別紙１

個人番号関係事務の外部委託における

契約事務の取扱について

2016 年 1 月より社会保障、税、災害対策分野で番号制度（マイナンバー制度）が開始しました。事業者は、「行政手続き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。）に従い、個人番号（マイナンバー）及び個人番号をその内容に含む個人情報（以下「特定個人情報等」という。）を適正に取り扱うことが求められます。特に、番号法上の「個人番号関係事務の業務委託契約」に該当する契約では、発注者が受注者の行う安全管理措置に対する監督義務を負います。具体的には、特定個人情報等の保護に関する条項を含む契約の締結、業務委託機関の安全管理措置実施状況の確認および定期検査等、通常の業務委託契約にはない追加的な対応が求められます。

応札者および受注者に対応して頂く事項は、以下の通りです。

１。契約前の当機構による安全管理措置の確認

（１）当機構の安全管理措置について

当機構は、番号法において「個人番号関係事務の業務委託契約」に該当する契約について、当機構の安全管理措置と同等の措置が講じられるよう契約相手方の監督義務を果たすことが求められており、それに応ずるための対応をとる必要があります。つきましては、当機構の特定個人情報等の安全管理に関する基本方針（別添１）を確認の上、応札または受注後の契約事務をお願いします。

※尚、当機構は、（「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号）第２条第１項に規定する独立行政法人等をいう。）に該当する独立行政法人です。このため、当機構の業務において特定個人情報等の漏洩等の「番号法」違反の事案又は「番号法」違反のおそれのある事案が発覚した場合には、外務省や個人情報保護委員会への報告が必要となり、情報漏えいの事実が公表される可能性があります。

この対応は、当機構が管理責任を持つ「個人番号関係事務の業務委託

契約」にも適用されます。このため、機構との契約で特定個人情報等の漏洩などの事案が発生した場合は、受注者の名前を含めて公表される可能性があることを予めご理解下さい。

（２）当機構による応札者・契約交渉相手の安全管理措置の確認への協力依頼

上記１.（１）に示した当機構の安全管理措置に準拠し、応札者や契約交渉相手に於いても同等の安全管理措置が講じられているか否か、別添２「個人情報の安全管理措置に関する調査シート」を用いて確認します。手順は次の通りです。

ア　機構からの求めに応じ、別添２のリストに回答を記載・押印の上、提出して下さい。

イ　必要に応じて当機構からの電話等による追加ヒアリングを行いますので、ご協力をお願いいたします。

ウ　また、上記ア、イの調査を踏まえ、契約締結後には、安全管理措置に関する実地検査を行う予定ですので、依頼のあった際にはご協力をお願いいたします。

２。特定個人情報等の保護に関する条項を含む契約の締結

入札説明書第５の契約書（案）を参照下さい。特定個人情報などの保護については、第２３条の２を参照下さい。

３。契約締結後の対応

（１）特定個人情報等の管理責任者および担当者の確認

受注者の安全管理措置の実施体制に応じて、該当する契約に於ける次の担当者を打合簿にて確認します。

・保有個人情報の管理責任者と担当者
・特定個人情報等の管理責任者と担当者

打合せ簿の案は、別添３のとおりです。

（２）当機構業務主管部門による年一回以上の定期検査等への対応

「番号法」に対応した業務委託契約書の雛形にあるとおり、契約期間中、報告書の提出のタイミング等を目途に、年―回以上の安全管理措置の実施状況に関する定期検査を行います。

定期検査の方法としては、次の方法を想定しています。

・業務報告書に必要な報告内容を記載する。

・必要に応じて、電話等でのヒアリングまたは実地検査を行う。

報告内容としては、マイナンバーの収集・保管、廃棄等のアクセスログや、業務従事者への教育の実施回数等を確認します。

（３）契約終了時のマイナンバーの廃棄・削除証明の提出

契約終了時には、契約期間中に収集・利用・保管したマイナンバーに関するデーター式を、復元不可能な形で廃棄・削除し、その廃棄・削除証明を業務完了報告書に添付して提出して下さい。様式案は別添４のとおりです。

