情報セキュリティ対応の見直しについて（コンサルタント等契約、その他役務の提供等にかかる契約）説明会資料

2025/1/29

国際協力機構
情報システム部、国際協力調達部

本日の内容

１．改正の背景・経緯

２．サプライチェーン・リスクへの対応

３．受託者の皆様に求める情報セキュリティ対策等

４．適用対象案件

５．契約書雛形改正の主なポイント

６．コンサルタント等契約　関連ガイドライン/様式の変更点

７．その他役務の提供等にかかる契約関連様式の変更点

８．質疑応答

1-1.今次改正の背景・経緯（１）

- 近年、サイバー攻撃が急増し、攻撃手法も巧妙化・高度化している。

国立研究開発法人情報通信研究機構（NICT）が運用している大規模サイバー攻撃観測網（NICTER）における**サイバー攻撃関連の通信数の推移**

出典
総務省｜令和6年版 情報通信白書｜サイバーセキュリティ上の脅威の増大において、国立研究開発法人情報通信研究機構「NICTER観測レポート2023」を基に作成されたものを引用

1-1.今次改正の背景・経緯（２）

- 特に、**サプライチェーンの弱点を悪用した攻撃**が増えている。

情報セキュリティ10大脅威 2024

IPA

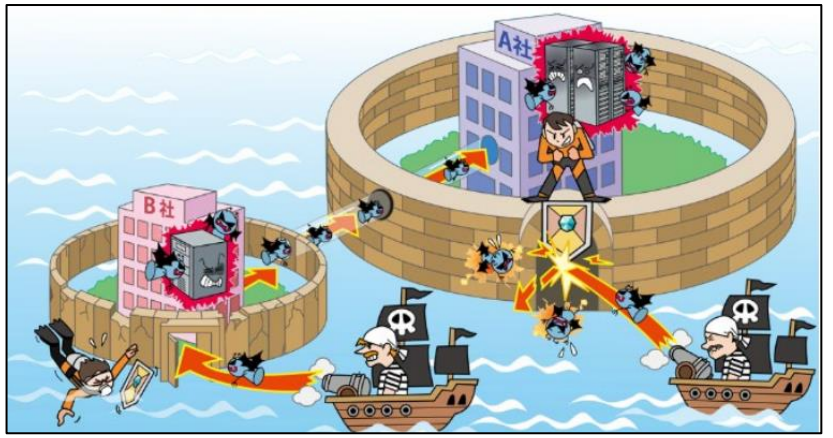
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した脅威	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2017年	2年連続2回目

出典
情報セキュリティ10大脅威 2024 簡易説明資料 [組織編]（独立行政法人情報処理推進機構（IPA））

1-2.サプライチェーン・リスクについて

- 調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足がかりとして攻撃され、情報漏えい等が起きるリスクを、「**サプライチェーン・リスク**」と呼ぶ。

引用：情報セキュリティ10大脅威 2024 簡易説明資料 [組織編] (ipa.go.jp)



- 想定されるサプライチェーン・リスクの脅威例
  - JICAの秘密情報を取扱う受託者又は再受託者が攻撃され、委託先又は再委託先が取り扱っているJICAの秘密情報が窃取される。
  - 受託者又は再受託者の従業員による内部不正や人為的ミスにより、JICAの秘密情報が第三者に流出する。

- サプライチェーン・リスクの脅威を増大させる要因となる脆弱性の例
  - 受託者又は再受託者において、業務に用いる情報システムや機器等のセキュリティ対策が不十分である
  - 受託者又は再受託者の従業員に対する情報セキュリティに係る管理（含む周知・教育）が不十分である
  - 受託者が、再受託者の情報管理に対して責任を負うことを意識していない又はその能力を有していない
  - 受託者若しくは再受託者又はこれらに属する役員若しくは従業員の中に、日本政府との利益相反が生じる可能性がある外国の政府機関に関連する者が存在する

1-3.サプライチェーンの弱点を悪用した攻撃事例

- 事例① 複数の保険会社

  - 2023年1月 業務委託先から顧客の個人情報の流出があったことを公表
  - 原因は、業務委託先の適切なセキュリティ対策がされていないサーバーへの不正アクセス
  - 多いところで約130万人分の情報流出となり、調査や対応に追われた

出典
個人情報流出に関するお詫びとお知らせ(アフラック生命保険株式会社) ：個人情報流出に関するお詫びとお知らせ
個人情報漏えいに関するお詫びとご報告(チューリッヒ保険会社) ：個人情報漏えいに関するお詫びとご報告｜チューリッヒ保険会社

- 事例② LINEヤフー

  - 2023年11月、顧客情報が漏えいしたことを公表（ユーザーに関する情報が約30万件、取引先等に関する情報が約9万件、従業員等に関する情報が約5万件が漏えい）
  - 原因は、第三者による社内システムへの不正アクセス。グループ会社であるNAVER Cloud社のさらに委託先の企業で従業員のPCがウイルス感染したことが発端。

出典
不正アクセスによる、情報漏えいに関するお知らせとお詫び(LINEヤフー株式会社)：不正アクセスによる、情報漏えいに関するお知らせとお詫び｜LINEヤフー株式会社

1-4.個人情報保護について

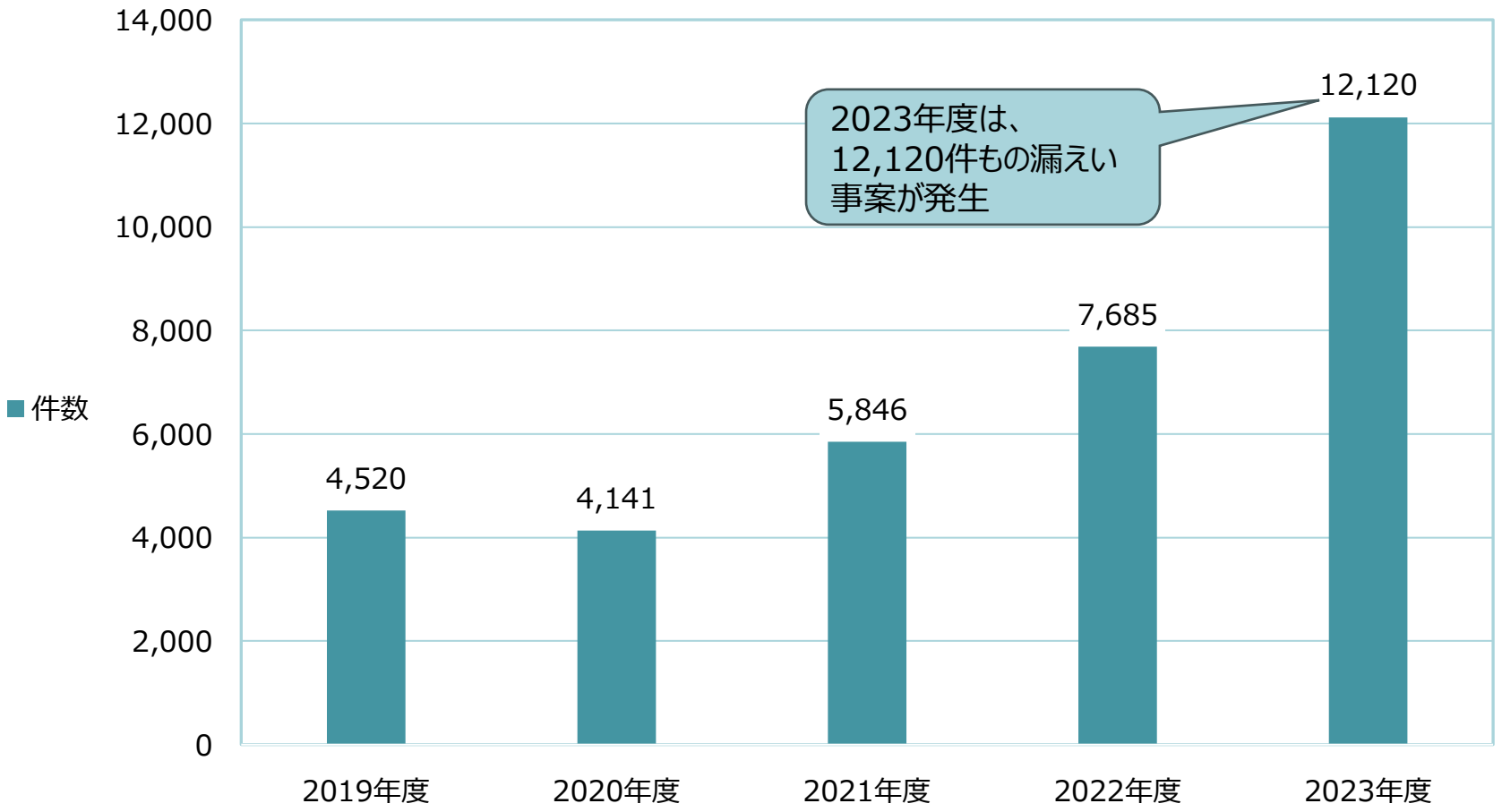
- 個人情報保護法
  正式名称「個人情報の保護に関する法律」は、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とした個人情報の取扱いに関する法律。個人情報の漏洩や不正利用を防ぐため、個人情報を取り扱う場合のルールについて定めている。

- JICA等の行政機関に義務付けられていること
  保有する個人情報の漏えい等の事態が生じた場合には、速やか（発覚日から3～5日以内）に**委員会へ報告**するとともに、本人に対して通知する必要がある。 参照先：個人情報保護委員会 個人情報の保護に関する法律についてのガイドライン（行政機関等編）

- 個人情報保護委員会へ報告が必要な場合
  - **要配慮個人情報**（病歴等）が含まれる保有個人情報の漏えい等（又はそのおそれ）
  - 不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等（又はそのおそれ）
  - 不正の目的をもって行われたおそれがある保有個人情報の漏えい等（又はそのおそれ）
  - 保有個人情報に係る本人の数が**100人を超える**漏えい等（又はそのおそれ）

