別添

情報セキュリティに関する事項

Ⅰ 業務委託に係る対策

Ⅰ－１ 共通事項

（受注要件）

１　受注者は、本仕様書及び契約書に記載の情報セキュリティ対策を講ずること。

２　受注者は、本業務において取り扱う情報について、IPA が定める情報の格付及び取扱制限に従うとともに、以下の事項を遵守すること。

（１）業務の範囲に関する制限

本業務として許可された範囲内でのみ情報を取り扱い、本業務以外の業務においては利用しないこと。

（２）情報の取扱いに関する制限

本業務に必要な範囲内で当該情報を適切に取り扱い、放置や必要以上の複製、又は許可なく第三者へ提供するなどの行為を行わないこと。

（３）取扱場所等に関する制限

情報の格付及び取扱制限その他の特性に応じ、IPA が指定する場所及び環境においてのみ情報を取り扱うものとし、特に機密性の高い情報については、管理区域外で取り扱わないこと。

３　受注者は、一定以上の情報セキュリティ水準を確保するにあたり、情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC 27001」又は ISMS の認証を有し、当該認証が有効であること。

４　受注者は、本業務において取り扱う情報の適正な取扱いのための、情報セキュリティ対策の実施内容及び管理体制を整備すること。また、これらの体制について書類等により確認ができること。

（目的外利用の禁止）

５　受注者は、契約期間中及び契約終了後においても、本業務に関して知り得た IPA の業務上の情報について、他に漏らし、又は他の目的に利用してはならない。

（情報セキュリティインシデントへの対処方法）

６　受注者は、本業務の遂行において、情報セキュリティが侵害され、又はそのおそれがある場合の対処方法（対処手順、責任分界、対処体制等）について IPA に提示し、承認を得ること。

（情報の受渡し方法等）

７　受注者は、IPA との情報の受渡し、保存、運搬、送信について、IPA が承認した手順に従うこと。

（情報の廃棄方法等）

８　受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体並びにこれらの複製を含む。）について、IPA の指示に従い、本業務の実施期間中及び実施期間終了時

において、速やかに返却し、又は廃棄し、若しくは抹消するとともに、その実施結果を書面により報告すること。その際、IPA の確認を受けること。

（情報セキュリティ対策の遵守方法及び管理体制等に関する確認書の提出）

９　本業務の実施前までに、受注者は、以下の内容を含む情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書（別紙１）等を提出すること。また、変更があった場合は、速やかに再提出すること。

（１）本業務に携わる者の特定

（２）本業務に携わる者が実施する具体的な情報セキュリティ対策の内容

（本業務の実施期間中における情報セキュリティ対策）

10　受注者は、本業務の実施期間中において、以下の措置を含む情報セキュリティ対策を講ずること。

（１）受注者は、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合に、受注者が IPA に的確な報告を行いつつ、それらの事態に迅速かつ適正に対処できるよう、報告手順及び対処手順を確立し、維持すること。

（２）受注者は、IPA が提供する要保護情報等及びそれを取り扱う情報システムにアクセスする主体を特定し、それが正当な主体であることを検証するための主体の識別及び主体認証を行うこと。併せて、情報システムの特性及び取り扱う情報の格付や取扱制限に応じ、権限を有する者のみがアクセス可能となるよう、適切なアクセス制御を行うこと。

（３）受注者は、IPA が提供する要保護情報等を取り扱う情報システムへの不正アクセスを検知・抑止するためのログを取得・監視すること。また、要保護情報等にアクセスする全てのシステム利用者について、システム操作履歴を取得すること。

（４）受注者は、IPA が提供する要保護情報等を格納する装置、機器、記録媒体及び紙媒体の使用や保管に係る物理的保護対策を実施すること。

（５）受注者は、本業務に従事する従業員等及び IPA が提供する要保護情報等を取り扱う情報システムにアクセスを許可する従業員等に、業務上遵守すべき情報セキュリティ対策に関する事項を確実に認識させること。

（６）受注者は、IPA が提供する要保護情報等を取り扱う情報システムに用いる機器等について、ソフトウェアバージョン及び設定情報の文書化並びに変更による悪影響の防止等の適切な構成管理を実施すること。また、要保護情報等を取り扱う情報システムの運用管理で用いるツール、技法、仕組み及び要員を組織的に管理するとともに、当該情報システムの運用並びに情報の処理、保管及び送信に伴うリスクについて継続的に評価すること。

（７）受注者は、IPA が提供する要保護情報等を取り扱う情報システムが接続するネットワークの外部境界及び主要な内部境界において、通信又は送受信データを監視し、制御し、保護すること。

