# 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応について

《初版》

2025 年 1 月

独立行政法人国際協力機構

情報システム部

国際協力調達部

**改訂履歴**

| 改定年月日 | 改定箇所 | 改定内容 |
|---|---|---|
| 2025 年 1 月 27 日 | ― | 初版決定 |

# 目次

# 1　はじめに

## 1.1　本ガイドラインの目的

近年、調達から販売、業務委託等に至るまでの一連の商流において、セキュリティ対策が不十分な組織への攻撃の足がかりとしてのサプライチェーン攻撃や、ソフトウェア開発のライフサイクルに関与するモノ（ライブラリ、各種ツール等）や人の繋がり（ソフトウェアサプライチェーン委託、組織、プロセス等）を攻撃されるといった脅威が顕在化し、業務を委託している外部組織から情報漏えいが発生する事案が度々報じられています。独立行政法人情報処理推進機構（IPA）より毎年公開されている「情報セキュリティ 10 大脅威 2024」[1]では、こうした「サプライチェーンの弱点を悪用した脅威」が、6 年連続で 6 回とも上位に位置付けられたことが示されています。

こうした状況を背景に、サイバーセキュリティ基本法に基づきサイバーセキュリティ戦略本部が決定する政府機関等における対策基準である「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」[2]（以下「政府統一基準群」）では、こうした外部委託（業務委託、クラウドサービス利用、機器等の調達）におけるサプライチェーン上のリスクに対応するための対策が、改定の都度見直され厳格になってきています。独立行政法人国際協力機構（以下「JICA」）は、この政府統一基準群に準拠するよう情報セキュリティポリシーを策定し、こうした対策基準を遵守することが求められています。

また、3 年毎に改正される「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」）においても、個人情報の漏えい、滅失又は毀損（以下「漏えい等」）を防止するために、受託者を含め安全管理措置を講じることが義務付けられ、個人情報保護法ガイドライン[3]では個人情報の取扱いに係る業務を外部に委託する場合に講ずべき対策や安全管理措置が示されています。

本ガイドラインは、こうしたサプライチェーン上のリスクに対応するために、受託者の皆様にお願いする事項を含む調達・契約の手続き及び書面について解説するものです。

## 1.2　サプライチェーン・リスク

### 1.2.1　JICA が想定しているサプライチェーン・リスクに係る脅威の例

JICA におけるサプライチェーンは、様々な事業の受託者やその再受託先、ソフトウェア・機器・サービス提供元等、多岐に渡ります。JICA にて強固なセキュリティ対策を実施し、

[1] IPA｜情報セキュリティ 10 大脅威 2024（https://www.ipa.go.jp/security/10threats/10threats2024.html）
[2] 内閣官房内閣サイバーセキュリティセンター（NISC）｜
「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」
（https://www.nisc.go.jp/policy/group/general/kijun.html）
[3] 個人情報保護委員会｜個人情報保護法等＞法令･ガイドライン等（https://www.ppc.go.jp/personalinfo/legal/）

JICA への直接攻撃が困難であったとしても、そのサプライチェーンの脆弱な部分を攻撃者が攻撃することで、JICA が受託者に提供した秘密情報[4]（政府統一基準群における「要機密情報」）が第三者に流出したり、その脆弱な部分を経由して間接的および段階的に標的組織となる JICA 及び関係する政府機関等への侵入を許してしまったりすることが想定されます。

以下に想定されるサプライチェーン・リスクに係る脅威の例を示します。

- JICA の秘密情報を取扱う受託者又は再受託者（再々受託等、多重の受委託が行われる場合はその全ての受託者を含む。）が攻撃され、受託者又は再受託者が取り扱っている JICA の秘密情報が窃取される
（JICA を標的とした攻撃として受託者又は再受託者が狙われる場合もあれば、無差別な攻撃[5]により結果的に JICA の秘密情報が窃取される場合も想定される）

- 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

情報システムに関する内容を含む契約はさらに以下の脅威があります。

- JICA が利用しているソフトウェアの開発元や MSP（マネージドサービスプロバイダー）等が攻撃されることで、当該ソフトウェアやサービスにウイルス等が仕込まれ、ソフトウェアやサービス利用開始時や提供開始時またはバージョンアップ時にウイルスに感染させられ、JICA の秘密情報の窃取及び情報の改ざんや情報システムを停止させるなどして、情報システムを機能不全に陥れ、JICA の業務を混乱させる

- 受託者又は再受託者の従業員が、JICA の情報システムが稼働した後に容易

---

[4] 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

[5] 近年では、特にランサムウェア※による被害が頻発しており、受託者又は再受託者の情報システムやサービス自体が侵害されることで、委託元の機密情報が流出してしまう事案が絶えない状況にあります。

※ ランサムウェアとは、Ransom と Software を組み合わせた造語であり、ウイルスの一種です。攻撃者は PC やサーバーをランサムウェアに感染させ、様々な脅迫により金銭を要求します。さらに、攻撃者は複数の脅迫を組み合わせる（ランサムウェアにより暗号化したデータ復旧のための金銭要求だけでなく、盗んだデータを外部公開されないための金銭要求も行われることが一般化）ことで、攻撃を受けた組織がシステムを復旧するために金銭を支払うことを検討せざるを得ない状況を作り出そうとします。攻撃者は組織の規模や業種に関係なく攻撃を行う点にも注意が必要です。
（参考）NISC ストップ！ ランサムウェア ランサムウェア特設ページ
（https://www.nisc.go.jp/tokusetsu/stopransomware/）

に機密情報を窃取することを可能とする仕組みを、開発時に悪意を持って組み込むことにより、当該情報システムの稼働開始後に、当該情報システムで取り扱われる秘密情報を窃取するなどの攻撃が行われる

- 悪意のある製品ベンダ又は当該ベンダの従業員によって、JICA が利用する機器が構成するシステムに不正に侵入することができる経路や、不正に情報を窃取するための経路等を生じさせる不正プログラムを製造過程においてあらかじめ組み込み、当該製品を JICA で調達することで、当該情報システムの稼働開始後に、情報システムを停止させるなどして JICA の情報システムを機能不全に陥れ、業務を混乱させる
- JICA の情報システムの運用・保守の受託者又は再受託者若しくはこれらの従業員が、ソフトウェア更新作業の際に不正プログラムを情報システムに組み込むことにより、当該情報システムが踏み台となって、他の情報システムへ攻撃が行われる
- JICA の情報システムの運用・保守の受託者又は再受託者若しくはこれらの従業員の中に日本政府との利益相反が生じる外国の政府機関に関連する者が存在し、当該従業員が正規の運用作業を装って、情報システムから外国との交渉に関わる秘密情報を窃取する

### 1.2.2　JICA が想定しているサプライチェーン・リスクに係る脆弱性の例

以下に前節に示したサプライチェーン・リスクの脅威を増大させる要因となる脆弱性の例を示します。

- 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

情報システムに関する内容を含む契約はさらに以下の脆弱性があります。

- 受託者又は再受託者において、納入する機器やソフトウェアの設計書の管理が不十分である

- 受託者又は再受託者において、開発環境や納入物品、従業員等の情報セキュリティ管理に係る手順が整備されていない
- 受託者又は再受託者による運用中の情報システムのハードウェア交換又はソフトウェア更新等において、交換するハードウェア若しくは更新するソフトウェア等の安全性の確認又は作業における情報セキュリティ管理が不十分である
- 受託者又は再受託者が、製造過程や製造場所等が不明確な機器等を使用しているなど、機器等の製造事業者から安全性に関わる十分な情報を得ていない