参照先：個人情報保護委員会 漏えい等の対応とお役立ち資料

1-5.個人情報の漏えい件数の増加



漏えい等事案に関する報告の処理件数
（個人情報保護法に基づく個人情報取扱事業者等からの報告件数）

参照先：個人情報保護委員会　年次報告・上半期報告 ｜個人情報保護委員会

2-1.サプライチェーン・リスクへの対応

※「JICAの情報」＝JICAの要保護情報

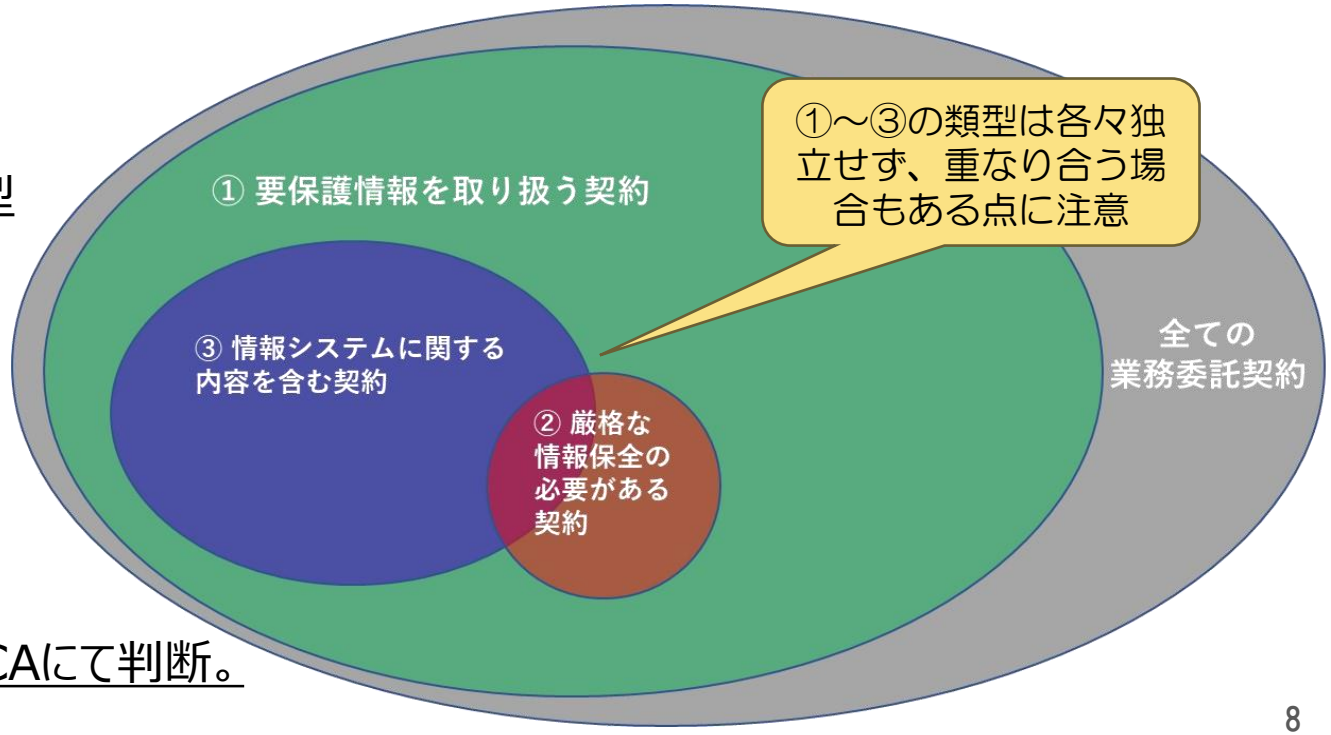
- 「**業務委託**」における**サプライチェーン・リスク**への対応
  - 「**JICAの情報※を取り扱わせる契約**」を対象とし、受託者の皆様に最低限講じていただきたい個人情報取扱い安全管理措置及び情報セキュリティ対策を契約に含め、同対策の遵守を求める。主な変更点は以下の通り
    - 契約書及び約款雛形の改正（情報セキュリティ及び個人情報保護に関連した条項について詳しく規定）p.19～
    - 「個人情報取扱い安全管理措置並びに情報セキュリティ対策」の遵守について表明いただく　p.10～
    - その管理体制及び実施体制等の確認のため、「個人情報保護及び情報セキュリティに関する情報」を提出いただく　p.16～

- ３つの類型
  - 業務内容や取り扱う情報により、大きく以下3つの類型を想定。対策は、この類型に応じて異なる。

①要保護情報を取り扱う契約

②厳格な情報保全の必要がある契約

③情報システムに関する内容を含む契約



  - 契約がどの類型に当てはまるかは、契約内容に応じJICAにて判断。

（参考）要保護情報とは

参照：
情報公開 ｜ JICAについて – JICA
より、「サイバーセキュリティ対策実施細則」第7条情報の格付の区分

	格付の区分	分類の基準
機密性	機密性3情報	機構における業務で取り扱う情報のうち、法人文書管理規程第2条第10号に定める極秘区分に該当する情報かつ他の機関等から提供された「行政文書の管理に関するガイドライン（平成23年4月1日内閣総理大臣決定。以下「文書管理ガイドライン」という。）」に定める秘密文書としての取り扱いを要する情報
	機密性2情報	機構における業務で取り扱う情報のうち、独立行政法人等の保有する情報の公開に関する法律（平成13年法律第140号。以下「情報公開法」という。）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報であって、「機密性3情報」以外の情報
	機密性1情報	機構における業務で取り扱う情報のうち、情報公開法第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報
完全性	完全性2情報	業務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は業務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
	完全性1情報	完全性1情報とは、完全性2情報以外の情報（書面を除く。）
可用性	可用性2情報	業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
	可用性1情報	可用性1情報とは、可用性2情報以外の情報（書面を除く。）

要機密情報
要保全情報
要安定情報

いずれか一つでも該当する場合

要保護情報

物品の購入、定期購読、レンタル契約（PC等）などの契約は、要保護情報を取り扱わないため、対象外としている。

3-1.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

（書面１）「個人情報取扱い安全管理措置並びに情報セキュリティ対策」

- 受託者に、個人情報の取り扱いについて留意いただくべき安全管理措置、並びに、JICA業務において利用する機器、情報システム及びクラウドサービス等に関して講じていただきたい情報セキュリティ対策を示したもの。その遵守について表明いただく想定。
- 契約内容により、以下2種類のどちらかを入札説明書や募集要項等にてJICAが予め提示する。
  - ■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**①要保護情報を取扱う契約用**）」
  - ■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**②厳格な情報保全が必要な契約用**）」
- 書面の内容、及び参照したガイドラインについて（内容の厳しさは①＜②）

項目→	１．個人情報取扱い安全管理措置	２．情報セキュリティ対策
別添１：「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**①要保護情報を取扱う契約用**）」	個人情報保護委員会より公開されている「個人情報の保護に関する法律についてのガイドライン（通則編）」10（別添）講ずべき安全管理措置の内容における「中小規模事業者における手法の例示」を参照の上作成。（https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a10）	独立行政法人情報処理推進機構（IPA）より公開されている「中小企業の情報セキュリティ対策ガイドライン」を参照の上作成。（https://www.ipa.go.jp/security/guide/sme/about.html）
別添２：「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**②厳格な情報保全が必要な契約用**）」	**上記に加え、**内閣官房内閣サイバーセキュリティセンターより公開されている「政府機関等の対策基準策定のためのガイドライン」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf#page=160）p.151-156を参照の上、別添1に追記。	同左

別添１の内容は、一般的にIT機器やインターネットを利用する際に留意すべき、基本的な安全管理措置や情報セキュリティ対策。

別添２では、別添１の内容に新たな対策項目等を追記している。

3-2.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**①要保護情報を取扱う契約用**）」

個人情報取扱い安全管理措置並びに情報セキュリティ対策

1　個人情報及び特定個人情報の取り扱いに際し講ずべき安全管理措置

本業務を実施するにあたって、次に示す安全管理措置を実施する[1]。なお、個人情報及び特定個人情報は以下総称し「個人情報」と記載する。

大項目	No.	小項目
1. 個人情報の取扱いに係る規律の整備	1	個人情報の取得、利用、保存等を行う場合の基本的な取扱方法を整備する。
2. 物理的安全管理措置	2	個人情報を取り扱う区域を管理し、入退室管理を行う。
	3	個人情報を取り扱うサーバー等の機器を管理している場合は、侵入対策、災害等に備えた予備電源の確保・防水対策等を行う。
	4	記録機能を有する機器・媒体の接続制限を行うとともに、端末を限定する。
	5	個人情報を取り扱う機器及び電子媒体等の盗難等を防止するための措置を講じる。また、持ち出しは責任者の許可制とする。
	6	（電子媒体等を持ち運ぶ場合）持ち運ぶ際に個人情報が漏えいしないための措置を講じる。 （例） ・個人データが記録された電子媒体又は個人データが記載された 書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
	7	本業務の完了後、速やかに個人情報の利用を中止し、個人情報を含む媒体等を発注者に返却、又は、個人情報を復元できないよう消去若しくは適切に媒体等を破壊した上で廃棄する。
3.技術的安全管理措置 *情報機器（PCやスマートフォン等）、及び情	8	個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
	9	個人情報を取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別したうえで認証する

[1] 個人情報保護委員会より公開されている「個人情報の保護に関する法律についてのガイドライン（通則編）」10（別添）講ずべき安全管理措置の内容における「中小規模事業者における手法の例示」参照のこと。（https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a10）

