安否確認・災害情報配信システムの利用
要求仕様書

１．はじめに

自然災害（地震、津波、台風等）発生後、中央省庁は、国家的判断や広域的調整の中心的役割を果たす組織であり、発生状況等に関する情報を正確かつ早急に把握した上で、速やかに緊急業務（災害復旧・復興業務の一部や自然災害発生後に新たに発生する他の緊急業務）に着手することが必要である。その際に、職員の安否確認は、緊急業務遂行のための人的資源確保の前提となることから、組織として実施すべき重要な業務と位置づけられる。

安否確認・災害情報配信システム（以下「本システム」という。）は、インターネットに接続可能な携帯電話及びパソコン等情報通信機器にて、自然災害発生時における経済産業省（以下「当省」という。）の職員（以下「利用者」という。）の安否確認及び情報全般の配信を迅速に行うためのシステムであり、本要求仕様書は、その利用に係るサービス（以下「本サービス」という。）の整備を行うものである。

また、弾道ミサイル情報に基づき、万が一日本の領土内に着弾した場合も想定した、安否確認を迅速に行える仕組みも整備する。

さらに、昨今の海外情勢のリスク高騰に基づき、海外出張者、赴任職員に対する安否確認状況も把握する必要がある。海外出張者、赴任者の渡航情報管理、海外リスク情報把握、安否確認サービスを行える仕組みを、上記国内の仕組みとは別途整備を行うものとする。

２．システム要件

本システムは、ＡＳＰサービス型のシステムであること。

３．機能要件（国内向け）

（１） 基本機能

ａ．利用者への電子メールの一斉配信（以下「一斉配信」という。）に対し、利用者より応答が可能なこと。

電子メール送信は災害発生等により，ネットワークが混雑している場合でも，携帯電話会社（大手３キャリア）で制限されることなく本システムの役務請負業者（以下「受注者」という。）から携帯電話会社へ電子メールが送信されること。また、受注者と主な携帯電話会社の間で輻輳規制を受けない、特定接続が行われていること。

ｂ．システム障害や輻輳等で電子メールの利用が困難な場合、利用者がＩＤ・パスワード等の個人認証コードを入力しなくても、簡易にかつ自主的に安否、登庁可否等の項目を報告可能なこと。

ｃ．インターネットに接続可能な携帯電話からの利用は、日本国内でサービスを提供している全てのキャリアの機種に対応していること。

ｄ．一斉配信は、安否確認以外の目的でも容易に利用可能であり、システムの管理権限を付与された利用者（以下「システム管理者」という。）により一斉配信可能なこと。

ｅ．利用者を、複数階層グループで管理が可能なこと。また、グループごとに管理者（以下「グループ管理者」という。）を設定可能なこと。（以下、システム管理者とグループ管理者を併せて「管理者」という。）

ｆ．１利用者につき１つ以上の地域を登録可能なこと。

ｇ．１利用者につき１つ以上の電子メールアドレスを登録可能なこと。

ｈ．１利用者につき１０以上のグループに属することが可能なこと。

ｉ．１利用者につき１つのＩＤと利用者名が登録可能なこと。

（以下、利用者に関するｅ．～ｉ．の情報を「利用者データ」という。）

ｊ．利用者の応答状況について、応答済、未回答等の項目ごとに、配信数に対し集計を行い、管理者により集計結果が容易に確認可能なこと。

ｋ．当省があらかじめ設定した震度以上の地震が発生した場合、当省のシステム管理者に代わり、受注者が安否確認メールの代行送信を直ちに行うこと。

同時期に発生した複数の災害に対して，複数災害事象として同時に管理ができ、各々の事象ごとに安否確認が行えること。

大規模地震が発生した場合、気象庁発表情報を元に、単にシステム的に安否確認メールを送信するのではなく、誤報情報か否か等の情報の正確性を判断するための人による判断を行い、安否確認メールを送信できる仕組みであること。

大規模地震の際、余震については一定の判断の下で，本震とした一つの事象として管理が可能であり、余震発生の毎に不要な安否確認メールが送信されない工夫がされていること。

ｌ．指定する利用者に対して、当省があらかじめ設定した震度以上の地震が発生した場合、地震速報情報として発生時刻、予測規模等の情報を自動的に配信する機能を有すること。