## 2　JICA が求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

### 2.1　手続きのポイント

業務委託に際して受託者の皆様に最低限講じていただく「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１、別添２）の遵守について表明いただくと共に、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」（別添３）を提出いただきます。具体的な手続きにつきましては、契約種別毎に異なりますので、入札説明書や募集要項等をご確認ください。

### 2.2　サプライチェーン・リスク対応が必要な契約類型

JICA では、サプライチェーン・リスク対応が必要な契約として、業務内容や取り扱う情報により、大きく以下の３つの類型があると想定しています。

① 要保護情報[6]を取扱う契約

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[7]を含む契約

---

[6] 「要保護情報」とは、要機密情報、要保全情報、要安定情報のいずれかに該当する情報を指します。
「要機密情報」とは、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）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む情報を指します。
「要保全情報」とは、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を指します。
「要安定情報」とは、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を指します。

[7] 委託する業務内容に情報システムの開発・構築又は運用・保守、アプリケーション・コンテンツの開発を含む場合（主目的が情報システム）と、委託業務を実施するために受託者が新たに構築・運用する情報システム（当該情報システムにおいてクラウドサービス等を利用する場合も含む）を用いる場合（主目的が情報システム以外）の双方が対象です。なお、例えば相手国の開発事業への支援の一環として情報システムの構築支援等を行う場合は、JICA の要保護情報を扱わないので対象外となります。

受託者の皆様に最低限講じていただくべき「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」の厳格さは、②＞① の順となるよう定めており、大多数の契約が該当する① については、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水準となる基本的な情報セキュリティ対策の実施を受託者の皆様にお願いするものです。

「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」は、基本的に中小規模事業者を対象として作成・公表されている各種ガイドライン文書を参照して策定しており、対策項目毎の簡単な説明と例示に留めていますので、その考え方や具体的な運用については、出典としている各ガイドライン文書の内容も参照いただいた上で、受託者の皆様の組織及び運用環境にて実際に講じている対策状況を確認ください（詳細は 2.5 参照）。

なお、①～③の類型は各々独立しているものではなく、下図に示すように「厳格な情報保全の必要がある契約」かつ「情報システムに関する契約」に該当する場合もある点に留意ください。

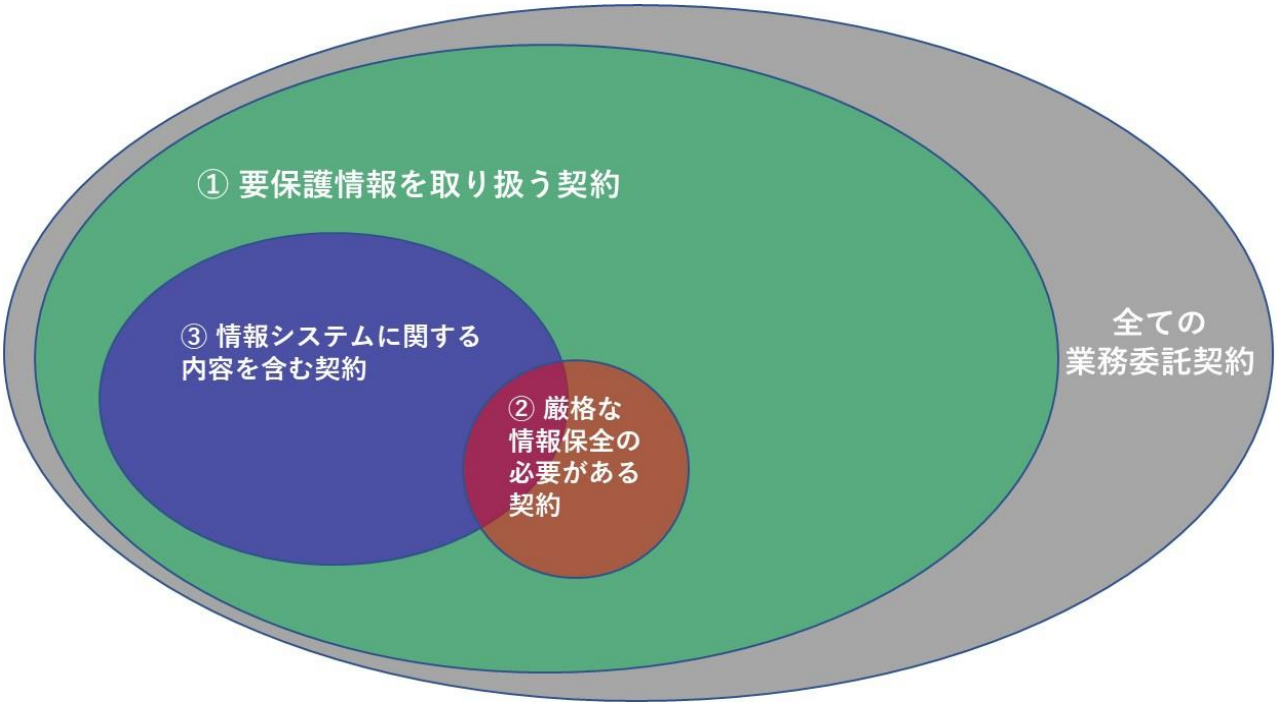


**図 1　契約類型のベン図**

委託する業務内容及び取扱う情報の格付に応じ、「どの契約類型に該当するか」や「契約書にて適用すべき条項」が異なることとなり、受託者に最低限講じていただくべき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水準も異なります。

JICA では、関連する以下の書面を定めています。

- 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）」
- 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

保全の必要がある契約用）」

- 別添３：「個人情報保護及び情報セキュリティに関する情報」

別添１及び別添２の「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」は、JICA の委託契約において、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です。別添１は「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）」、別添２は「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厳格な情報保全の必要がある契約用）」の内容となりますが、「③情報システムに関する内容を含む契約」の場合、別添１又は別添２どちらを使用するかについては、当該契約の内容に鑑みて、入札説明書や募集要項等にて指定させていただきます。

別添３「個人情報保護及び情報セキュリティに関する情報」は、「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記入いただくものです。

なお、「③情報システムに関する内容を含む契約」については、情報システムに JICA の意図しない変更が行われないことを保証する管理体制の提示を別添３の書面提出を通じて追加的に求めています（2.6「契約締結時にご提示いただく情報」の 1 を参照ください）。また、対象となる情報システム固有の業務仕様・要件については別途明示することとなり、当然ながらその一部として情報セキュリティ対策に関する要件を含みます。

## ２.３　契約書・約款における関連条文

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のいずれも、基本的に、各契約種別（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・草の根技術協力事業にかかる契約等）に応じて定められた同一の契約書・約款を利用します。①~③の区別に応じた異なる雛形があるわけではありませんので、ご留意ください。

以下にその他役務の提供等にかかる契約（一般契約）における契約書雛形より引用し、個人情報保護及び情報セキュリティに関する条文について解説します（条文番号は契約種別ごとの契約書・約款により異なります）。

**■＜第 26 条　個人情報保護＞**

四角枠内が条文です。下線部については、後に解説を記載しています。

（個人情報保護）
第 26 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。

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

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

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。

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。

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。

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。

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。

1. 【条文】第 26 条第 1 項第 2 号「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」

1.1 【解説】第 26 条第 1 項第 2 号（イ）～（ホ）の事項を確認する書面としては、JICA よりお示しする契約類型に応じた「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１又は別添２）及び対策実施のための管理体制等に関する「個人情報保護及び情報セキュリティに関する情報」（別添３）が相当します。「2．1　手続きのポイント」に記載のとおり、JICA にご提出いただき、双方で確認・合意させていただきます。