報システムを使用して個人情報を取り扱う場合（インターネット等を通じて外部と送受信等をする場合を含む）に講じる措置		（ユーザーID、パスワード、磁気・IC カード等）。また、管理者権限は最小限の人数に絞る。
	10	外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。 （例） ・個人情報を取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人情報を取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。
	11	個人情報を取り扱うサーバー等の機器を管理している場合は、アクセスログ等を定期的に確認、またはアクセス状況を監視し、一定量以上の情報が情報システムからダウンロードされた場合に警告表示されるなどの機能の設定、定期確認などを行う。アクセスログについては、その記録の改ざん・不正な消去の防止等を講じる。
	12	（該当ある場合）業務上、情報システムで個人情報を取り扱う場合は、入力情報の照合（入力原票や既存の情報等との照合）を行う。
	13	（該当ある場合）業務上、個人情報を取り扱う情報システムの設計・開発・運用保守を伴う場合は、当該情報システムの設計書、構成図等の文書が外部に知られないような対策をする。
	14	取り扱う個人情報のバックアップを作成し、外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。
	15	情報システムの使用に伴う漏えい等を防止するための措置を講じる。 （例） ・メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

2

次スライドへつづく

3-3.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**①要保護情報を取扱う契約用**）」

2　情報セキュリティ対策

本業務を実施するにあたって、次に示す情報セキュリティ対策を実施する[2]。

大項目	No.	小項目
Part1.技術的対策	1	業務で使用する機器の OS やソフトウェアは常に最新の状態とする。
	2	業務で使用する機器にはウイルス対策ソフトを導入し、ウイルス定義ファイル（セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル）が自動更新されるよう設定する。
	3	業務で使用する機器、サービス及びシステムにログインする際のパスワードは、強固なパスワードを設定する。 （例） ・10 桁以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」し、複数のサービス間で使いまわさない。 ・可能な場合は多段階認証や多要素認証を利用する。
	4	情報へのアクセス（データ保管などのウェブサービス及びサービス上での共有設定等）を業務上必要な者のみがアクセスできるよう設定する。
	5	脅威や攻撃の手口を知り、対策に活かす。
Part2.業務従事者としての対策	6	不審な電子メールの添付ファイルや URL を安易に開かない。
	7	電子メールの送信先を確認し、送信ミスを防ぐ。
	8	秘密情報[3]を送信する際には、メール本文ではなく添付ファイルに記述しパスワードで保護する。パスワードは予め決めておくか、携帯電話の SMS（ショートメッセージサービス）等の別手段で通知する。

[2] 独立行政法人情報処理推進機構（IPA）より公開されている「中小企業の情報セキュリティ対策ガイドライン」参照のこと。（https://www.ipa.go.jp/security/guide/sme/about.html）

[3] 秘密情報とは、受託者が、本業務を実施する上で、発注者その他本業務の関係者から、文書、口頭、電磁的記録媒体その他開示の方法及び媒体を問わず、また、本契約締結の前後を問わず、開示された一切の情報。ただし、次の各号に定める情報については、この限りでない。
（1）開示を受けた時に既に公知であったもの
（2）開示を受けた時に既に受託者が所有していたもの
（3）開示を受けた後に受託者の責に帰さない事由により公知となったもの
（4）開示を受けた後に第三者から秘密保持義務を負うことなく適法に取得したもの
（5）開示の前後を問わず、受託者が独自に開発したことを証明しうるもの
（6）法令並びに政府機関及び裁判所等の公の機関の命令により開示が義務付けられたもの
（7）第三者への開示につき、発注者又は秘密情報の権限ある保持者から開示について事前の承認があったもの

3

	9	業務で無線 LAN を利用する場合は、安全に利用するために無線 LAN のセキュリティ設定をする。 （例） ・強固な暗号化方式（WPA2、WPA3）を選択する。 ・Wi-Fi ルーター設定のための管理用パスワードを強固で推測されにくいものにする。
	10	業務でのインターネット利用する際の注意、制限をルール化し遵守する。
	11	秘密情報のバックアップを定期的に行う。
	12	秘密情報は机の上等に放置せず、不要時は鍵付き書庫に保管する。
	13	秘密情報の持ち出し時は、PC、スマートフォンなどはパスワードロックをかける等、盗難や紛失の対策を実施する。
	14	離席時・退社時に他人が PC を使えない状態にする（スクリーンロックやシャットダウンをする等）。
	15	執務室への関係者以外の立ち入りを禁止する。
	16	機器・備品の盗難防止対策を行う。
	17	作業場所の施錠忘れ対策を行う（最終退出者は、施錠し退出の記録を残す等）。
	18	秘密情報の記録された媒体を破棄する際には、復元できないように消去し、書面で発注者に報告する。
Part3.組織的対策	19	業務従事者に守秘義務を徹底する。
	20	業務従事者にセキュリティに関する教育や注意喚起を行う。
	21	個人所有の情報機器の業務利用は行わない。やむを得ず利用する場合は、セキュリティ対策を徹底する。
	22	再委託先等との契約において秘密保持や情報セキュリティ対応方針に関する文書を取り交わし、対策状況を確認する。
	23	クラウドサービス等の外部サービスを利用する場合には、安全性・信頼性を把握し選定する。
	24	セキュリティインシデントの発生に備えて緊急時の体制整備や対応手順を作成する。
	25	情報セキュリティ対策に関するルールを明文化し、組織内に周知する。

以上

4

3-4.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**②厳格な情報保全が必要な契約用**）」

個人情報取扱い安全管理措置並びに情報セキュリティ対策

1　個人情報及び特定個人情報の取り扱いに際し講ずべき安全管理措置

本業務を実施するにあたって、次に示す安全管理措置を実施する[1]。なお、個人情報及び特定個人情報は以下総称し「個人情報」と記載する。

大項目	No.	小項目
1. 個人情報の取扱いに係る規律の整備	1	個人情報の取得、利用、保存等を行う場合の基本的な取扱方法を整備する。
2. 物理的安全管理措置	2	個人情報を取り扱う区域を管理し、入退室管理を行う。
	3	個人情報を取り扱うサーバー等の機器を管理している場合は、侵入対策、災害等に備えた予備電源の確保・防水対策等を行う。
	4	記録機能を有する機器・媒体の接続制限を行うとともに、端末を限定する。 （例） ・使用を想定しないUSBポートの無効化、委託事業以外での使用制限等の対策を行う。
	5	個人情報を取り扱う機器及び電子媒体等の盗難等を防止するための措置を講じる。また、持ち出しは責任者の許可制とする。
	6	（電子媒体等を持ち運ぶ場合）持ち運ぶ際に個人情報が漏えいしないための措置を講じる。 （例） ・個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
	7	本業務の完了後、速やかに個人情報の利用を中止し、個人情報を含む媒体等を発注者に返却、又は、個人情報を復元できないよう消去若しくは適切に媒体等を破壊した上で廃棄する。
3.技術的安全管理措置 *情報機器（PC	8	個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
	9	個人情報を取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別したうえで認証する（ユーザーID、パスワード、磁気・ICカード等）。また、管理者権限は最小限の人数に絞る。
やスマートフォン等）、及び情報システムを使用して個人情報を取り扱う場合（インターネット等を通じて外部と送受信等をする場合を含む）に講じる措置	10	外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。 （例） ・個人情報を取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人情報を取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。
	11	個人情報を取り扱うサーバー等の機器を管理している場合は、アクセスログ等を定期的に確認、またはアクセス状況を監視し、一定量以上の情報が情報システムからダウンロードされた場合に警告表示されるなどの機能の設定、定期確認などを行う。アクセスログについては、その記録の改ざん・不正な消去の防止等を講じる。 （例） ・ログの取得対象は継続的に見直しを実施する。 ・ログの取得プロセスの障害監視を行う。
	12	（該当ある場合）業務上、情報システムで個人情報を取り扱う場合は、入力情報の照合（入力原票や既存の情報等との照合）を行う。
	13	（該当ある場合）業務上、個人情報を取り扱う情報システムの設計・開発・運用保守を伴う場合は、当該情報システムの設計書、構成図等の文書が外部に知られないような対策をする。
	14	取り扱う個人情報のバックアップを作成し、外部からの不正アクセス等を防止するための措置（セキュリティ対策）を講じる。
	15	情報システムの使用に伴う漏えい等を防止するための措置を講じる。 （例） ・メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