ｍ．指定する利用者に対して、当省があらかじめ設定した震度以上の地震が発生した場合、気象庁の地震情報をもとに、発生時刻、確定震度、確定震源地（都道府県単位）等の情報（以下「地震確定情報」という。）を自動的に配信する機能を有すること。

ｎ．指定する利用者に対して、津波、台風等の災害関連情報（以下、「地震以外の自然災害情報」という。）を自動的に配信する機能を有すること。

ｏ．弾道ミサイル情報（国民保護に関する情報） でミサイルが日本の領土・領海に落下した場合又は、ミサイル落下場所等の都道府県が発表された場合、受注者は、職員があらかじめ登録した携帯電話等の電子メールアドレスに安否等を確認する一斉電子メールを送信する。一斉電子メール送信の対象者は、大規模地震発生時の都道

府県の設定と同一の対象者とする。

（２） システム管理者機能

ａ．利用者を対象とした、一斉配信用電子メールの作成・送信が容易に可能なこと。

ｂ．インターネットに接続可能な携帯電話及びパソコン等情報通信機器から一斉配信、安否状況確認等の操作が容易に可能なこと。

ｃ．安否、登庁可否等の設問及びそれに対する回答の文面を任意に設定が可能なこと。

ｄ．利用者が、一斉配信に対して未応答等であった場合、該当者のみに対して再度の一斉配信が容易に可能なこと。

ｅ．一斉配信の送信履歴確認が容易に可能なこと。

ｆ．利用者個別指定及びグループ指定による一斉配信が可能なこと。

ｇ．グループへの利用者の追加・削除及び変更が簡易に行える機能を有すること。

ｈ．利用者の電子メールアドレスの登録状況が容易に確認可能なこと。

ｉ．登録してある各利用者の電子メールアドレスが有効であるか無効であるか、定期的にシステムが確認し、その結果をシステム管理者が閲覧可能である機能を備えていること。

ｊ．システム管理者による利用者データの一括登録・更新が容易に可能なこと。

ｋ．システム管理者による利用者データの一括ダウンロードが容易に可能とすること。

ｌ．利用者データをダウンロードする場合、利用者の電子メールアドレスは、システム管理者であっても抽出不可であること（ドメイン部分を除く）。

（３） グループ管理者機能

ａ．システム管理者とは別に、グループ管理者を１，０００人以上設定可能なこと。

ｂ．１つのグループに２人以上のグループ管理者を登録可能なこと。

ｃ．設定された配下のグループ情報のみ閲覧・管理とすること。

ｄ．設定された配下のグループの職員の応答内容に対し、返答が可能なこと。

４．機能要件（海外向け）

（１） 基本機能

ａ．リスク情報配信機能大手通信会社など、海外で発生しているリスク情報を、所定の管理者と、渡航者へ電子メールで送信可能であること。

なお、配信するリスク情報は、多数の死傷者／行方不明者や邦人の関与が認められるケース、クーデターや非常事態など危機管理上重要な速報記事などを中心に送信すること。

ｂ．海外渡航者の管理機能システム管理者が国別に渡航情報を登録、閲覧することが可能であること。

ｃ．安否確認サービス機能上記ａ．で発生したリスク情報と連動して、国別の渡航情報に基づき、管理者機能にて安否確認を行う電子メールの送信が可能であること。また、上記リスク情報とは連動せず、渡航情報から安否確認を行うことも可能とする。

（２） システム管理者機能

ａ．インターネットに接続可能な携帯電話及びパソコン等情報通信機器から一斉配信、安否状況確認等の操作が容易に可能なこと。ただし、リスク情報内容表記は日本語表記が可能な通信機器のみとする。