2 【条文】第 26 条第 2 項「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。」

2.1 【解説】発注者が「必要があると認めるとき」とは、例えば、業務において取り扱

う個人情報の量が著しく多い場合や秘匿性等が高い場合等、発注者が検査が必要と判断するとき、また、受注者の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、問題が発生（又はそのおそれを確認）したときにあたります。原則として、実地検査の方法で行いますが、委託先が遠隔にある等の理由がある場合は、例えばテレビ通話や写真等で管理の現況を確認することも可能です。

3　【条文】第 26 条第３項「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。」

3.1　【解説】受注者が再委託をする場合は、再委託先における個人情報の管理等が十分になされるよう、受注者が、再委託先における第 1 項各号についての履行を確認し、第 2 項に定める検査の措置を実施します。また、受注者は、発注者との定例会議等で、再委託先の個人情報の管理等の実施状況について適宜報告し、発注者の確認を得てください。

4　【条文】第 26 条第４項「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。」

4.1　【解説】再々委託先にも、受注者や再委託先と同様の義務を履行いただく必要があります。上記解説 3.1 に記載の、再委託時に受注者から再委託先に対して行う確認や、受注者が発注者に対して行う報告等を参考にご対応ください。例えば、第 26 条第 1 項第 2 号の「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」について、再々委託先の遵守状況については、再委託先から委託先、及び委託先から受注者への報告を通じ、最終的には委託先から発注者へ報告される必要があります。

**■＜第 26 条の 2　特定個人情報保護＞**

（特定個人情報保護）

第 26 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 26 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。

1　【条文】第 26 条の２第１項「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。」

1.1　【解説】「特定個人情報等」とはマイナンバー（個人番号）を含む個人情報のことです。委託業務においてマイナンバーを取り扱わない場合は、JICA からご提示する契約書案に２６条の２の記載はありません。

**■＜第 27 条　情報セキュリティ＞**

（情報セキュリティ）
第 27 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。
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
（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。

1　【条文】第 27 条第１項第２号「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。」

1.1 【解説】第 27 条第 1 項第 2 号（イ）～（ヘ）の事項を確認する書面としては、JICA よりお示しする契約類型に応じた「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 1 又は別添 2）及び対策実施のための管理体制等に関する「個人情報保護及び情報セキュリティに関する情報」（別添３）が相当します。「2．1　手続きのポイント」に記載のとおり、JICA にご提出いただき、双方で確認・合意させていただきます。

2 【条文】第 27 条第 2 項「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。」

2.1 【解説】発注者が「必要があると認めるとき」とは、情報セキュリティに関する問題が発生（又はそのおそれを確認）したときにあたります。主な監査内容としては、第 27 条第 1 項各号における情報セキュリティ対策の義務が正しく履行されているかを確認します。

3 【条文】第 27 条第 3 項「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。」

3.1 【解説】受注者が再委託をする場合は、再委託先における情報セキュリティ対策が十分になされるよう、受注者が、再委託先における第 1 項各号についての履行を確認し、第 2 項に定める情報セキュリティ監査の措置を実施します。また、受注者は、発注者との定例会議等で、再委託先の情報セキュリティ対策の実施状況について適宜報告し、発注者の確認を得てください。

**■＜第 27 条の 2　情報システムに関する業務における情報セキュリティ＞**

（情報システムに関する業務における情報セキュリティ）
第 27 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。

1 【条文】第 27 条の 2 第 1 項「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。」

1.1 【解説】委託業務内容が以下（１）、（２）のいずれにも当てはまらない場合は、JICAからご提示する契約書案に第 27 条の２の記載はありません。

（1）委託する業務内容に情報システムの開発・構築又は運用・保守、アプリケーション・コンテンツの開発を含む場合（主目的が情報システム）

（2）委託業務を実施するために委託先が新たに構築・運用する情報システム（当該情報システムにおいてクラウドサービス等を利用する場合も含む）を用いる場合（主目的が情報システム以外）

２ 【条文】第 27 条の２第１項第１号「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」

2.1 【解説】情報システムに関する業務委託において、「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」が確保されることを求めています。本内容に対応する情報として、「個人情報保護及び情報セキュリティに関する情報」（別添３）の「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」の箇所において、「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）」を記載ください。

３ 【条文】第 27 条の２第１項第２号「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」

3.1 【解説】第 27 条の２第１項第１号における管理体制等を確認するための参考情報として提出いただくものです。契約種別によって呼称が異なりますが、ここでいう「業務責任者」は、業務主任者、業務管理者と同義です。また、本内容については、基本的に契約プロセスの中でご提出いただく資料等に含まれていますが、そうでない場合はご提出をお願いいたします。

## ２.４ 契約中の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

「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」は、本契約締結後に提出いただく書面にて対策実施の遵守を誓約いただきます[8]。

多くの契約が対象となる ①要保護情報を取り扱う契約 では、個人情報保護委員会より公

[8] 特定の項目が遵守できない場合には、打合せ簿等の書面にてその合理的な理由を示していただいた上で、項目を適用しないことを記載いただくのが望ましいと考えます。

表されている「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）」[9]に記載されている“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」”（以下、「個情委ガイドライン（通則編）」と記します。）及び IPA より公表されている「中小企業の情報セキュリティ対策ガイドライン」[10]（以下「情報セキュリティ対策ガイドライン」と記します。）に添付されている“付録 3：5分でできる！情報セキュリティ自社診断”[11]に基づき記載しています。（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」（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のガイドライン（通則編）には、安全管理措置として講じるべき措置及び各措置における多くの手法が例示されていますので、これらを参照の上、実際に講じている対策をご確認ください。

また、情報セキュリティ対策ガイドラインには、組織の経営層に意識していただくべきこと（経営者編）と実運用上講ずべき対策（実践編）について示され、実践編には対策項目の詳細についても記載されていますので、これらを参照の上、実際に講じている対策をご確認ください。

「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」に記載している対策は項目毎の簡単な説明と例示に留めていますので、その考え方や具体的な運用については、出典としている各ガイドラインの内容も参照のうえ、受託者の皆様の組織及び運用環境にて実際に講じている対策状況を確認ください。

## ２.５　契約締結時にご提示いただく情報

「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」実施のための管理体制等に関する「個人情報保護及び情報セキュリティに関する情報」（別添 3）には、以下の記入項目を設けておりますので、適切な情報を記入の上ご提示願います。

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」として、「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。③情報システムに関する内容を含む契約のみ。）」を記入いいただきます。これら３つの責任者・管理者については、それぞれ兼任可能です。（「品質保証管理者」についての記載は、「政府機関等の対策基準策定の

[9] 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（通則編）（https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a10）
[10] IPA｜中小企業の情報セキュリティガイドライン（https://www.ipa.go.jp/security/guide/sme/about.html）
[11] IPA｜中小企業の情報セキュリティガイドライン 付録３：５分でできる！情報セキュリティ自社診断（https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf）

ためのガイドライン（令和５年度版）の一部改定（令和６年７月）」p.159、基本対策事項 4.1.2(1)-1 a) に記載の「・情報システムの開発工程において、機関等の意図しない変更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、当該品質保証体制が書類等で確認できること。」を反映したものです。）また、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される方についても記入いただきます。