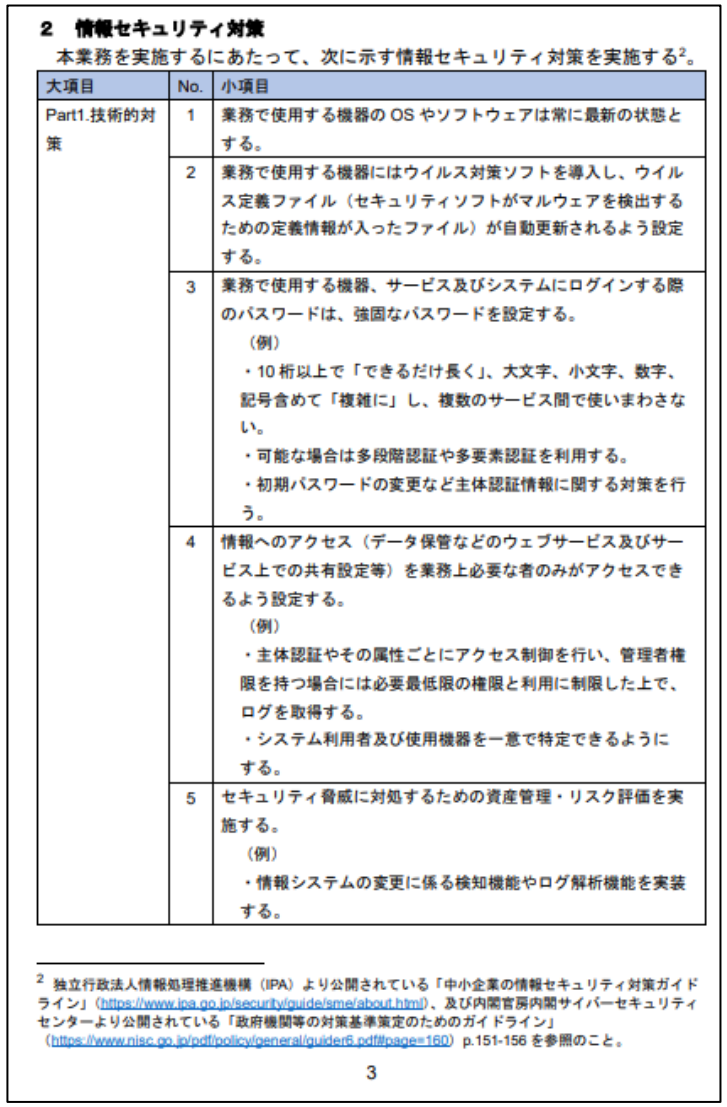
[1] 個人情報保護委員会より公開されている「個人情報の保護に関する法律についてのガイドライン（通則編）」10（別添）講ずべき安全管理措置の内容における「中小規模事業者における手法の例示」（https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a10）、及び内閣官房内閣サイバーセキュリティセンターより公開されている「政府機関等の対策基準策定のためのガイドライン」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf#page=160）p.151-156を参照のこと。

2

次スライドへつづく

3-5.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**②厳格な情報保全が必要な契約用**）」



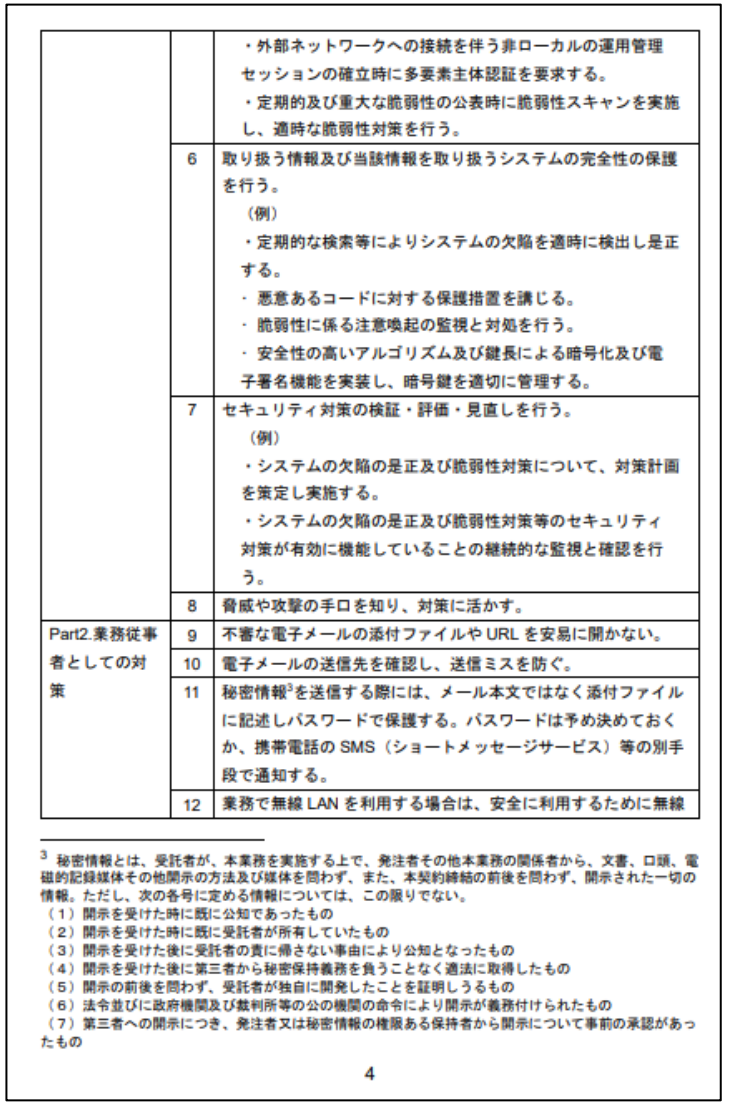
２　情報セキュリティ対策

本業務を実施するにあたって、次に示す情報セキュリティ対策を実施する[2]。

大項目	No.	小項目
Part1.技術的対策	1	業務で使用する機器の OS やソフトウェアは常に最新の状態とする。
	2	業務で使用する機器にはウイルス対策ソフトを導入し、ウイルス定義ファイル（セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル）が自動更新されるよう設定する。
	3	業務で使用する機器、サービス及びシステムにログインする際のパスワードは、強固なパスワードを設定する。 （例） ・10 桁以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」し、複数のサービス間で使いまわさない。 ・可能な場合は多段階認証や多要素認証を利用する。 ・初期パスワードの変更など主体認証情報に関する対策を行う。
	4	情報へのアクセス（データ保管などのウェブサービス及びサービス上での共有設定等）を業務上必要な者のみがアクセスできるよう設定する。 （例） ・主体認証やその属性ごとにアクセス制御を行い、管理者権限を持つ場合には必要最低限の権限と利用に制限した上で、ログを取得する。 ・システム利用者及び使用機器を一意で特定できるようにする。
	5	セキュリティ脅威に対処するための資産管理・リスク評価を実施する。 （例） ・情報システムの変更に係る検知機能やログ解析機能を実装する。

[2] 独立行政法人情報処理推進機構（IPA）より公開されている「中小企業の情報セキュリティ対策ガイドライン」（https://www.ipa.go.jp/security/guide/sme/about.html）、及び内閣官房内閣サイバーセキュリティセンターより公開されている「政府機関等の対策基準策定のためのガイドライン」（https://www.nisc.go.jp/pdf/policy/general/guider6.pdf#page=160）p.151-156 を参照のこと。

3



		・外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時に多要素主体認証を要求する。 ・定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時な脆弱性対策を行う。
	6	取り扱う情報及び当該情報を取り扱うシステムの完全性の保護を行う。 （例） ・定期的な検索等によりシステムの欠陥を適時に検出し是正する。 ・悪意あるコードに対する保護措置を講じる。 ・脆弱性に係る注意喚起の監視と対処を行う。 ・安全性の高いアルゴリズム及び鍵長による暗号化及び電子署名機能を実装し、暗号鍵を適切に管理する。
	7	セキュリティ対策の検証・評価・見直しを行う。 （例） ・システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施する。 ・システムの欠陥の是正及び脆弱性対策等のセキュリティ対策が有効に機能していることの継続的な監視と確認を行う。
	8	脅威や攻撃の手口を知り、対策に活かす。
Part2.業務従事者としての対策	9	不審な電子メールの添付ファイルや URL を安易に開かない。
	10	電子メールの送信先を確認し、送信ミスを防ぐ。
	11	秘密情報[3]を送信する際には、メール本文ではなく添付ファイルに記述しパスワードで保護する。パスワードは予め決めておくか、携帯電話の SMS（ショートメッセージサービス）等の別手段で通知する。
	12	業務で無線 LAN を利用する場合は、安全に利用するために無線

[3] 秘密情報とは、受託者が、本業務を実施する上で、発注者その他本業務の関係者から、文書、口頭、電磁的記録媒体その他開示の方法及び媒体を問わず、また、本契約締結の前後を問わず、開示された一切の情報。ただし、次の各号に定める情報については、この限りでない。
（１）開示を受けた時に既に公知であったもの
（２）開示を受けた時に既に受託者が所有していたもの
（３）開示を受けた後に受託者の責に帰さない事由により公知となったもの
（４）開示を受けた後に第三者から秘密保持義務を負うことなく適法に取得したもの
（５）開示の前後を問わず、受託者が独自に開発したことを証明しうるもの
（６）法令並びに政府機関及び裁判所等の公の機関の命令により開示が義務付けられたもの
（７）第三者への開示につき、発注者又は秘密情報の権限ある保持者から開示について事前の承認があったもの

4

次スライドへつづく

3-6.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（１）～

■「個人情報取扱い安全管理措置並びに情報セキュリティ対策（**②厳格な情報保全が必要な契約用**）」

		LAN のセキュリティ設定をする。 （例） ・強固な暗号化方式（WPA2、WPA3）を選択する。 ・Wi-Fi ルーター設定のための管理用パスワードを強固で推測されにくいものにする。 ・無線 LAN へのアクセス主体の認証等の対策を行う。
	13	業務でのインターネット利用する際の注意、制限をルール化し遵守する。
	14	秘密情報のバックアップを定期的に行う。
	15	秘密情報は机の上等に放置せず、不要時は鍵付き書庫に保管する。
	16	秘密情報の持ち出し時は、PC、スマートフォンなどはパスワードロックをかける等、盗難や紛失の対策を実施する。 （例） ・テレワークを実施する場合、情報セキュリティ対策[4]を行う。
	17	離席時・退社時に他人が PC を使えない状態にする（スクリーンロックやシャットダウンをする等）。
	18	執務室への関係者以外の立ち入りを禁止する。
	19	機器・備品の盗難防止対策を行う。
	20	作業場所の施錠忘れ対策を行う（最終退出者は、施錠し退出の記録を残す等）。
	21	秘密情報の記録された媒体を破棄する際には、復元できないように消去し、書面で発注者に報告する。
Part3.組織的対策	22	業務従事者に守秘義務を徹底する。 （例） ・委託業務に伴う情報を取り扱う従業員等の資格条件を明確化する。 ・従業員等の異動・退職等の際に情報を保護すること等を求める。
	23	業務従事者にセキュリティに関する教育や注意喚起を行う。
	24	個人所有の情報機器の業務利用は行わない。やむを得ず利用する場合は、セキュリティ対策を徹底する。