（８）受注者は、IPA が提供する要保護情報等を取り扱う自らの組織における情報セキュリティ対策を評価し、必要な是正を行うこと。

（情報セキュリティ対策の履行状況の報告）

11　契約期間中において定期的に、情報セキュリティを確保するための体制及び対策等に係る実施状況（「情報セキュリティに関する事項に係る実施状況報告書」（別紙２））を IPA に提出すること。なお、報告の内容について、IPA が不十分であると認めた場合、受注者は、速やかに IPA と協議し対策を講ずること。

また、本業務の実施終了時には、本業務の実施期間を通じて、情報セキュリティ対策が適切に実施されたことを「情報セキュリティに関する事項に係る実施状況報告書」（別紙２）により報告すること。

（情報セキュリティ対策の履行が不十分な場合の対処方法）

12　情報セキュリティ対策の履行が不十分であると認められる場合、受注者は、IPA と協議の上、必要な改善策を策定し、合意した内容に基づき速やかに当該改善策を実施すること。

また、当該事象を認知した場合には、速やかに IPA に報告し、原因究明及び対処について IPA の指示に従うこと。

（再委託先における情報セキュリティの確保）

13　受注者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）する場合は、再委託に伴い生ずる脅威に対して情報セキュリティが十分に確保されるよう、５から 13 までに定める事項について、契約等により再委託先に遵守させること。また、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に必要な資料を IPA に提供し、IPA の承認を受けること。

（その他の必要な対策）

18　情報セキュリティの観点から、本仕様書で定める要件以外に必要な措置がある場合には、IPA と受注者が協議の上、当該措置を決定するものとする。受注者は、当該決定内容に従い、必要な対策を講ずること。

（情報セキュリティ対策に係る提出書類）

19　情報セキュリティ対策に関する提出書類は下表のとおりとする。変更があった場合は、速やかに再提出すること。

なお、提出書類には再委託先に係るものも含むこととする。

提出時期	提出書類
契約締結前まで （入札説明書に定める提出期限）	①　３の「情報セキュリティ水準」を証明する資料 ②　４の「情報セキュリティ対策の実施内容及び管理体制」 ③　６の「インシデント発生時の対処方法」
本業務の実施前まで	９に関する確認書等
本業務の実施期間中及び業務終了時	①　８の情報資産の返却・廃棄・消去に関する証明書等 ②　11 の「情報セキュリティに関する事項に係る実施状況報告書」（別紙２）

Ｉ－２　クラウドサービスの選定・調達を外部委託する場合の対策

（ISMAP クラウドサービスリストからの選定）

１　受注者は、要機密情報を取り扱うクラウドサービスを提供事業者又は販売代理店等から調達する場合には、「政府情報システムのためのセキュリティ評価制度（ISMAP)」のISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから選定し、調達すること。

やむを得ず、ISMAP クラウドサービスリスト等に登録されていないクラウドサービスを調達する場合には、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（３桁の番号で表現される項目）及び末尾にＢが付された詳細管理策（４桁の番号で表現される項目）を原則として全て満たしていることを証明する資料（IPA から別途様式を提供する）を提出し、IPA の承認を得ること。

（情報が保存される国・地域及び契約に定める準拠法等）

２　クラウドサービスで取り扱う情報が保存されている場所が国内か、国外であってもそこで情報を取り扱うことのリスクを判断するための情報が十分提供されており、そのリスクが許容できる範囲内であると判断できる場所であること。また、クラウドサービスの契約に定める準拠法が国内法であること。

（情報セキュリティに関する役割及び責任の範囲）

３　クラウドサービス提供者と利用者との責任分担及び情報セキュリティ対策に関する責任範囲が、契約、約款又は SLA 等により明確化されていること。また、サービス障害又は情報セキュリティインシデント発生時の対応方針が文書として確認可能であること。

（クラウドサービスの利用終了時における対策）

４　受注者は、クラウドサービスの利用終了に際して、以下の情報セキュリティ対策を講ずること。また、クラウド基盤上から抹消されていることを IPA が確認可能な方法で証明すること。

（１）更改・廃棄時における情報の廃棄

①　クラウドサービス上で取り扱った全ての情報を当該クラウドサービス基盤上から確実に抹消すること。

②　暗号化消去が実施できない場合は、サービスの基盤となる装置等をセキュアな方法で処分する又は再利用のための方針及び手順に基づいて確実に実施すること。

（２）更改・廃棄時におけるアカウントの廃棄

①　作成されたクラウドサービス利用者アカウントをすべて削除すること。

②　上記①を確認したうえで利用したクラウドサービスにおける管理者アカウントを削除すること。また、当該アカウントを再利用できないよう措置を講じなければならない。

③　ストレージアカウント等のクラウドサービス利用者アカウント以外の特殊なアカウントを作成した場合には、当該アカウントを削除するとともに、当該アカウントを利用して作成された情報についても廃棄すること。