「（２）業務作業場所」については、自然災害等の影響への考慮や、機密性の高い情報を受託者従業員の家で取り扱う場合はリモートワークのセキュリティ対策状況に考慮するなど、情報セキュリティの観点から、JICA と受託者が業務の作業場所についての共通認識を持つことが重要となります。可能な限り具体的に記載ください。

2　**個人情報の取り扱いに際し講ずべき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」及び「（２）履行状況の確認頻度」を検討し、記入いただきます。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りますので、特に決まったものはありませんが、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ます。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ます。

## ２.６　情報システムに関する契約にて考慮いただくべき事項

情報システムに関する契約に該当する場合には、必要に応じ入札時及び業務仕様・要件において、以下に関する資料提出及び情報提供をお願いする場合がありますので、個々の調達時にご確認ください。

- 当該情報システムにおいてクラウドサービス等を利用する場合には、JICA 内規等の定めに従い JICA 内にて申請・承認手続きを経る必要があり、そうした手続きに必要な書面・資料の提出をお願いすることとなります。政府統一基準群では、クラウドサービスにて秘密情報を取扱う場合には、原則として「政府情報システムのためのセキュリティ評価制度（ISMAP（Information System Security Management and Assessment Program））」に基づきクラウドサービスリストに登録されたクラウドサービスから選定するよう定められており、もし未登録のクラウドサービスを利用する場合には、「ISMAP 管理基準の管理策基準が求める対策と同等以上の水準にあること」を確認させていただく必要があります。

（参考）ISMAP ポータル｜ISMAP 概要
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005

- 関連する機器・役務等の調達が政府決定である「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」制度の対象となる場合には、JICA は内閣サイバーセキュリティセンター（NISC）を窓口として NISC 及びデジタル庁と協議する必要があるため、調達先に対し協議に必要な情報の提供をお願いすることとなります。また、NISC による確認の結果、調達内容を修正・追加する場合があり、調達先に対しそうした手続きに必要な書面・資料の提出をお願いすることとなります。

（参考）「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」
https://www.nisc.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf

- 調達対象となる機器等に関し、情報セキュリティ機能の客観的な評価を必要とする場合には、CC（Common Criteria）認証製品を調達要件とする場合がありますので、要件を満たす機器等をご提案願います。（Appendix 2.3　情報技術セキュリティの評価基準（ISO/IEC 15048）参照）
- 調達対象となるソフトウェア及び機器等に関し、ソフトウェアの透明性の確認を行い、脆弱性に関する対策の効率化の観点から、SBOM の提供等を調達先に求める場合がありますので、要件を満たす調達先を選定の上ご提案願います。（Appendix 2.5　ソフトウェアの脆弱性管理のための SBOM 活用 参照）

## Appendix 1　JICA におけるサプライチェーン・リスク対応の考え方

サプライチェーンとは、一般的に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するもので、商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群を指しますが、このような「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しく、関係組織も含めたセキュリティ対策が必要な脅威と言えます。また、ソフトウェア開発のライフサイクルに関与する全てのモノ（ライブラリ、各種ツール等）や人の繋がり（ソフトウェア開発に関わる人、組織、プロセス等）をソフトウェアサプライチェーンと呼び、このような「ソフトウェアの繋がり」を悪用した攻撃も近年大きな脅威となっており、更なる対策が必須となっています。

1.2　サプライチェーン・リスクに記したように、JICA の要保護情報を取扱う業務受託者、ソフトウェアやサービスの提供元、機器等の調達先等のサプライチェーンに介在する全ての事業者において十分なセキュリティ対策が講じられているかを JICA が確認することは困難であり、サプライチェーンを構成する一部の脆弱な事業者等が攻撃を受けることで、JICA も間接的及び段階的に被害を受けてしまうことが想定されます。また、サプライチェーンの中には、我が国との利益相反が存在する可能性がある他国の政府によって所有、指示又は補助を受けている事業者が存在していることも否定できず、政府機関等ではそのような事業者による不正行為に起因した情報窃取等の発生も懸念されています。クラウドサービス利用についても同様のリスクが存在することは否定できません。

このような現状を踏まえ、政府統一基準群ガイドラインには、要保護情報を取扱う業務を委託する場合、情報システムの構築やアプリケーションの開発等の業務を委託する場合、クラウドサービス利用する場合、機器等を調達する場合等において、調達元となる政府機関等が実施すべき情報セキュリティ上のサプライチェーン・リスクへの対応に係る様々な遵守事項及び基本対策事項が定められています。

JICA においても、政府統一基準群に準拠するよう定めている内部規程「独立行政法人国際協力機構サイバーセキュリティ対策に関する規程」（平成 29 年 4 月 3 日規程㈱第 14 号、以下「規程」）第 19 条に外部委託に際し講ずべき対策を定め、政府統一基準群ガイドラインにおける遵守事項及び講ずべき基本対策事項に準拠するよう「サイバーセキュリティ対策実施細則」（平成 29 年 4 月 3 日細則㈱第 11 号、以下「細則」）第 4 編 外部委託（第 53 条～第 72 条）を定め、多くの基本対策事項を複数の準内部規程として規定しています（以下、JICA の内部規程及び準内部規程を「JICA 内規等」と記します。）。また、個人情報保護法令・ガイドライン等、マイナンバー関係法令・ガイドライン等及び EU GDPR（一般データ保護規則）に準拠するよう定めている内部規程「個人情報保護に関する実施細則」（平成 17 年 4 月 1 日細則(総)第 11 号、以下「個人情報保護細則」）第 7 章 保有個人情報等の取扱いに係る業務の委託等（第 45 条・第 46 条）においては、個人

情報の取扱いの委託を実施する際に講ずべき対策について規定しています。

サプライチェーン・リスクを軽減するためには、委託元である JICA が、受託者における管理体制が信頼できるものであるか否か、受託者によって提供された製品やサービス等の成果物が JICA の業務や情報を守る上で信頼できるものか否かを見極めなければなりませんが、全ての受託者又は再受託者による管理体制の適切性を詳細に確認する、あるいは全てのハードウェア及びソフトウェアに JICA が意図しない不正プログラム等のリスクが存在しないことを検証する、といったことを直接実施するのは困難であり、膨大なコストが必要となります。

そのため、受託者の皆様に対して、最低限講じていただくべき対策を示す、委託業務及び調達対象となる製品やサービスに関する事業の実施状況に係る情報を求める、発注者の意図しない変更を攻撃者が情報システムや機器等に加えることにより、機密情報を窃取するなどの情報セキュリティ上のサプライチェーン・リスクへの対応のための厳格な管理体制を求めるなどの対策を中心に、受託者の皆様が委託業務にて使用する機器・サービス及び、それらに係る再受託者における対策実施をお願いすることとしたものです。

調達案件に関連する業務や取り扱う情報の特性に応じ、1.2.1 節や 1.2.2 節に示した脅威や脆弱性を踏まえ、サプライチェーン・リスクを特定、分析し、委託する業務内容（提供する情報の保管・利用・廃棄、情報システム等の企画・要件定義、調達・構築及び運用・保守・廃棄のライフサイクル）の各工程で求められる対策を適切に実施いただくよう、受託者の皆様と合意形成しなければなりません。