[4] 独立行政法人情報処理推進機構（IPA）より公開されている「テレワークを行う際のセキュリティ上の注意事項」参照のこと。（https://www.ipa.go.jp/security/anshin/measures/telework.html）

5

	25	再委託先等との契約において秘密保持や情報セキュリティ対応方針に関する文書を取り交わし、対策状況を確認する。
	26	クラウドサービス等の外部サービスを利用する場合には、安全性・信頼性を把握し選定する。
	27	セキュリティインシデントの発生に備えて緊急時の体制整備や対応手順を作成する。 （例） ・識別・防御・検知・対応・復旧を例とした、準備から事後処理に至る全般的なインシデント対処プロセスを確立する。 ・報告フロー等の概要について、説明ができるようにする。
	28	情報セキュリティ対策に関するルールを明文化し、組織内に周知する。

以上

6

3-7.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（２）～

（書面２）「個人情報保護及び情報セキュリティに関する情報」

- （書面１）「個人情報取扱い安全管理措置並びに情報セキュリティ対策」の管理体制及び実施体制等に関する情報を以下のシートに沿って記入し、JICAに提出いただくもの。
  - ■ 「個人情報保護及び情報セキュリティに関する情報」

- 主な内容

１　個人情報取扱い安全管理措置並びに情報セキュリティ対策に関する管理体制・作業場所

（１）管理体制：「情報セキュリティ責任者」、「個人情報保護管理者」、「品質保証管理者（※「③情報システムに関する内容を含む契約」のみ記入。）」、及び、個人情報の漏えいを含む情報セキュリティインシデントが発生した場合に窓口となって対応いただく方を記入いただく。

（２）業務作業場所：例として、「国際協力機構の麹町本部」、「受注者の執務室」等、可能な限り具体的に記載いただく。

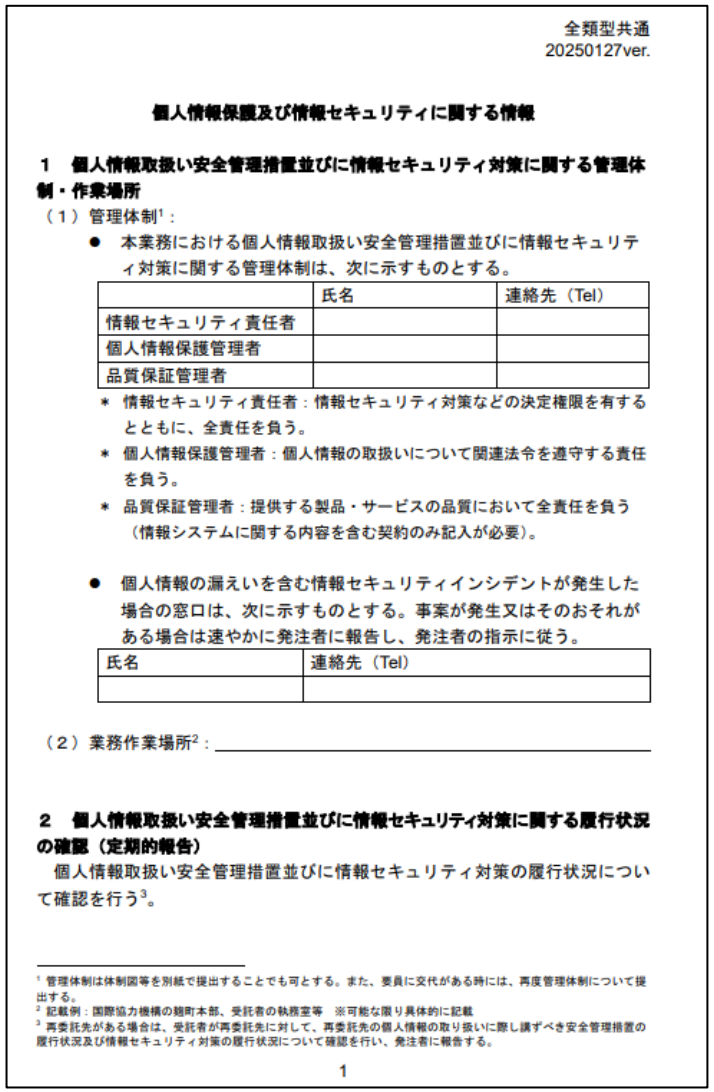
２　個人情報取扱い安全管理措置並びに情報セキュリティ対策に関する履行状況の確認（定期的報告）

（１）履行状況の確認方法：JICAと受託者で相談の上、「会議体による報告」、「書面による報告」等を記載いただく。

（２）履行状況の確認頻度：JICAと受託者で相談の上、「～ヶ月に1回」、「1年に1回」等を記載いただく。望ましい確認頻度は、契約期間・規模及び取り扱う個人情報の規模や秘匿性によるため、特に決まったものはない。例えば、業務実施状況を報告する会議体があれば、当該報告時に対策履行状況報告を含めていただくことが想定される。あるいは、契約期間が1年未満の場合は3か月に1回程度、1年以上の場合は1年に1回程度が適切な確認頻度と考えられる。（3か月未満の契約であれば、業務完了報告時に履行状況の報告も含めていただくことが想定される。）

3-8.受託者の皆様に求める情報セキュリティ対策等
～関連する書面（２）～

■「個人情報保護及び情報セキュリティに関する情報」



全類型共通
20250127ver.

個人情報保護及び情報セキュリティに関する情報

１　個人情報取扱い安全管理措置並びに情報セキュリティ対策に関する管理体制・作業場所

（１）管理体制[1]：

- 本業務における個人情報取扱い安全管理措置並びに情報セキュリティ対策に関する管理体制は、次に示すものとする。

	氏名	連絡先（Tel）
情報セキュリティ責任者		
個人情報保護管理者		
品質保証管理者		

＊ 情報セキュリティ責任者：情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
＊ 個人情報保護管理者：個人情報の取扱いについて関連法令を遵守する責任を負う。
＊ 品質保証管理者：提供する製品・サービスの品質において全責任を負う（情報システムに関する内容を含む契約のみ記入が必要）。

- 個人情報の漏えいを含む情報セキュリティインシデントが発生した場合の窓口は、次に示すものとする。事案が発生又はそのおそれがある場合は速やかに発注者に報告し、発注者の指示に従う。

氏名	連絡先（Tel）

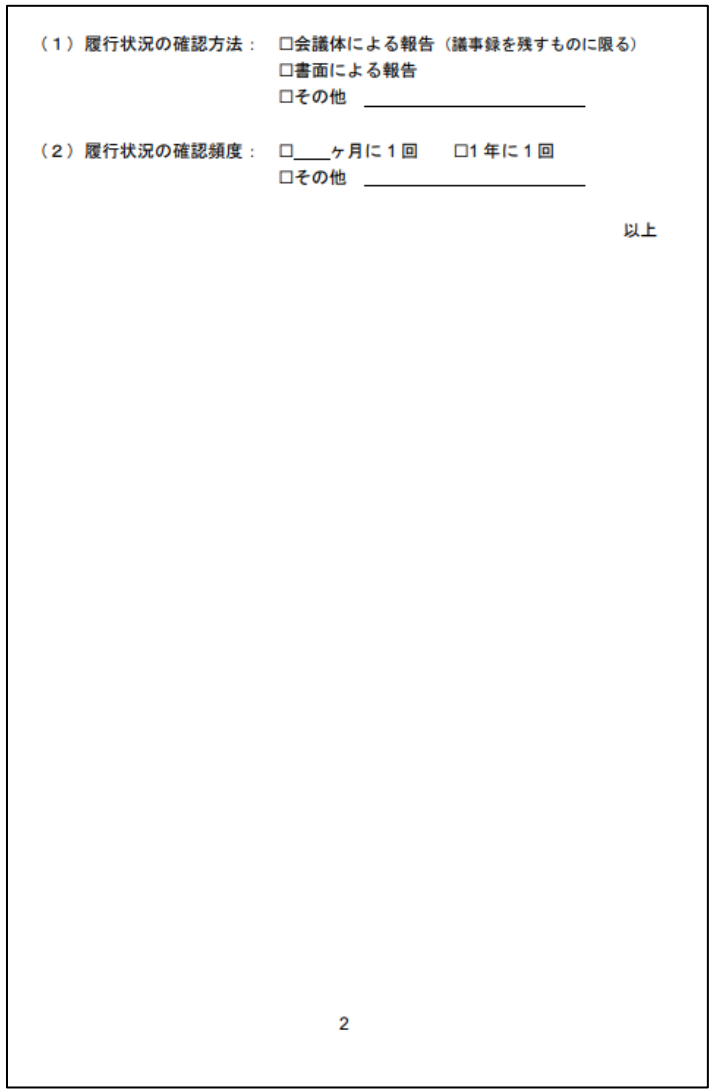
（２）業務作業場所[2]：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

２　個人情報取扱い安全管理措置並びに情報セキュリティ対策に関する履行状況の確認（定期的報告）

個人情報取扱い安全管理措置並びに情報セキュリティ対策の履行状況について確認を行う[3]。

[1] 管理体制は体制図等を別紙で提出することでも可とする。また、委員に交代がある時には、再度管理体制について提出する。
[2] 記載例：国際協力機構の麹町本部、受託者の執務室等　※可能な限り具体的に記載
[3] 再委託先がある場合は、受託者が再委託先に対して、再委託先の個人情報の取り扱いに際し講ずべき安全管理措置の履行状況及び情報セキュリティ対策の履行状況について確認を行い、発注者に報告する。