ｂ．利用者が、一斉配信に対して未応答等であった場合、該当者のみに対して再度の一斉配信が容易に可能なこと。

ｃ．一斉配信の送信履歴確認が容易に可能なこと。

ｄ．利用者の電子メールアドレスの登録状況が容易に確認可能なこと。

ｅ．システム管理者による利用者データの一括登録・更新が容易に可能なこと。

ｆ．システム管理者による利用者データの一括ダウンロードが容易に可能とすること。

ｇ．利用者データをダウンロードする場合、利用者の電子メールアドレスは、システム管理者であっても抽出不可であること（ドメイン部分を除く）。

５．性能要件（国内向け）

（１） １１，５００人以上に対し、簡易的な操作で一斉配信が可能なこと。

（２） 地震速報情報は、地震発生から３分程度にて配信が可能なこと。

（３） 地震確定情報は、気象庁よる地震確定後１０分程度にて配信が可能なこと。

（４） 地震以外の自然災害情報は、災害発生から１０分程度にて配信が可能なこと。

（５） 弾道ミサイル情報（国民保護に関する情報）は、所要の要件を満たした時から可及的速やかに配信が可能なこと。

（６） 上記（２）～（５）の内容について、提供の内容を確認するまでに要する時間が要求時間を大幅に超えた場合は、原因を究明し、再発防止対策を講じるとともに遅滞なく経済産業省大臣官房秘書課及び大臣官房業務改革課情報システム室に報告を行うこと。

（７） 大量の一斉電子メール配信時における輻輳対策を講じること。

６．性能要件（海外向け）

（１） 約５００人に対して、利用可能であること。

（２） 海外リスク情報は、受注者が海外リスク情報を把握後、速やかに電子メール送信可能とすること。

７．信頼性要件

（１） 災害発生時に主たる拠点が倒壊し、サービス提供が出来なくなった場合は、本サービスを停止することなく別の拠点にてサービス提供が可能なこと。

（２） 新機種の携帯電話及びパソコン等情報通信機器が発売された場合には、新機種においても、本システムが利用可能になるよう対応を行うこと。

（３） 震度５強以上の地震発生時に１１，０００人以上の対象人員に対して地震速報情報及び安否確認を電子メールで滞りなく配信した実績を有すること。

８．セキュリティ要件

（１） 業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、別記「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

（２） 情報漏洩対策として、本システムに利用者がアクセスした際に受信する情報は受信者側の端末に蓄積させないこととし、原則サーバ側に蓄積させた情報を、受信者側から参照可能なこと。

（３） 個人情報や管理機能部分においては、ＳＳＬ／ＴＬＳによる暗号化機能を付加したプロトコルでサーバとブラウザ間の通信を暗号化すること。

（４） 本システムへの不正ログインを防止する機能を有していること。

（５） 本システムをＡＳＰサービスで提供するに当たり、ＡＳＰサービスが用いるシステム・データ領域は当省専用とすること。

（６） 提供された当省専用のシステム・データ領域については、当省職員及び当省向け本システムの保守・運用監視のために必要な者のみアクセス可能とする対策を講じること。

（７） ＩＳＭＳ若しくはＩＳＯ２７００１を取得していること。又はＪＩＳ Ｑ １５００１に適合したマネジメントシステムを有することについて、第三者の制度による認証を受けていること。

（８） 受注者は、本サービスの契約（以下「本契約」という。）内容の全部又は一部を第三者に再請負しないこと。

（９） 個人情報の取扱については以下のとおり定める。

ａ．受注者は、本契約の締結及び実施に当たり知り得た当省の機密情報を契約期間中であるか契約終了後であるかを問わず、一切第三者に漏洩してはならない。

ｂ．受注者は、機密情報を取り扱う場合、管理者を定め、本契約の目的に限り、使用又は利用可能とすること。

ｃ．受注者は、個人情報を機密情報と同等以上として扱い、細心の注意義務をもって管理し、知る必要のある従業員（以下「関係者」という。）のみに必要最小限の範囲で開示するものとし、その他の従業員には開示しないこと。

ｄ．受注者は、関係者（個人情報の開示を受けた後、退職した者も含む。）に対し、上記ｃ．で定める受注者の義務と同等の義務を負わせるものとすること。

ｅ．受注者は、本契約が終了した場合又は本契約の目的に必要でなくなった場合には、当該機密情報及び個人情報を復元できない形で直ちに廃棄又は削除し、それを証明する資料、及び別紙の確認書を経済産業省大臣官房秘書課へ提出すること。

ｆ．受注者は、電気通信事業における個人情報保護に関するガイドライン（最終改正令和６年３月１２日個人情報保護委員会・総務省告示第５号）を遵守すること。

９．保守・運用監視要件

（１） ２４時間３６５日、本サービスの運用監視及び保守を行うこと。

（２） 本サービス提供期間中、本サービスの利用全般に対し、障害等が発生した場合には、責任をもった原因の特定・切り分け、対処案の策定のための速やかな情報提供を経済産業省大臣官房秘書課及び大臣官房業務改革課情報システム室へ行うとともに、受注者の負担で障害等の対応を行うこと。