JICA では、以上のような考え方に基づき、受託者の皆様に本ガイドラインに示す対応をお願いすることとしたものです。

# Appendix 2　国際規格等と政府方針文書等における記述との関係

政府統一基準群におけるサプライチェーン上のリスクに対応するための対策は、様々な国際規格等や政府方針文書を踏まえ定められています。

## Appendix 2.1　サプライチェーン・リスク対策に関する国際規格（ISO/IEC 27036）

サイバーセキュリティにおけるサプライチェーン・リスク対策に関する国際規格として ISO/IEC 27036 が策定されています。ISO/IEC27036 は「第 1 部：概要及び概念（Part 1: Overview and concepts）」、「第 2 部：要求事項（Part 2: Requirements）」、「第 3 部：ハードウェア，ソフトウェアおよびサービスのサプライチェーンセキュリティに関するガイドライン（Part 3: Guidelines for hardware, software, and services supply chain security）」、「第 4 部：クラウドサービスのセキュリティの指針（Part 4: Guidelines for security of cloud services）」という 4 パートで構成され、ライフサイクルプロセスに対応したフレームワークとして整理されています。内閣官房内閣セイバーセキュリティセンター（NISC）が定める「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」（以下「サプライチェーン・リスク対応手引書」と記します。）には、対策の考え方や具体的な対策事項記述に際し同規格を参考としたことが示されています。

（参考）NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」
https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf

## Appendix 2.2　非政府機関における要保護情報等の保護に関する対策基準（NIST SP800-171）

米国国立研究所（NIST）が策定するガイドライン NIST SP800-171 は、サプライチェーンを通じての情報漏えいを防ぐことを目的に、非政府機関における要保護情報等の取扱いに係る情報セキュリティ対策の基準を定めたものです。政府統一基準群では、「統一基準 4.1.1(3)業務委託実施期間中の対策」として委託業務における情報の適正な取扱いを受託者に担保させるために実施することを求めるべき対策として、この NIST SP800-171 を参考とした対策が示されています。

（参考）NIST「SP800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations」
https://csrc.nist.gov/pubs/sp/800/171/r3/final

### Appendix 2.3　情報技術セキュリティの評価基準（ISO/IEC 15048）

情報技術に関連した製品及びシステムが情報技術セキュリティの観点から適切に設計され、その設計が正しく実装されていることを評価するための枠組みである CC（Common Criteria）に関する標準は、国際規格 ISO/IEC 15048 として策定されています。同規格は多くの国で政府調達基準とされており、政府統一基準群では、政府機関の情報システムの構成要素として適切なセキュリティ対策が必要とされる「セキュリティ要件リスト」に記載された次の 11 分野の製品に関し、情報セキュリティ機能の客観的な評価を必要とする場合には、CC 認証製品を調達要件とすることが求められています。

（参考）経済産業省「IT セキュリティ評価及び認証」
https://www.meti.go.jp/policy/netsecurity/cc.html

（参考）独立行政法人情報処理推進機構（IPA）「CC(ISO/IEC 15408)概説」
https://www.ipa.go.jp/security/jisec/about/about.html

（参考）独立行政法人情報処理推進機構「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」
https://www.ipa.go.jp/security/it-product/guidebook.html

### Appendix 2.4　安全なソフトウェア開発の慣行に基づく開発についてのフレームワーク（NIST SP800-218）

NIST が策定するガイドライン NIST SP800-218 は、安全なソフトウェア開発の慣行に基づく開発についてのフレームワークであり、政府統一基準群では、ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認において、調達先が安全なソフトウェア開発の慣行に基づく開発を実施していることを確認するために同フレームワークを参考にすることが示されています。

（参考）NIST「SP800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities」
https://csrc.nist.gov/pubs/sp/800/218/final

### Appendix 2.5　ソフトウェアの脆弱性管理のための SBOM 活用

SBOM（Software Bill of Materials：ソフトウェア部品表）とは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストのことで、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができるもので、経済産業省より SBOM に関する手引書が公表されています。また、米国では国家のサイバーセキュリティの改善に関する大統領令として発令されています。

政府統一基準群では、調達対象となるソフトウェア及び機器等の選定基準の一つとして、SBOM の提供等を調達先に求めることでソフトウェアの透明性の確認を行い、脆弱性に関する対策の効率化の観点から SBOM を活用することも考えられることが示されています。

（参考）：経済産業省

「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0」

https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

（参考）：米国大統領令

「Executive Order on Improving the Nation’s Cybersecurity」

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

「Improving the Nation's Cybersecurity (EO) 14028」

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

# Appendix 3　対象となる JICA 内規等における定め

本書の対象となる JICA 内規等の定めを以下に示します（下線部がサプライチェーン・リスクに関連する記述となります）。

## Appendix 3.1　サイバーセキュリティ対策に関する規程における定め

■ 規程

(外部委託)
第 19 条 機構は、機構の情報を取り扱わせる業務を委託する場合には、必要な措置を定め、実施するものとする。
2 機構は、業務委託を実施する際に要機密情報を取り扱わせる場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様にも含めるものとする。
3 機構は、クラウドサービスを利用する場合には、情報セキュリティを確保するための措置を定め、実施するものとする。
4 機構は、機器等の調達に当たり、機器等の開発等で不正な変更が加えられない管理がなされている等のサプライチェーン・リスクへの適切な対処を含む選定基準を定めるものとする。

※　上記の規定は「政府機関等のサイバーセキュリティ対策のための統一規範」第 19 条に準拠するよう定めているものです。

## Appendix 3.2　サイバーセキュリティ対策実施細則における定め

**細則 第 1 編 総則 第 2 章 情報の格付の区分・取扱制限**

(情報の格付の区分)
第 7 条 情報について、機密性、完全性及び可用性の 3 つの観点を区別し、本細則で用いる格付の区分を用いる。
2 格付の定義を変更又は追加する場合には、その定義に従って区分された情報が、本細則で定めるセキュリティ水準と同等以上の水準で取り扱われるようにするものとする。
3 他機関等へ情報を提供するときは、機構の対策基準における格付区分と本統一基準における格付区分の対応について適切に伝達するため、本条に定める格付及び取扱制限を明示する。
4 機密性についての格付の定義は以下のとおりとする。
(1) 機密性 3 情報とは、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とする。
(2) 機密性 2 情報とは、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」以外の情報とする。