以上

別添１：特定個人情報等の安全管理に関する基本方針
別添２：個人情報の安全管理措置に関する調査シート
別添３：打合簿案（特定個人情報等の管理責任者および担当者の確認用）
別添４：廃棄・削除証明書案

特定個人情報等の安全管理に関する基本方針

1。特定個人情報等の保護に関する考え方

独立行政法人国際協力機構では、「行政手続における特定の個人を識別する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。）に定められた事務において特定個人情報等を取り扱う。番号法においては、「独立行政法人等の保有する個人情報の保護に関する法律」（平成 15 年法律第 59 号。以下「独立行政法人個人情報保護法」という。）に定められる措置の特例として、特定個人情報等の利用範囲を限定する等、より厳格な保護措置を定めていることから、管理体制及び管理規程、取扱規程等を整備し、職員等に遵守させる等の措置を講じ、適正に特定個人情報等を取り扱う。

2。特定個人情報等の保護方針

個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う全ての事務において、次のとおり特定個人情報等を適正に取り扱う。

（法令遵守）

①特定個人情報等の適正な取扱いに関する法令等（ｔ）を遵守する。

（注）法令等には次のものを含む。

- 番号法
- 独立行政法人個人情報保護法等関連法令
- 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・地方公共団体等編）（平成 26 年特定個人情報保護委員会告示第 6 号）
- 独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年 9 月 14 日付け総管情第 85 号総務省行政管理局長通知、一部改正平成 27 年 8 月 25 日総管管第 71 号）

(安全管理措置)

②特定個人情報等の漏えい、滅失及び毀損の防止その他の適切な管理のために必要な安全管理措置を講ずる。

(適正な収集・保管・利用・廃棄、目的外利用の禁止)

③特定個人情報等は、番号法に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内で適正に利用、収集・保管及び提供するとともに、不要となった特定個人情報等は速やかに廃棄する。また、目的外利用を防止するための措置を講ずる。

（委託・再委託）

④特定個人情報等を取り扱う事務の全部又は一部を委託する場合、委託先（再委託先を含む。）において、番号法に基づき機構自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行う。

(継続的改善)