（３） 定期的に、当省が指定した特定のシステム管理者宛に訓練用の災害通知メールを送信し、正常に電子メールが受信されていることを確認すること。

１０．データセンター要件

（１） 本サービスは、国内２か所以上のデータセンター内に配置されたシステムで提供されるサービスであること。

（２） 相互のデータセンター間は、概ね３００ｋｍ以上離れていること。

（３） 本サービス提供のための主たる拠点となるデータセンターについては災害監視及びシステム監視要員が常駐し、２４時間及び３６５日、データセンターの運用監視及び保守を行うこと。

（４） 本サービスを提供するデータセンターは以下の耐震強度を有すること。

① 主たる拠点：震度７相当の地震で建物が倒壊しないこと。

② 別の拠点：震度６相当の地震で建物が倒壊しないこと。

１１．利用者数

＜国内向け＞

システム管理者数	３５人
グループ管理者数	１，０００人
同時アクセス可能管理者数	５００人
安否確認利用者数	１１，５００人
地震速報情報利用者数	２５０人
地震確定情報利用者数	２５０人

災害関連情報利用者数	２５０人

＜海外向け＞

システム管理者数	５人
グループ管理者数	１０人
同時アクセス可能管理者数	１０人
安否確認利用者数	５００人

１２．導入期間

令和７年４月１日（火）から令和８年３月３１日（火）まで、本サービスを実現可能とすること。

１３．納品物品監査

（１） 操作説明書（システム管理者用、グループ管理者用）

（２） 操作説明書（利用者用）

（３） 環境設定書等

以上を保管した電子媒体を１部

なお、電子媒体は、ＩＳＯ２６３００（ＯＤＦ）形式又はＩＳＯ１９００５－１（ＰＤＦ／Ａ）のファイルをＩＳＯ９６６０のファイルシステムにフォーマットされたＣＤ又はＤＶＤに記録して納入すること。

また、納入物品であるＣＤ又はＤＶＤの表面には件名及び納入年月日を明記すること。

１４．納入場所

経済産業省大臣官房秘書課

１５．その他

（１） 当省からサービスの提供に関する運用上必要な情報の提示について要求があった場合には速やかに対応すること。

（２） 上記（１）で開示出来ない情報が発生した場合には、開示出来ない明確な理由を提示すること。

（３） 当省が改善の余地有りと判断した事項については、当省と協議の上で改善に必要な措置を速やかに講ずること。

（別記）

情報セキュリティに関する事項

以下の事項について遵守すること。

【情報セキュリティ関連事項の確保体制および遵守状況の報告】

1）受注者（委託契約の場合には、受託者。以下同じ。）は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下 2)～17)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、経済産業省（以下「当省」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（別紙））を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

なお、報告の内容について、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

【情報セキュリティ関連規程等の遵守】

2）受注者は、「経済産業省情報セキュリティ管理規程（平成 18･03･22 シ第 1 号）」、「経済産業省情報セキュリティ対策基準（平成 18･03･24 シ第 1 号）」及び「政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）」（以下「規程等」と総称する。）を遵守すること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

3）受注者は、当省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

【情報セキュリティを確保するための体制】

4）受注者は、本業務に従事する者を限定すること。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示すること。

5）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、再委託されることにより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、1)から 17)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

【情報の取扱い】

6）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であってこれらの複製を含む。）の取扱いには十分注意を払い、当省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

7）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）について、担当職員の許可なく当省外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

8）受注者は、本業務を終了又は契約解除する場合には、受注者において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であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

9）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当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

　なお、当省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

【情報セキュリティに係る対策、教育、侵害時の対処】

10）受注者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

11）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について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

【クラウドサービス】

12）受注者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、2)に掲げる規程等で定める不正アクセス対策を実施するなど規程等を遵守すること。

13）受注者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「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調達することを原則とすること。

14）受注者は、前 2 項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用】

15）受注者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること。

①各工程において、当省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。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

③不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。 また、以下を含む対策を行うこと。

(a) 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。
(b) 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。
(c) 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。
(d) 不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。
(e) EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

④情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた、又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

⑥受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。

⑦ウェブサイト又は電子メール送受信機能を含むシステム等の当省外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。

⑧外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。
・サービス開始前および、運用中においては年１回以上、ポートスキャン、脆弱性検

査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。

なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

⑨電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともにSMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