(3) 機密性 1 情報とは、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とする。

(4) 機密性 2 情報及び機密性 3 情報を「要機密情報」という。

5 完全性についての格付の定義は、以下のとおりとする。

(1) 完全性 2 情報とは、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とする。

(2) 完全性 1 情報とは、完全性 2 情報以外の情報（書面を除く。）とする。

(3) 完全性 2 情報を「要保全情報」という。

6 可用性についての格付の定義は、以下のとおりとする。

(1) 可用性 2 情報とは、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とする。

(2) 可用性 1 情報とは、可用性 2 情報以外の情報（書面を除く。）とする。

(3) 可用性 2 情報を「要安定情報」という。

7 要機密情報、要保全情報又は要安定情報に一つでも該当する情報は、「要保護情報」という。

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」1.2(1) に準拠するよう定めているものです。

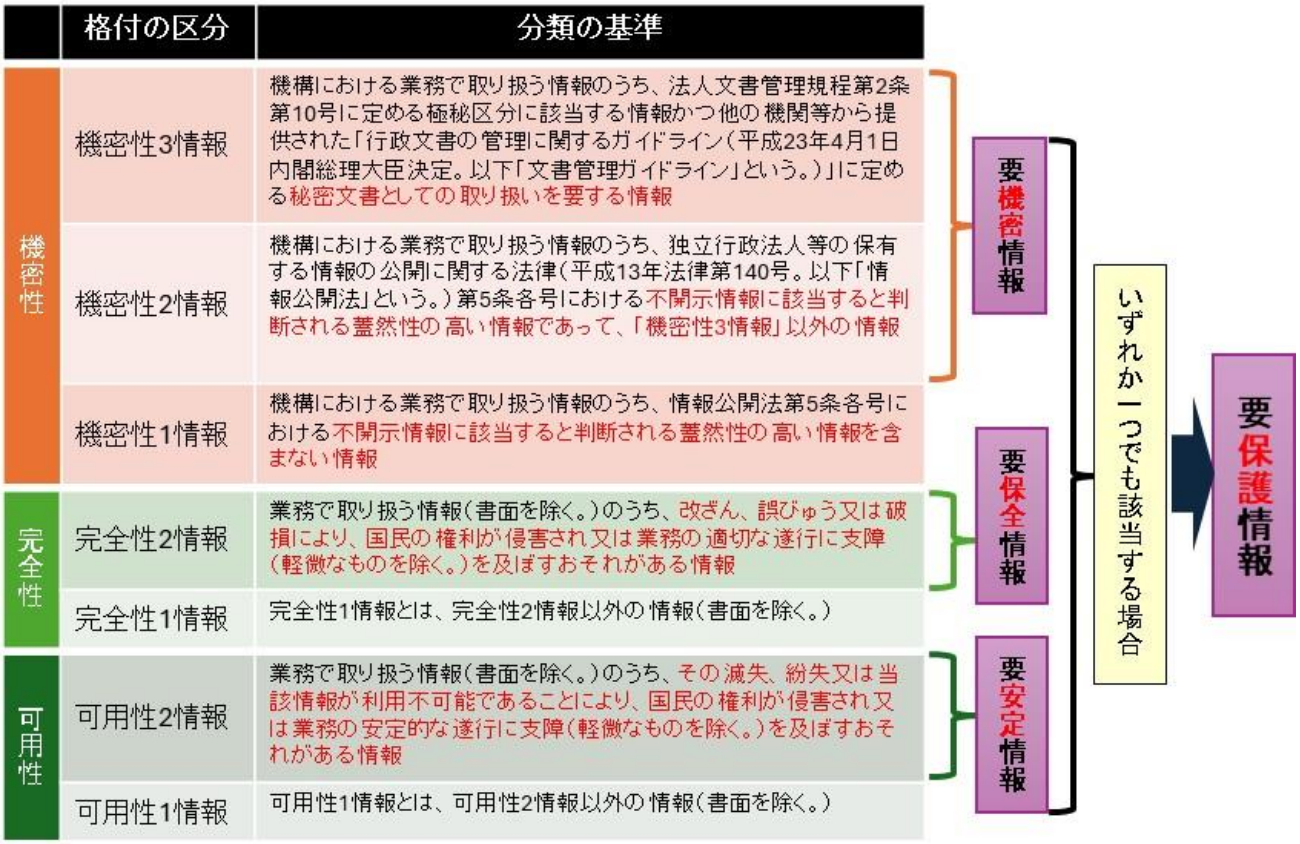

**図 2　情報の格付の区分**

**■ 細則 第 4 編 外部委託 第 1 章 業務委託 第 1 節 業務委託**

(業務委託実施前の対策)

第 54 条 情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施する。

(1) 委託する業務内容の特定

(2) 委託先の選定条件を含む仕様の策定

（中略）

2 情報セキュリティ責任者は、以下を全て含む情報セキュリティ対策を実施することを委託先の選定条件とし、その旨を仕様に含める。

(1) 委託先に提供する情報の委託先における目的外利用の禁止

(2) 委託先における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

(3) 情報セキュリティインシデントへの対処方法

(4) 情報セキュリティ対策その他の契約の履行状況の確認方法

(5) 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

3 情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含める。

(1) 情報セキュリティ監査の受入れ

(2) サービスレベルの保証

4 情報セキュリティ責任者は、委託先との情報の受渡し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委託先と合意し、定められた手順により情報を取り扱う。

5 情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、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、本条第 2 項及び第 3 項の措置の実施を委託先に担保させるとともに、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に必要な情報を機構に提供し、機構の承認を受けるよう、仕様に含める。また、委託判断基準及び委託先の選定基準に従って再委託の承認の可否を判断する。

6 情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求める。

(1) 仕様に準拠した提案

(2) 契約の締結

(3) 委託先において要機密情報を取り扱う場合は、秘密保持契約（NDANDA）の締結

7 情報セキュリティ責任者は、以下を全て含む委託先における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等を提出させること。また、変更があった場合は、速やかに再提出させること

(1) 当該委託業務に携わる者の特定

(2) 当該委託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

(業務委託実施期間中の対策)

第 55 条 情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施する。

（中略）

(2) 契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認

| |
|---|
| （中略）<br>2 情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求める。<br>(1) 情報の適正な取扱いのための情報セキュリティ対策<br>(2) 契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告<br>(3) 委託した業務において、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おける、委託事業の一時中断などの必要な措置を含む対処 |
| (業務委託終了時の対策)<br>第 56 条 情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施する。<br>(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収<br>(2) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認<br>2 情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求める。<br>(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検<br>(2) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消 |

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」4.1.1⑵、4.1.1⑶、4.1.1⑷ に準拠するよう定めているものです。

**■ 細則 第 4 編 外部委託 第 1 章 業務委託 第 2 節 情報システムに関する業務委託**

| |
|---|
| (情報システムに関する業務委託における共通的対策)<br>第 57 条 情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に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対策に係る選定条件を加え、仕様を策定する。<br>2 情報システムセキュリティ責任者は、委託先の選定に際し、以下を全て含む情報セキュリティ対策を実施することを情報システムに関する業務委託先の選定条件に加え、その旨を仕様に含める。<br>(1) 委託先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<br>(2) 委託先の資本関係、役員等の情報、委託事業の実施場所並びに委託事業従事者の所属、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 、実績及び国籍に関する情報提供 |
| (情報システムの構築を業務委託する場合の対策)<br>第 58 条 情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求める。<br>(1) 情報システムのセキュリティ要件の適切な実装<br>(2) 情報セキュリティの観点に基づく試験の実施<br>(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 |
| (情報システムの運用・保守を業務委託する場合の対策) |

第 59 条 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、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ための要件について、契約に基づき、委託先に実施を求める。

2 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求める。

(機構向けに情報システムの一部の機能を提供するサービスを利用する場合の対策)

第 60 条 情報システムセキュリティ責任者は、機構外の一般の者が機構向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加える。

（中略）

4 情報システムセキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、業務委託サービスを選定する。また、業務委託サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求める。

5 情報システムセキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、業務委託先の信頼性が十分であることを総合的・客観的に評価し判断する。

（以下略）

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」4.1.2(1)、4.1.2(2)、4.1.2(3)、4.1.2(4) に準拠するよう定めているものです。

**■ 細則 第 4 編 外部委託 第 2 章 クラウドサービス 第 1 節 クラウドサービスの選定**

(クラウドサービスの選定)

第 62 条 情報システムセキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討する。

2 情報システムセキュリティ責任者は、取り扱う情報の格付及び取扱制限並びにクラウドサービス提供者との情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定める。