1



（１）履行状況の確認方法：　□会議体による報告（議事録を残すものに限る）
□書面による報告
□その他 ＿＿＿＿＿＿＿＿＿＿

（２）履行状況の確認頻度：　□＿＿ヶ月に１回　□1 年に１回
□その他 ＿＿＿＿＿＿＿＿＿＿

以上

2

４．適用対象案件

◆JICA本部における公告・公示情報のうち、コンサルタント等契約及びその他役務の提供等にかかる契約。

「その他調達情報（調達部以外）案件公示」及び「各国内拠点（JICA緒方研究所を含む）における公告・公示情報」は現時点では適用対象外。

◆2025年3月1日以降に公告・公示を行う契約より適用

◆公告・公示を行わない契約（特命随意契約や期分けの継続契約等）については2025年3月1日以降に契約交渉を行う契約を対象

2025年2月28日以前に公告・公示を行った案件、2025年3月1日以降に契約変更を行う案件は本件適用対象外。

５．契約書雛形改正の主なポイント

◆改正対象条項は、**①個人情報保護**、**②特定個人情報保護**、**③情報セキュリティ**、**④情報システムに関する業務における情報セキュリテイ**、の4つ。このうち②及び④は、該当する案件にのみ適用されるオプション条項。

- ✓ コンサルタント等契約においては、①及び③については従来の約款上の文言を変更、②及び④については契約書本体の第3条（約款の一部変更適用）にオプション条項として新たに追加。
- ✓ その他役務の提供等にかかる契約においては、①～③については従来の契約書参考雛形上の文言を変更、④についてはオプション条項として新たに追加。

◆個人情報保護及び情報セキュリティのいずれについても、受注者側の具体的な対策に関し、契約締結後速やかに**書面にて発注者に提出**し、発注者の確認を得る旨を追記。

◆発注者が提供する情報（個人情報を含む）を取り扱う再委託業務がある場合について、**再委託先も受注者と同様の義務を履行する必要**があることを追記。

（①-1　個人情報保護）

以下、今次改正に伴う変更内容を赤字で記載

第●条　受注者は、本契約において、発注者の保有個人情報（「個人情報の保護に関する法律」（平成15年法律第57号。以下「個人情報保護法」という。）第60条第1項で定義される保有個人情報を指し、以下「保有個人情報」という。）を取り扱う場合は、次の各号に定める義務を負うものとする。

（１）当該取扱いに係る個人情報に関する秘密を保持し、利用目的以外に利用しないこと。

（２）本契約締結後速やかに、次の各号に掲げる事項を記載した書面を発注者に提出し、本業務の開始に先立って発注者の確認を得ること。＊提出→確認というプロセスを規定

書面1及び書面2

イ　当該取扱いに係る個人情報の複製等の制限に関する事項

ロ　当該取扱いに係る個人情報の漏えい等の事案の発生時における対応に関する事項

ハ　契約終了時における当該取扱いに係る個人情報の消去及び媒体の返却に関する事項　＊現行では「又は」

ニ　本業務における責任者及び業務従事者等の管理体制及び実施体制に関する事項

ホ　前号及び次号の遵守状況についての定期的報告に関する事項　＊現行では「発注者の求めがあった場合」

ヘ　イからホまでに定めるもののほか、当該取扱いに係る個人情報の漏えい、滅失又は毀損の防止その他個人情報の適正な管理のために発注者が必要と判断した措置に関する事項

（３）前号の書面に記載された事項を遵守すること。　・・・・・・

次スライドへつづく

（①-2　個人情報保護）

・・・・・・・・・

２　発注者は、必要があると認めるときは、受注者における個人情報の管理体制、実施体制及び個人情報の管理の状況について、検査により確認する。この検査は、原則として、実地検査の方法で行う。

３　業務内容の一部を再委託する場合においては、受注者は、再委託先に対し、第1項各号の義務を履行させる。この場合において、発注者は、再委託する業務に係る保有個人情報の秘匿性等に応じて、受注者を通じて、又は発注者自らが前項の検査を実施する。 **＊再委託先に同様の義務の履行を求める規定を追加**

４　前項の規定は、再委託先が委託先の子会社である場合又は再委託先が再々委託を行う場合も同様とする。

＊再々委託先に同様の義務の履行を求める規定を追加

５　受注者は、保有個人情報の漏えい等による被害発生のリスクを低減する観点から、利用目的、業務の内容、保有個人情報の秘匿性等を考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。 **＊必要に応じて削除・置き換えを行う規定を追加**

６　第1項第1号及び第2項ないし第4項の規定は、本業務が完了した後も引き続き効力を有する。 **＊存続条項を追加**

（② 特定個人情報保護）

第●条の２　前条第1項ないし第4項の規定は、受注者が本契約において特定個人情報等（「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」（平成25年法律第27号。以下「番号法」という。）第2条第5項で定める個人番号及び同条第8項で定める特定個人情報を指す。以下同じ。）に係る関係事務を実施する場合について準用する。この場合において、同項中「個人情報」とあるのは「特定個人情報」と読み替えるものとする。

２　前項の場合において、受注者は、前項に定めるもののほか、業務従事者等が前項に違反したときは、業務従事者等及び受注者に適用のある番号法が定める罰則が適用され得ることを、業務従事者等に周知するものとする。

３　第1項が準用する第●条第1項第1号及び第2項ないし第4項の規定は、本業務が完了した後も引き続き効力を有する。　＊存続条項を追加

（③-1　情報セキュリティ）＊現行では機構の規程を準用のうえ対策を講じることを規定

第■条　受注者は、本契約において発注者が提供する情報（以下「情報」という。）を取り扱う場合は、次の各号に定める義務を負うものとする。

（１）当該情報提供の目的以外に情報を利用しない等、提供された情報を適正に取り扱うこと。

（２）本契約締結後速やかに、次に掲げる事項を記載した書面を発注者に提出し、本件業務の開始に先立って発注者の確認を得ること。当該書面に記載した事項に変更があった場合には、速やかに発注者に書面で報告し、発注者の確認を得ること。

書面1及び書面2

イ　情報の適正な取扱いを目的とした情報セキュリティ対策の実施内容
ロ　情報セキュリティ対策を実施・管理するための管理体制
ハ　本業務に係る業務従事者及び作業場所
ニ　情報セキュリティインシデントが発生した場合の具体的な対処方法
ホ　情報セキュリティ対策に係る履行状況の発注者への報告方法及び頻度
ヘ　情報セキュリティ対策の履行が不十分である場合の対処方法
ト　イからヘまでに定めるもののほか、情報の適切な取扱いのために必要と発注者が判断した事項

・・・・・・

次スライドへつづく

（③-2　情報セキュリティ）

・・・・・・・・・・

（３）情報の受領方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について発注者と合意すること。

（４）第2号の書面及び前号の取扱手順に基づき情報を取り扱うこと。

２　発注者は、受注者が取り扱う情報の格付等を勘案のうえ、必要があると認めるときは、受注者の事務所等における情報セキュリティ監査を実施する。この場合において、受注者による情報の取扱いが前項第4号に違反する場合には、発注者は、受注者に対し、改善を指示することができる。

３　業務内容の一部を再委託する場合は、受注者は、再委託先に対し、第1項各号に定める義務を履行させ、かつ第2項に定める情報セキュリティ監査の措置を実施する。この場合において、受注者は、発注者に対し、第4条に定められている事項に加え、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情報を提供し、発注者の確認を得る。

（④　情報システムに関する業務における情報セキュリティ）

書面2

第■条の2　受注者は、契約締結後速やかに、発注者に対し、次の各号に定める事項を記載した書面を提出し、本業務の開始に先立って発注者の確認を得なければならない。

（１）　受注者企業若しくはその従業員、再委託先企業若しくはその従業員又はその他の者によって、情報システムに機構の意図せざる変更が加えられないための管理体制

（２）　受注者の資本関係、役員等の情報、本契約業務の実施場所並びに業務責任者の所属、専門性(情報セキュリティに係る資格（情報処理安全確保支援士等）及び研修実績等)、実績及び国籍

２　受注者は、前項第1号の管理体制を遵守しなければならない。

６-１．コンサルタント等契約 関連ガイドライン/様式の変更点（その１）

１．主な修正箇所

（1）誓約事項の変更
（2）様式１－１及び１－２の修正
（3）ゼロ号打合簿の添付書類の追加
（4）コンサルタント等契約における現地再委託ガイドラインの修正
（5）コンサルタント業務従事月報への追加

6-2. コンサルタント等契約 関連ガイドライン/様式の変更点（その２）

２．変更箇所詳細

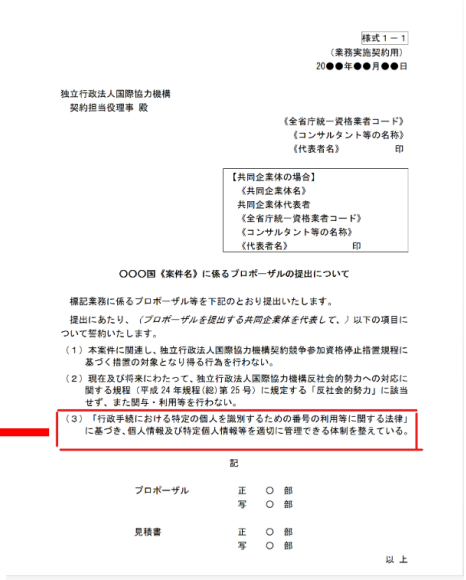
（１）誓約事項の変更：「コンサルタント等契約におけるプロポーザル作成ガイドライン（以下「プロポーザル作成GL」）の別添11、及び別添12の該当箇所を以下の通り変更