⑤特定個人情報等の保護に関する取扱規程等及び安全管理措置を継続的に見直し、その改善に努める。

3.問合せ先

総務部総務課　電話 03-5226-8830

【様式3-1】　　**個人情報の安全管理措置に関する調査シート**

調査実施日	
調査対象	
調査実施場所	
調査者	

No.	分類	項目	判断基準	結果	備考
1	組織的安全管理措置	特定個人情報等の具体的な取扱いを定める規定を整備していますか。	・管理段階（取得・利用・保存・提供・削除/廃棄）毎の取扱方法、責任者・事務取扱担当者及びその任務等に関して規定されているか、確認する。 ・4つの安全管理措置（組織的、人的、物理的、技術的）が規定されているか、確認する。		
2		安全管理措置を講ずるための組織体制を整備していますか。	・管理責任者（或いは総括責任者）が任命されており、体制図等の書面に明記されているか、確認する。		
3		特定個人情報の取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における事務担当者を設置しているか。	・事務担当者が任命されており、役割が文書化されるなど明確化されているか、確認する。		
4		事務取扱担当者が取り扱う特定個人情報等の範囲は明確にされていますか。	・書面等により、当該業務で取り扱う特定個人情報等の範囲が明確に規定されているか、確認する。		
5		個人情報の漏えい等の事故が発生した場合又は、発生の可能性が高いと判断した場合の、代表者等への報告連絡体制は整備されていますか。	・連絡体制図、若しくは連絡先を書面等に明記しているか、確認する。		
6		特定個人情報の取扱状況について定期的に点検を実施していますか。	・定期点検の計画、実施状況、出来れば改善等を行った結果があれば、確認する。		
7	人的安全管理措置	新入社員等が入った場合、特定個人情報の取扱い等について教育等を実施していますか。	・資料などを作成しているか、受講者や講師名を含め、教育の記録を残しているか、確認する。		
8		特定個人情報等を取り扱う事務取扱担当者と誓約書を締結していますか。	・実際にこの件で誓約書を締結しているか、確認する。		
9	物理的安全管理措置	特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講じていますか。	・入退室の記録を取得しているか、記録が残っているか、確認する。 ※建物内への入退室記録、取扱区域への入退室記録、管理区域内への入退室記録、情報システム室等への入退室記録などの確認		
10			・部外者を識別するための措置を講じていいますか		
11			・持ち込み機器等の制限等の措置を講じているか、確認する。		
12			・部外者が入室する場合の立会い等の措置を講じているか、確認する		
13			・入室する権限を有する者を定めているか、確認する。		
14			・入室に係る認証機能の設置は設置されているか、確認する。		
15			・不正侵入に備えて、警報装置や監視装置の設置等の措置を講じているか、確認する。		
16			・離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置を禁止しているか、確認する。		
17		管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講じていますか。	・電子媒体又は書類等は、施錠キャビネットや書庫又は必要に応じてい耐火金庫に保管しているか、確認する。 ・情報機器に関しては、セキュリティワイヤー等により固定されているか、確認する。 ・上記の鍵の保管についても確認する。		
18			個人情報を含む文書の保管場所、利用場所を限定しているか、確認する。		
19			・深夜等、関係者不在時に、文書利用／保管場所の施錠を行っているか、確認する。		
20		電子媒体等に取扱いにおいて、情報の漏えい等の防止のために措置を講じていますか。	・データの暗号化、パスワードによる保護が実施されているか、確認する。		
21			・電磁的記録媒体の情報システム端末等への接続制限や一定数以上の個人情報をダウンロードする際には、警告等が表示されるなどの措置が実施されいるか、確認する。		
22		特定個人情報が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しないような措置、追跡可能な移送手段の利用等、安全な方策を講じていますか。	・データの暗号化、パスワードによる保護が実施されているか、確認する。該当する状況において、個人情報の持ち運び、パスワード設定／暗号化の措置をどのように行うか、担当者に手順をヒアリングする、手順書を閲覧する、実地にて操作状況を確認する等の手段により、判断する。 ・書類に関しては、封緘、目隠しシール等が使用されいるか、確認する。 ・持出記録等があるか、確認する。		
23			・特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための対策を行っているか、確認する。		