(1) クラウドサービスに求める情報セキュリティ対策

(2) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(3) クラウドサービスに求めるサービスレベル

3 情報システムセキュリティ責任者は、クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則として ISMAP 等クラウドサービスリストからクラウドサービスを選定する。

(クラウドサービスの利用に係る調達)

第 62 条 情報システムセキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含める。

2 情報システムセキュリティ責任者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得る。また、調達仕様の内容を契約に含める。

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」4.2.1⑵、4.2.1⑶ に準拠するよう定めているものです。

**■ 細則 第 4 編 外部委託 第 2 章 クラウドサービス 第 2 節 クラウドサービスの利用**

(クラウドサービスの利用に係るセキュリティ要件の策定)

第 66 条 クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係る内容を確認する。

2 クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、前条各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定する。

(クラウドサービスを利用した情報システムの導入・構築時の対策)

第 67 条 クラウドサービス管理者は、第 65 条第 1 項で定めた運用規程を踏まえて、前条第 2 項において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずる。また、導入・構築時に実施状況を確認・記録する。

（中略）

3 クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備する。

(1) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(2) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(3) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

(クラウドサービスを利用した情報システムの運用・保守時の対策)

第 68 条 クラウドサービス管理者は、第 65 条第 2 項で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録する。

（中略）

3 クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。

(クラウドサービスを利用した情報システムの更改・廃棄時の対策)
第 69 条 クラウドサービス管理者は、第 65 条第 3 項で定めた運用規程を踏まえて、更改・廃棄時の必要な措置を講ずる。また、クラウドサービスの利用終了時に実施状況を確認・記録する。

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」4.2.2(2)、4.2.2(3)、4.2.2(4)、4.2.2(5) に準拠するよう定めているものです。

**■ 細則 第 4 編 外部委託 第 3 章 機器等の調達 第 1 節 機器等の調達**

(機器等の調達に係る運用規程の整備)
第 72 条 統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備する。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機構が確認できることを加える。
2 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備する。

※ 上記の規定は「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」4.3.1(1) に準拠するよう定めているものです。

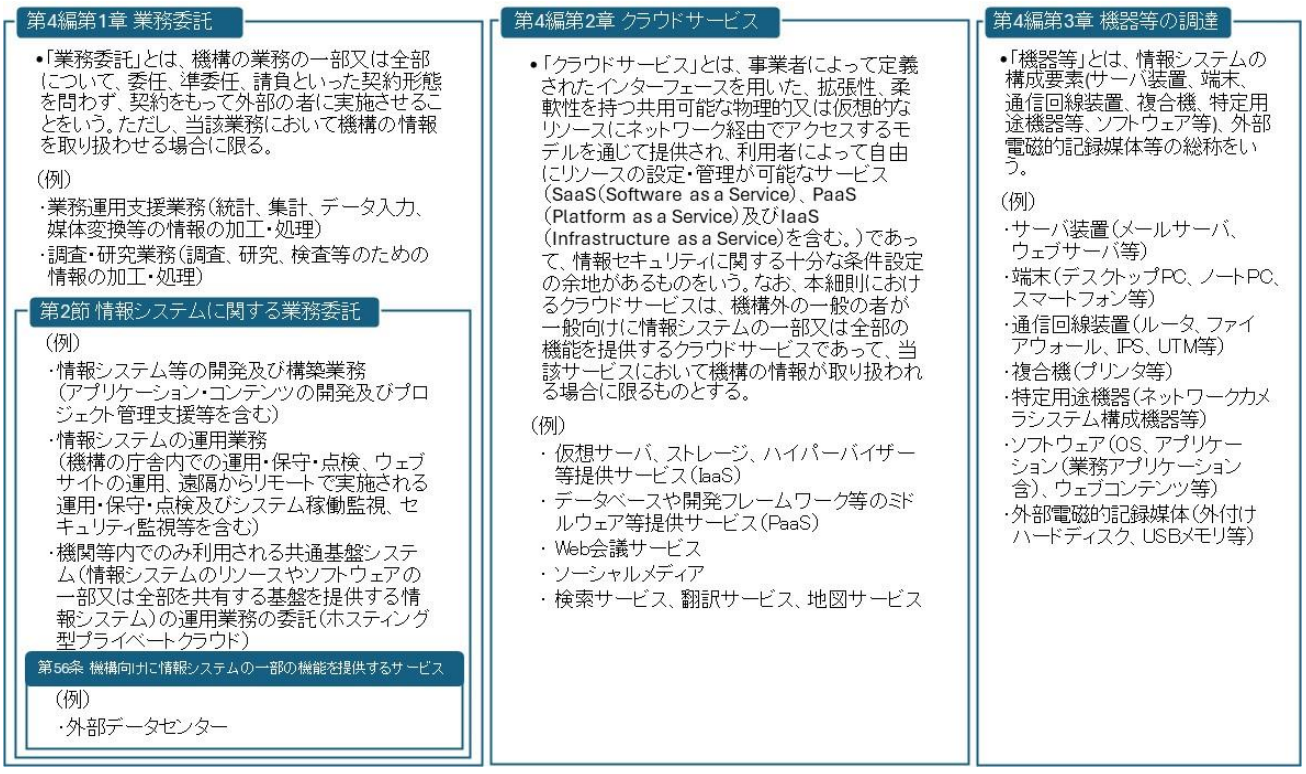


**図 3 JICA 細則 第 4 編に係る用語定義等**

## Appendix 3.3　個人情報の保護に関する実施細則における定め

### ■ 個人情報保護細則 第 7 章 保有個人情報等の取扱いに係る業務の委託等

(業務の委託等)

第 45 条 責任者は、次の各号に掲げる者が当該各号に定める業務を行う場合における保有個人情報等の取扱いに際し、第 15 条に定める保有個人情報等の安全管理が図られるよう、当該各号に掲げる者に対する必要かつ適切な監督を行う。

(1) 機構から保有個人情報等の取扱いの委託を受けた者及び当該委託を受けた業務

(2) 前号に掲げる者から前号が定める業務の委託（二以上の段階にわたる委託を含む。）を受けた者及び当該委託を受けた業務

(3) 前 2 号以外の法第 66 条第 2 項各号に掲げる者及び業務

2 責任者は、前項第 2 号に掲げる委託を認める場合には、当該業務を行う場合における保有個人情報等の安全管理が図られるよう、前項第 1 号に掲げる者に担保させるとともに、判断に必要な情報の提供を求め、その内容を確認した上で、当該委託の可否を判断する。

3 責任者は、個人情報の取扱いに係る業務を外部に委託（契約の形態・種類を問わず、行政機関等が他の者に個人情報の取扱いを行わせることをいう。個人情報の入力（本人からの取得を含む。）、編集、分析、出力等の処理を行うことを委託すること等が想定されるが、これらに限られない。）する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置（セキュリティ対策実施細則に基づく委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準や委託先の選定基準等の整備等）を講ずる。

4 責任者は、個人情報の取扱いに係る業務を外部に委託する場合には、契約書に、次の事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。

(1) 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務

(2) 再委託（再委託先が委託先の子会社（会社法（平成 17 年法律第 86 号）第 2 条第 1 項第 3 号に規定する子会社をいう。）である場合も含む。本項及び第 7 項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項（委託先との契約書に、再委託に際して再委託先に求める事項は、再委託先が子会社である場合も、同様に求めるべきことを明記すること。）