修正箇所	修正前	修正後
別添資料11 「６．誓約事項」（2）	（2）個人情報及び特定個人情報等の保護 法人として「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「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（平成26年12月11日特定個人情報保護委員会）」に基づき、個人情報及び特定個人情報等を適切に管理できる体制を整えていること。	(2)個人情報等の保護及び情報セキュリティ対策の遵守 契約締結後には、令和5年度版「政府機関の情報セキュリティ対策のための統一基準群」及びこれに準拠する機構内関連規程に基づき機構が定める「個人情報取扱い安全管理措置並びに情報セキュリティ対策」（別添●、別添●）を遵守するとともに、「個人情報保護及び情報セキュリティに関する情報」（別添●）にて、個人情報保護及び情報セキュリティにかかる管理体制等の報告を行うこと。
別添資料12 「４．誓約事項」（2）	（2）個人情報及び特定個人情報等の保護 法人として「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「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（平成26年12月11日特定個人情報保護委員会）」に基づき、個人情報及び特定個人情報等を適切に管理できる体制を整えていること。 本契約において、「個人番号関係事務」を委託することは想定していませんが、業務に関連して競争参加者が謝金等を支払う可能性も想定されるため、そのような場合において、法令に基づく適切な管理ができる体制にあるのかを確認させていただくことが趣旨です。	(2)個人情報等の保護及び情報セキュリティ対策の遵守 契約締結後には、令和5年度版「政府機関の情報セキュリティ対策のための統一基準群」及びこれに準拠する機構内関連規程に基づき機構が定める「個人情報取扱い安全管理措置並びに情報セキュリティ対策並びに情報セキュリティ対策方針」（別添●、別添●）を遵守するとともに、「個人情報保護及び情報セキュリティに関する情報」（別添●）にて、個人情報保護及び情報セキュリティにかかる管理体制等の報告を行うこと。 本契約において、「個人番号関係事務」を委託することは想定していませんが、業務に関連して競争参加者が謝金等を支払う可能性も想定されるため、そのような場合において、法令に基づく適切な管理ができる体制にあるのかを確認させていただくことが趣旨です。

6-3. コンサルタント等契約 関連ガイドライン/様式の変更点（その３）

（２）プロポーザル作成GL　様式１－１、１－２の修正

修正箇所	修正前	修正後
誓約事項（3）	（3）「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」に基づき、個人情報及び特定個人情報等を適切に管理できる体制を整えている。	（3）令和5年度版「政府機関の情報セキュリティ対策のための統一基準群」に基づき機構が定める「個人情報取扱い安全管理措置並びに情報セキュリティ対策」を遵守するとともに、「個人情報保護及び情報セキュリティに関する情報」にて、個人情報保護及び情報セキュリティにかかる管理体制等の報告を行う



様式１－１
（業務実施契約用）
20●●年●●月●●日

独立行政法人国際協力機構
契約担当役理事　殿

《全省庁統一資格業者コード》
《コンサルタント等の名称》
《代表者名》　印

【共同企業体の場合】
《共同企業体名》
共同企業体代表者
《全省庁統一資格業者コード》
《コンサルタント等の名称》
《代表者名》　印

○○○国《案件名》に係るプロポーザルの提出について

標記業務に係るプロポーザル等を下記のとおり提出いたします。

提出にあたり、（プロポーザルを提出する共同企業体を代表して、）以下の項目について誓約いたします。

（１）本案件に関連し、独立行政法人国際協力機構契約競争参加資格停止措置規程に基づく措置の対象となり得る行為を行わない。

（２）現在及び将来にわたって、独立行政法人国際協力機構反社会的勢力への対応に関する規程（平成 24 年規程(総)第 25 号）に規定する「反社会的勢力」に該当せず、また関与・利用等を行わない。

（３）「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」に基づき、個人情報及び特定個人情報等を適切に管理できる体制を整えている。

記

プロポーザル　正　○　部
　　写　○　部

見積書　正　○　部
　　写　○　部

以　上

（３）ゼロ号打合簿の添付書類に「個人情報保護及び情報セキュリティに関する情報」を追加。

※　業務実施契約（単独型）については、ゼロ号打合簿を締結しませんので、契約締結後速やかに監督職員に「個人情報保護及び情報セキュリティに関する情報」を記入の上、提出ください。

６-４．コンサルタント等契約 関連ガイドライン/様式の変更点（その４）

（４）コンサルタント等契約における現地再委託

ガイドラインへの追記

①「第2-3．現地再委託先の選定」に右の通り追記

この契約交渉にて、現地再委託先の選定方法についても JICA、受注者双方にて確認を行います。

▪ ３．現地再委託先の選定

業務実施契約書を締結した後、同契約書で定めた現地再委託業務の範囲の中で、受注者は、現地再委託契約のための仕様書の作成、現地再委託先の選定及び契約の締結等の手続きを、自らの責任の下に行うこととなります。

再委託先が、発注者が提供する情報（個人情報を含む）を取り扱う場合、現地再委託先の選定においては、再委託先が業務実施契約約款に定める「個人情報保護及び情報セキュリティにかかる対策」を遵守できる体制にあることを確認し、下述４の「現地再委託契約の締結と JICA への報告」においても報告をお願いします。また、現地再委託契約履行中に、再委託先において当該体制を確保することができなくなった場合は、監督職員に速やかに申し出てください。

再委託契約の業務仕様書の詳細の確定は、原則として受注者の裁量となりますが、業務仕様書の詳細が、本体業務の質に大きく影響する場合（大規模な交通量調査等や課題分析の中核となるアンケート調査等）は、その内容について、監督職員と十分に打合せてください。

なお、一つの業務実施契約内で複数の現地再委託契約を行う場合、受注者の裁量で、費目（中項目）「再委託費」の総額内において、各々の現地再委託契約経費の調整が可能です。また、現地再委託契約履行中に、自然災害など予測困難な事態が発生し、当初の現地再委託業務を大きく変更せざるを得ない場合は、業務主任者は、速やかに監督職員に報告・相談願います。双方にて協議を行い契約変更等の対応を行うこととします。

【現地再委託先の選定のための評価基準】

現地再委託先を選定する評価基準は、大きく分けて以下の３つが考えられます。

①最低コストに基づく選定（Least Cost Selection）
②質及びコストに基づく選定（Quality and Cost Based Selection）
③質に基づく選定（Quality Based Selection）

上記①～③は、ウェブ、掲示等の方法により公告し、広く一般から募る方法、または事前の調査、カウンターパート機関等から入手した現地業者の情報等から、技術し

6-5. コンサルタント等契約 関連ガイドライン/様式の変更点（その５）

（４）コンサルタント等契約における現地再委託
ガイドラインへの追記

②「第2-４．現地再委託契約の締結とJICAへの報告」に右の通り追記

２）再委託業者名・連絡先（担当者名、住所、電話番号、Fax 番号、E-mail 等）
３）再委託契約履行期間
４）再委託契約金額（支払条件を含む）
５）再委託業務の概要
６）選定方法
７）特定業者との随意契約を行った場合、その理由
８）JICA 在外事務所担当者名及び事実確認日（下記５．のとおり）
９）（再委託先が、発注者が提供する情報（個人情報を含む）を取り扱う場合のみ）
再委託先における個人情報保護及び情報セキュリティにかかる対策の実施状況

この際、見積書の写し等を提出する必要はありませんが、JICA で選定手続きにおける関連書類を確認させていただく場合がありますので、書類は適切に保管願います。
現地再委託業務の内容に変更が生じた場合は、再委託契約の変更契約書を締結してください。個々の現地再委託契約の金額変更を伴う場合は、監督職員に打合簿をもって現地再委託の変更契約締結後に結果を報告ください（履行期間の延長等軽微な変更については打合簿不要です）。その際、上記各項目を”変更後金額”や”変更した業務の概要”、選定方法は“変更理由“と書き換えて報告ください。
なお、再委託先との契約変更に伴い JICA との契約内容や金額の変更（大・中項目の流用、特記仕様書の変更等）が必要な場合は、事前にそれらの打合簿締結や契約変更を行うことになります。

※□９）については、上述のとおり再委託先での確認結果を踏まえ、「個人情報保護及び情報セキュリティにかかる対策の実施状況」について以下の通り記載ください。
「再委託先における個人情報保護及び情報セキュリティにかかる対策の実施状況を確認し、再委託先が業務実施契約約款の個人情報保護条項及び情報セキュリティ条項に定める義務を履行可能であることを確認済）。」

▪ ５．JICA 在外事務所による現地再委託契約の事実確認
受注者から上記４.の打合簿にて選定経緯及び契約書写しの提出を受けて、JICA 在外事務所は現地再委託先に対して、面談や電話等を用い、再委託契約内容に関する事実（再委託契約の有無、契約金額、契約業務内容）の確認を行い、受注者からの報告内容と相違がないことを確認します。契約終了時は確認を省略します。