No.	分類	項目	判断基準	結果	備考
24		個人番号、特定個人情報ファイルの削除、機器及び電子媒体等の廃棄に際し、適切な措置を講じていますか。	・書類の廃棄の場合、復元不可能な手段（例：焼却、溶解等）が採用されているか、確認する。 廃棄するまでの書類や電子媒体の保管場所、保管方法について、取扱区域外に設置されていたり、誰でも持出可能な状態になっていないか、確認する。		※ 電子媒体はバックアップ先の媒体(DATテープ/外付けHDD等)についても確認の対象とする。
25			・個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存しているか、確認する。 （削除・廃棄を委託した場合、証明する記録等があるか、確認する。）		同上
26			・個人特定情報等を削除・廃棄したことを、責任ある立場の者が承認等を行っているか、確認する。 ・特定個人情報は保持期限前に削除・廃棄されていないことを確認する。 ・特定個人情報が、保持期限を過ぎてからも不必要に保管/保存されていないことを確認する。		同上
27	技術的安全管理措置	ID／パスワードによるユーザ認証等を行い、必要最低限の者のみ個人情報にアクセスできるようシステム上の制限を実施していますか。	・受託した個人情報を電子データにて保存する環境において、ID/パスワード等を使用してユーザ認証を行い、必要のない者がアクセスできないよう制限を行っているかどうか、システムの仕様を担当者にヒアリングする、実地にてユーザ認証の操作を調査することにより、判断する。		【ヒアリング内容の例】 １．システム上でアクセス可能なアカウント数 ２．１のアカウントを利用可能な人数 ３．OS上で情報にアクセス可能なアカウント数 ４．３のアカウントを利用可能な人数 ５．それぞれのパスワードの管理方法、変更等の規約
28		個人情報へのアクセス記録の取得を行っていますか。	・OS、データベース等において、個人情報へアクセスしたことについてのログ（アクセス対象、ユーザ名、アクセス時間等）を取得しているか、システムの仕様を担当者にヒアリングして判断する。		【ヒアリング内容の例】 １．取得可能なログの種類(例：OSのイベントログ、アプリのエラーログ) ２．(それぞれのログに関して)取得可能な情報(例：IPアドレス、端末名) ３．(それぞれのログに関して)保存期間
29			・不正な使用等がないか、ログのチェックを定期的に行っているか、確認する。		【ヒアリング内容の例】 １．チェックの周期 ２．チェックの観点
30		個人情報を格納しているシステム上にてウィルスチェックを行っていますか。	・ウィルスチェックを行っているか、定義ファイルは更新されているか、担当者に対するシステム仕様のヒアリング及び仕様書等による説明を受けて、判断する。		
31		外部からの不正アクセスから情報システムを保護する仕組みを導入し、運用していますか。	・不正アクセスへの対策として実施している内容について、担当者に対するシステム仕様のヒアリング及び仕様書等による説明を受けて、判断する。 ・また、ログの分析を定期的に実施しているか、確認する。		※ パブリッククラウド基盤等、複数の利用者で筐体、ネットワーク等を共有する場合は、他の利用者がマルウェア等の被害にあった場合の影響について把握し、その回避策について確認すること。
32		情報にアクセス可能な端末について、作業者の離席時におけるログオフ等、第三者に端末を使用されないような運用を行っているか。	離席時における対応手段を担当者にヒアリングする。また、ログオフによる運用を手順書等に明記しているか、若しくは実地にてスクリーンセーバーロックを設定しているか調査し、どちらかの対応を行っていればよいこととする。		
33		情報システム等の脆弱性への対応を行っていますか。	・脆弱性がある場合、それを管理し、対応策を実施しているか、確認する。		
34	再委託（機構から許可を得て個人情報を取り扱う業務の再委託を実施している場合）	再委託先における責任者等の管理体制は明確になっていますか。	再委託先の管理体制について、体制図等で明示されているか確認する。		
35		再委託先との契約において、以下の事項は契約に含まれていますか。	契約書の内容について、確認を行う。 ・秘密保持の義務 ・再々委託の制限または条件に関する事項 ・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 ・個人情報の複製等の制限に関する事項 ・再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 ・各項目に違反した場合における契約の解除権 ・再委託先における個人情報の管理状況に関する委託先の検査権		
最終評価					

最終評価：
1.問題なし
（チェック項目にすべて「A.実施」が記入されている場合）
2.要改善
（チェック項目に「B.一部のみ実施」、「C.未実施」が記入されている場合）
⇒改善を依頼することになりますので、その旨を備考欄に記載する。

別紙１の別添３

打　合　簿（案）

平成〇〇年〇〇月〇〇日
監督職員　　国際　太郎　⑩
業務主任者　　協力　一郎　⑩

件名　△△△△△△△△△△△△△に係る業務

打合項目	打合内容及び結果
保有個人情報および特定個人情報等の管理責任者と担当者の関係について	監督職員と業務主任者は、契約書第 21 条（個人情報保護）第一項（３）および第 22 条（特定個人情報保護）第１項（３）において、別途文書にて定めるとした責任者および担当者を次のとおり確認した。 第 21 条（個人情報保護）　・管理責任者：　・担当者：　第 22 条（特定個人情報保護）　・管理責任者：　・担当者： 以上
	【解説】　個人隋報保護並びに特定個人隋報保護の管理責任者、担当者が兼務の場合は、その様に記載して下さい

別紙１の別添４

独立行政法人国際協力機構
契約担当役理事

廃棄・削除証明書（案）

株式会社〇〇
代表取締役　〇〇
(公印)

以下のとおり特定個人情報を廃棄・削除しましたので、証明します。

処理(〇をつける)	廃棄・削除
廃棄または削除の方法	
処理日	
特記事項|	

証明欄:20●●年　月　日

１特定個人情報の削除･廃棄を委託した場合は、委託先から本紙と同様の証明書を受領の上、写しを添付して特記事項にその旨を記載下さい。