(3) 個人情報の複製等の制限に関する事項

(4) 個人情報の安全管理措置に関する事項

(5) 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

(6) 委託終了時における個人情報の消去及び媒体の返却に関する事項

(7) 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項（準拠法や裁判管轄について日本国内法令とすべきかについてもあらかじめ検討すること。）

(8) 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項（再委託先の監査等に関する事項を含む。）

5 保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

6 課等責任者は、保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年 1 回以上、原則として実地検査により確認する。

7 委託先において、保有個人情報等の取扱いに係る業務が再委託される場合には、委託先に第 1 項から第 4 項の措置を講じさせるとともに、再委託される業務に係る保有個人情報等の秘匿性等その内容に応じて、委託先を通じて又は機構自らが前項の措置を実施する。保有個人情報等の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

8 派遣先責任者(労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律(昭和 60 年法律第 88 条)第 41 条に規定する者をいう。)は、保有個人情報等の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等、個人情報の取扱いに関する事項を明記しなければならない。

9 保有個人情報等を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報等の秘匿性等その内容などを考慮し、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。

※ 上記の規定は「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」4.8.9 に準拠するよう定めているものです。

(個人番号関係事務の委託)

第 46 条 責任者は個人番号関係事務の全部又は一部を委託する場合には、前条の措置に加えて次の各号に掲げる措置についても講ずるものとする。

(1) 委託先において、番号法に基づき機構が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認する。

(2) 委託先において、機構が果たすべき安全管理措置と同等の措置が講じられているよう必要かつ適切な措置を行う。

(3) 委託先が当該業務を再委託する際には、委託する個人番号関係事務において取り扱う特定個人情報等の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。

※ 上記の規定は「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」第４－２－(1)を踏まえ定めているものです。

## Appendix 4　関連するガイドライン文書、研修資料等

本書に関連する政府決定等文書及びガイドライン・研修資料等の一覧を示します。なお、掲載しているリンク先情報（URL）は 2025 年 1 月時点のものとなります。

【内閣官房 内閣サイバーセキュリティセンター（NISC）関係重要文書】
（https://www.nisc.go.jp/policy/jyuyo-bunsho/index.html）

- サイバーセキュリティ戦略（閣議決定）
  https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf
- サイバーセキュリティ戦略（閣議決定）の概要
  https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf
- サイバーセキュリティ戦略（閣議決定）のパンフレット
  https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
- サイバーセキュリティ２０２４（年次計画・年次報告）
  https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf
- サイバーセキュリティ２０２４（年次計画・年次報告）の概要
  https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf

【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】
（https://www.nisc.go.jp/policy/group/general/kijun.html）

- 統一基準群の概要
  https://www.nisc.go.jp/pdf/policy/general/kijyungun-gaiyor5.pdf
- 政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）
  https://www.nisc.go.jp/pdf/policy/general/guider6.pdf
- 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）
  https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf
- 政府機関等のサイバーセキュリティ対策のための統一規範
  https://www.nisc.go.jp/pdf/policy/general/kihanr5.pdf
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル
  https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html
- 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書
  https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
- 統一基準群学習資料
  https://www.nisc.go.jp/pdf/policy/general/R0601_kijun_study.pdf
- 政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）のポイント
  https://www.nisc.go.jp/pdf/policy/general/rev_pointr6.pdf

- 統一基準群改定のポイント（令和５年度版）
  https://www.nisc.go.jp/pdf/policy/general/rev_pointr5.pdf

【個人情報保護等 法令・ガイドライン等】
（https://www.ppc.go.jp/personalinfo/legal/）

- 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）
  https://www.ppc.go.jp/files/pdf/241202_guidelines01.pdf
- 「個人情報の保護に関する法律についてのガイドライン」に関する Q&A
  https://www.ppc.go.jp/files/pdf/2412_APPI_QA.pdf
- 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）
  https://www.ppc.go.jp/files/pdf/241127_koutekibumon_guidelines.pdf
- 個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）
  https://www.ppc.go.jp/files/pdf/202412_koutekibumon_jimutaiou_guide.pdf
- 個人情報の保護に関する法律についてのＱ＆Ａ （行政機関等編）
  https://www.ppc.go.jp/files/pdf/202403_koutekibumon_qa.pdf
- 個人情報の研修資料・ヒヤリハットコーナー
  https://www.ppc.go.jp/personalinfo/hiyarihatto/
- 国の行政機関及び地方公共団体等向け研修資料等
  https://www.ppc.go.jp/personalinfo/kensyuushiryou_gyousei/

【特定個人情報の適正な取扱いに関するガイドライン】
（https://www.ppc.go.jp/legal/policy/）

- 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）
  https://www.ppc.go.jp/files/pdf/2405_my_number_guideline_jigyosha.pdf
- 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）
  https://www.ppc.go.jp/files/pdf/2405_my_number_guideline_gyousei.pdf
- 個人情報保護法第 58 条第１項各号に掲げる法人及び同条第２項各号に掲げる者における特定個人情報の適正な取扱いに関するガイドライン参照箇所
  https://www.ppc.go.jp/files/pdf/my_number_guideline_gyousei_kanmatsu2.pdf
- ガイドライン資料集
  https://www.ppc.go.jp/legal/policy/document/
- 研修資料等
  https://www.ppc.go.jp/legal/kensyuushiryou/

【個人情報保護に係る諸外国・地域の法制度】
（https://www.ppc.go.jp/enforcement/infoprovision/laws/）

- EU（外国制度）GDPR（General Data Protection Regulation：一般データ保護規則）
  https://www.ppc.go.jp/enforcement/infoprovision/EU/

【サイバーセキュリティ基本法、サプライチェーン・リスク対策、個人情報保護関連】
（https://www.nisc.go.jp/policy/group/kihon-2/policy.html）

- IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ
  https://www.nisc.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf
- 調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ
  https://www.nisc.go.jp/pdf/policy/kihon-2/ES_moushiawase.pdf

【ＩＳＭＡＰ - 政府情報システムのためのセキュリティ評価制度】
（https://www.ismap.go.jp/）

- ISMAP 概要
  https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005
- 制度紹介動画
  https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010008

【「ISO/IEC 15408」に基づく IT セキュリティ評価及び認証】

- IT セキュリティ評価及び認証
  https://www.meti.go.jp/policy/netsecurity/cc.html
- 評価認証制度（JISEC/ジェイアイセック）概要
  https://www.ipa.go.jp/security/jisec/about/jisec.html
- IT 製品の調達におけるセキュリティ要件リスト
  https://www.ipa.go.jp/security/it-product/gmcbt80000005uzp-att/cclistmetisec2018.pdf
- IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック
  https://www.ipa.go.jp/security/it-product/guidebook.html

【IoT 製品に対するセキュリティ適合性評価制度】

- IoT 製品に対するセキュリティ適合性評価制度構築方針
  https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
- セキュリティ要件適合評価及びラベリング制度（JC-STAR）
  https://www.ipa.go.jp/security/jc-star/index.html

【ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引】

- ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver2.0
  https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

【デジタル庁政策】

- デジタル社会の実現に向けた重点計画
  https://www.digital.go.jp/policies/priority-policy-program
- サイバーセキュリティ
  https://www.digital.go.jp/policies/security
- 国等の情報システムの統括・監理
  https://www.digital.go.jp/policies/development_management

- デジタル社会推進標準ガイドライン
  https://www.digital.go.jp/resources/standard_guidelines
  セキュリティに関するドキュメント
  https://www.digital.go.jp/resources/standard_guidelines#security