は、国内の裁判所とすること。

2　本業務に係る全ての契約の成立、効力、履行及び解釈に関する準拠法は、日本法とすること。

Ⅷ　業務の再委託における情報セキュリティの確保

1　受託者は、本業務の一部を再委託（再委託先の事業者が受託した事業の一部を別の事業

者に委託する再々委託等、多段階の委託を含む。以下同じ。）する場合には、受託者が上記Ⅱの１、Ⅱの２及びⅢの１において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、本会の許可を得ること。

２　受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、本会又は本会が選定した事業者による再委託先への立入調査等の監査を受け入れるものとすること。

３　受託者は、本会からの要求があった場合は、再委託先における情報セキュリティ対策の履行状況を報告すること。

Ⅸ　資料等の提出

上記Ⅱの１、Ⅱの２、Ⅲの１、Ⅴの１、Ⅴの２、Ⅵの１及びⅥの６において提出することとしている資料等については、最低価格落札方式にあっては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式にあっては提案書等の総合評価のための書類に添付して提出すること。

Ⅹ　変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ及びⅧに関して、本会に提示した内容を変更しようとする場合には、変更する事項、理由等を記載した申請書を提出し、本会の許可を得ること。