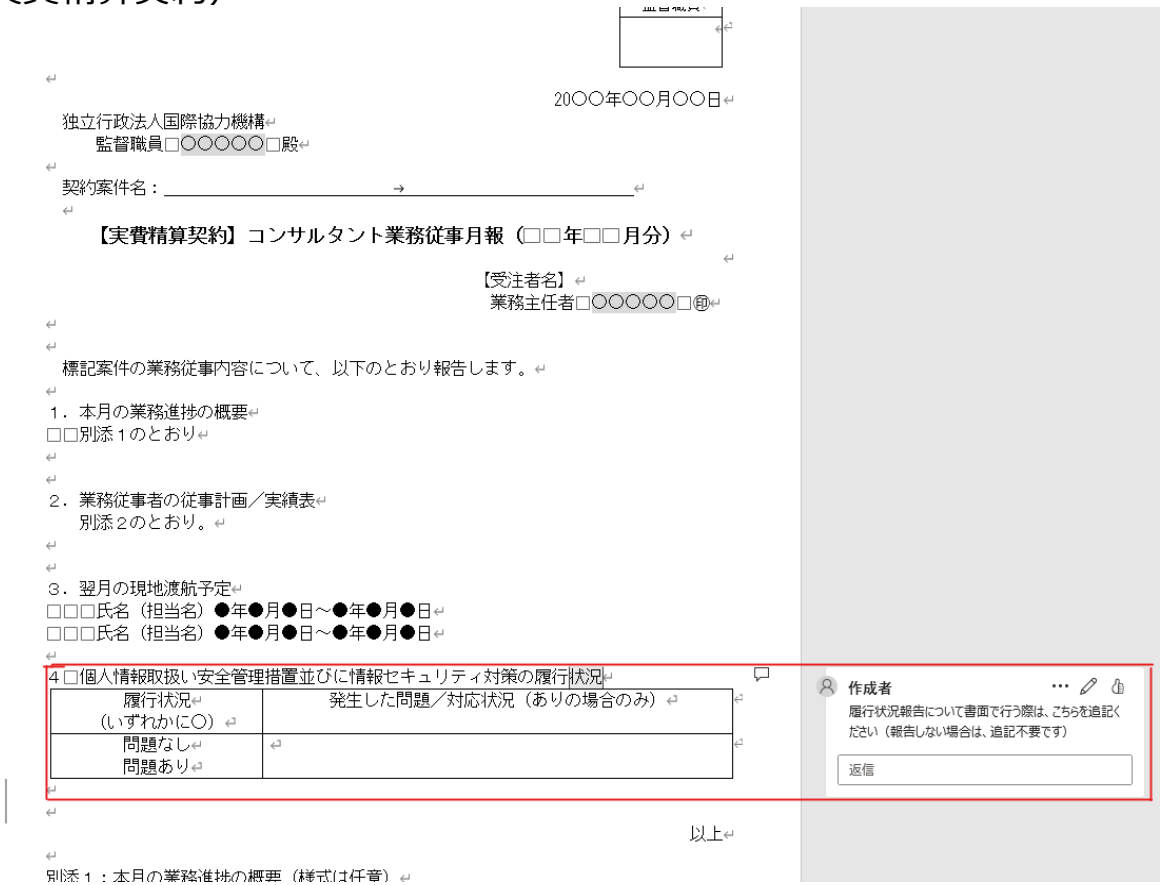
6-6. コンサルタント等契約 関連ガイドライン/様式の変更点（その６）

（５）コンサルタント契約業務従事月報への追記

①「個人情報保護及び情報セキュリティに関する情報」にて、書面にて履行状況の報告を選択した場合に当該内容が記載できるように文言を追記。

②発注者が提供する情報（個人情報を含む）を取り扱う再委託業務がある場合、再委託先が個人情報保護及び情報セキュリティ対策が履行できる旨を確認済であることを報告できるように文言を追記（再委託業務がランプサム方式となっている場合のみ）

（実費精算契約）



20〇〇年〇〇月〇〇日

独立行政法人国際協力機構
監督職員□〇〇〇〇〇□殿

契約案件名：

【実費精算契約】コンサルタント業務従事月報（□□年□□月分）

【受注者名】
業務主任者□〇〇〇〇〇□㊞

標記案件の業務従事内容について、以下のとおり報告します。

１．本月の業務進捗の概要
□□別添１のとおり

２．業務従事者の従事計画／実績表
別添２のとおり。

３．翌月の現地渡航予定
□□□氏名（担当名）●年●月●日～●年●月●日
□□□氏名（担当名）●年●月●日～●年●月●日

４□個人情報取扱い安全管理措置並びに情報セキュリティ対策の履行状況

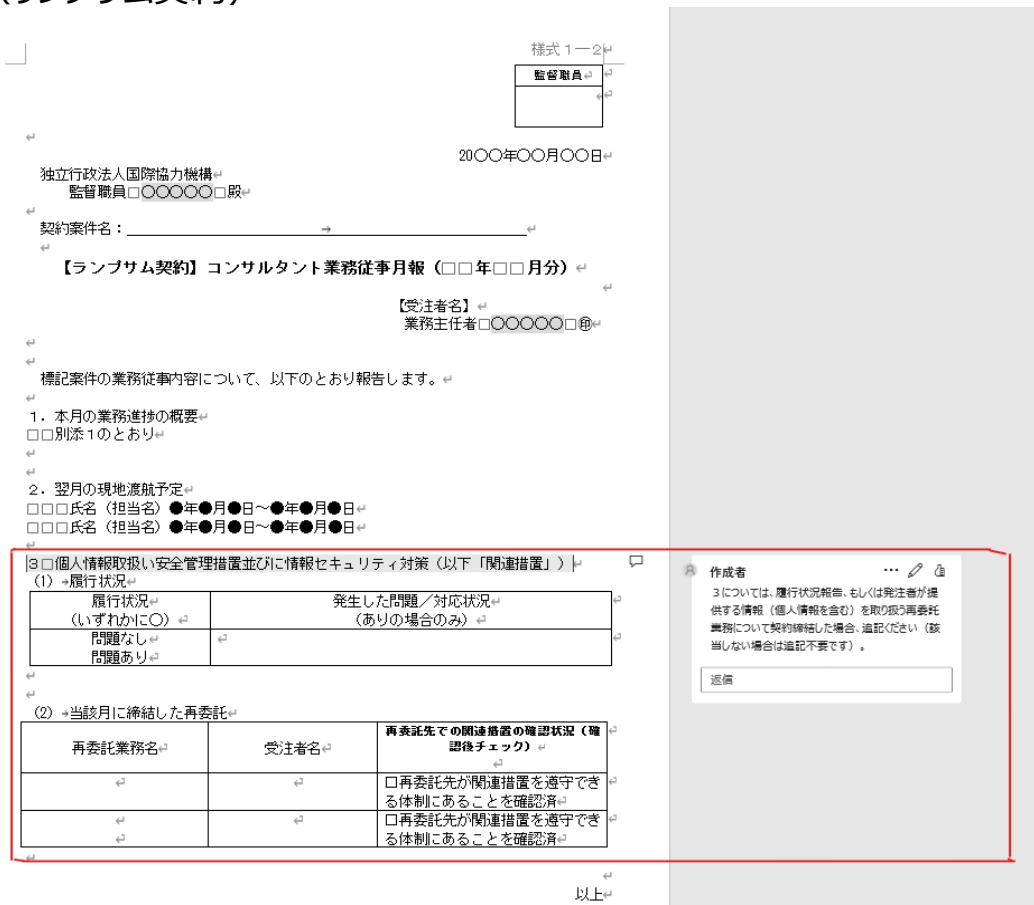
履行状況 （いずれかに〇）	発生した問題／対応状況（ありの場合のみ）
問題なし 問題あり	

以上

別添１：本月の業務進捗の概要（様式は任意）

作成者
履行状況報告について書面で行う際は、こちらを追記ください（報告しない場合は、追記不要です）
返信

（ランプサム契約）



様式１－２

監督職員

20〇〇年〇〇月〇〇日

独立行政法人国際協力機構
監督職員□〇〇〇〇〇□殿

契約案件名：

【ランプサム契約】コンサルタント業務従事月報（□□年□□月分）

【受注者名】
業務主任者□〇〇〇〇〇□㊞

標記案件の業務従事内容について、以下のとおり報告します。

１．本月の業務進捗の概要
□□別添１のとおり

２．翌月の現地渡航予定
□□□氏名（担当名）●年●月●日～●年●月●日
□□□氏名（担当名）●年●月●日～●年●月●日

３□個人情報取扱い安全管理措置並びに情報セキュリティ対策（以下「関連措置」）
（１）→履行状況

履行状況 （いずれかに〇）	発生した問題／対応状況 （ありの場合のみ）
問題なし 問題あり	

（２）→当該月に締結した再委託

再委託業務名	受注者名	再委託先での関連措置の確認状況（確認後チェック）
		□再委託先が関連措置を遵守できる体制にあることを確認済
		□再委託先が関連措置を遵守できる体制にあることを確認済

以上

作成者
３については、履行状況報告、もしくは発注者が提供する情報（個人情報を含む）を取り扱う再委託業務について契約締結した場合、追記ください（該当しない場合は追記不要です）。
返信

７．その他役務の提供等にかかる契約関連様式の変更点

１．入札説明書（総合評価落札方式、最低価格落札方式）・企画競争説明書（企画競争）における修正箇所

（１）情報保全案件の場合、「競争参加資格」として以下の項目を追加

契約締結後には、令和5年度版「政府機関の情報セキュリティ対策のための　統一基準群」及びこれに準拠する機構内関連規程に基づき機構が定める「個人情報取扱い安全管理措置並びに情報セキュリティ対策」（別添●、別添●）を遵守するとともに、「個人情報保護及び情報セキュリティに関する情報」（別添●）にて、個人情報保護及び情報セキュリティにかかる管理体制等の報告を行うこと。

（２）その他の案件の場合、「その他」欄に以下の項目を追加

契約締結後には、令和5年度版「政府機関の情報セキュリティ対策のための　統一基準群」及びこれに準拠する機構内関連規程に基づき機構が定める「個人情報取扱い安全管理措置並びに情報セキュリティ対策」（別添●、別添●）を遵守するとともに、「個人情報保護及び情報セキュリティに関する情報」（別添●）にて、個人情報保護及び情報セキュリティにかかる管理体制等の報告を行うこと

（３）再委託を行う場合（再委託先が発注者が提供する情報（個人情報を含む。）を扱う場合）

再委託先の選定に係る打合簿において、「再委託先が情報セキュリティ・個人情報保護に係る対策を遵守できる体制であること」を確認した旨を記載する。

（４）履行状況の確認

原則的に、各契約において定められる成果品又は提出物において、履行状況の報告をしていただくことを想定。

８．質疑応答

以下のお問い合わせFormsより、随時お問い合わせも受け付けています。（2025年3月末まで）

https://forms.office.com/r/CjtFzDijpy

JICAホームページにも掲載予定です。