【アプリケーション・コンテンツの情報セキュリティ対策】

16）受注者は、アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。

①提供するアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。

(a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

(b) アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。

(c) 提供するアプリケーション・コンテンツにおいて、当省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。

②提供するアプリケーション・コンテンツが脆弱性を含まないこと。

③実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

④電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政

府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

⑥当省外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当省外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。

17）受注者は、外部に公開するウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

別紙

令和　　年　　月　　日

経済産業省○○○課長　殿

住　　所
名　　称
代 表 者 氏 名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

情報セキュリティに関する事項１）の規定に基づき、下記のとおり報告します。

記

１．契約件名等

契約締結日	
契約件名	

２．報告事項

項目	確認事項	実施状況
情報セキュリティに関する事項２）	本業務全体における情報セキュリティの確保のため、「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年度版）、「経済産業省情報セキュリティ管理規程」（平成１８・０３・２２シ第１号）及び「経済産業省情報セキュリティ対策基準」（平成１８･０３･２４シ第１号）（以下「規程等」と総称する。）に基づく、情報セキュリティ対策を講じる。	
情報セキュリティに関する事項３）	経済産業省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行う。	
情報セキュリティに関する事項４）	本業務に従事する者を限定する。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報を担当職員に提示する。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示する。	
情報セキュリティに関する事項５）	本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して情報セキュリティに関する事項１）から１７）までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。	
情報セキュリティに関する事項６）	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であってこれらの複製を含む。）の取扱いには十分注意を払い、経済産業省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に経済産業省の担当職員	

	（以下「担当職員」という。）の許可を得る。 なお、この場合であっても、担当職員の許可なく複製しない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項７）	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）について、担当職員の許可なく経済産業省外で複製しない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明する。	
情報セキュリティに関する事項８）	本業務を終了又は契約解除する場合には、受注者において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であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。	
情報セキュリティに関する事項９）	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経済産業省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。 なお、経済産業省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供する。	
情報セキュリティに関する事項１０）	本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施する。	
情報セキュリティに関する事項１１）	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について担当職員に提示する。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従う。	
情報セキュリティに関する事項１２）	本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、「情報セキュリティに関する事項２）」に定める不正アクセス対策を実施するなど規程等を遵守する。	
情報セキュリティに関する事項１３）	本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「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調達することを原則とすること。	
情報セキュリティに関する事項１４）	情報セキュリティに関する事項１２）及び１３）におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。	
情報セキュリティに関する事項１５）	情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施する。 （１）各工程において、当省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。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。 （２）情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。 （３）不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。また、以下を含む対策を行うこと。 ①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。 ②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。 ③不正プログラム対策ソフトウェア等の設定変更権限については、システム	

	管理者が一括管理し、システム利用者に当該権限を付与しないこと。 ④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。 ⑤EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。 （４）情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。 （５）サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。 （６）受注者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。 （７）ウェブサイト又は電子メール送受信機能を含むシステム等の当省外向けシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「．ｇｏ．ｊｐ」を使用すること。 （８）外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。 ・サービス開始前および、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。 ・インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。 ・必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。 （９）電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともに SMTP によるサーバ間通信の TLS（SSL）化や S/MIME 等の電子メールにおける暗号化及び電子署名等により保護すること。	
情報セキュリティに関する事項１６）	アプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行う。 （１）提供するアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。 ①アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。 ②アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。 ③提供するアプリケーション・コンテンツにおいて、当省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。 （２）提供するアプリケーション・コンテンツが脆弱性を含まないこと。 （３）実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。	

	（４）電子証明書を用いた署名等、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。 （５）提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。 （６）当省外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をアプリケーション・コンテンツに組み込む場合は、当省外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該アプリケーション・コンテンツに掲載すること。	
情報セキュリティに関する事項１７）	外部公開ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に従う。また、ウェブアプリケーションの構築又は改修時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施する。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出する。 なお、チェックリストの結果に基づき、担当職員から指示があった場合には、その指示に従う。	

記載要領

１．「実施状況」は、情報セキュリティに関する事項２）から１７）までに規定した事項について、情報セキュリティに関する事項１）に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。

２．上記に記載のない項目を追加することは妨げないが、事前に経済産業省と相談すること。

（この報告書の提出時期：定期的（契約期間における半期を目処（複数年の契約において