

受託事業者における個人情報の漏えい等の防止を図るための取組を推進するための鳥取県個人情報・死者情報保護事務取扱要綱に係る FAQ

安全管理措置に係る報告書兼届出書について

問1 どのような受託者がこの報告兼届出書を提出しなければならないのか。

答1 特記仕様書の交付があった受託者に限られます。契約書等に特記事項が付されているだけでは該当しません。

問2 「安全管理措置に係る報告書兼届出書」の記載例はあるのか。

答2 インターネット（鳥取県公式ウェブサイト「とりネット」）で公表しています。
（「県民課」→「鳥取県庁の業務委託における個人情報等の保護」
URL：<https://www.pref.tottori.lg.jp/321755.htm>）

問3 「安全管理措置に係る報告書兼届出書」の記載留意事項について

答3 「安全管理措置に係る報告書兼届出書記載例」の赤字吹き出しコメントに留意の上、加えて、次の点にも留意してください。

「4 業務に係る緊急連絡先」

電話番号は、3の責任者等と容易かつ円滑に業務連絡を取ることができる電話番号を記載すること。

電子メールアドレスは、3の責任者等と容易かつ円滑に業務連絡を取ることができ、かつ個人情報その他の機微情報に含む記載についての送受信に用いることが受託者において許容されているものを記載すること。

いずれも受託者側の緊急連絡窓口を一本化するためのものでもあること。

「5 業務に係る従事者（責任者を含む。）の人数」

ここにいう従事者とは、業務に係る**個人情報の取扱いに従事**する者をいう。

受託事業者に本県が行うべき個人情報取扱事務を代行させるなど**本県の保有（管理責任）が及ぶべき個人情報を取り扱わせることを契約の主たる目的とする**ときは、人数も幅広となる公算が大である。

これに対し、事業執行のための緊急連絡網として本県職員又は第三者の名簿を共有するときなど、**契約の従たる目的として本県の保有（管理責任）が及ぶ個人情報を現に取り扱わせることとなる**ときは、人数は（たとえば管理職と事務担当者のみが該当するなど）少数とすることが見込まれる。

「6 個人情報保護関連資格等の有無」

該当する資格等を備えていない場合には、空欄のままとすること。

① プライバシーマーク（Pマーク）

詳細については、一般財団法人日本情報経済社会推進協会（JIPDEC）の公式ウェブサイト参照すること。

<https://privacymark.jp/>

② I S M S

詳細については、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）の公式ウェブサイト参照すること。

<https://isms.jp/>

③ その他の資格

①・②に掲げるものの外、個人情報保護法に基づき国の認定を受けた「認定個人情報保護団体」が個人情報の保護体制に対する第三者認証制度を設けていることがある。

詳細については、個人情報保護委員会の公式ウェブサイト参照すること。

<https://www.ppc.go.jp/personalinfo/nintei/list/>

④ 個人情報保護関係の損害保険に加入

名称を問わず、事業活動に関し個人情報漏えい等が発生した場合の初期対応費用や損害賠償責任に係る費用を補償する保険をいう。

「7 個人情報保護に関する社内規程等の有無」

業務において個人情報を取り扱う事業者において、特に令和4年4月1日の改正個人情報保護法の施行後に、何ら備えていないことは考え難いことではあるものの、何ら該当がない場合には「規程なし」を選択すること。

「8 個人情報保護に関する研修の実施」

受託者において独自の研修や教育を実施していない場合には、記載例のとおりとすることを推奨する。

「9 個人情報保護に係る内部点検・検査・監査の方法等」

受託者において整備している内部点検等の体制のあらましを記載すること。

業務において個人情報を取り扱う事業者において、特に令和4年4月1日の改正個人情報保護法の施行後に、何ら整備していないことは考え難いことではあるものの、何ら該当がない場合には「特になし」と記載すること。

「10 業務において利用する個人情報を取り扱う作業場所等の管理体制」

① 「(1) 作業場所の所在地」

本県からの郵便等の送付先としても利用するので、適確に記載すること。

② 「(6) 個人情報の送付方法」

記載例のとおりとすることを推奨する。

③ 「(7) 個人情報の廃棄方法」

記載例のとおりとすることを推奨する。

「11 業務において利用する個人情報の電算処理における保護対策」

① 「(1)業務において利用する個人情報に係る連絡のために用いる電子メールアドレス」

3の責任者又は5の従事者と容易かつ円滑に業務連絡を取ることができ、かつ個人情報その他の機微情報の記載についての送受信に用いることが受託者において許容されているものを記載すること。

受託者側の窓口を一本化するためのものであること。

「4 業務に係る緊急連絡先」と共通のものでも差し支えない。

② 「(2)作業を行う機器」

「限定していない」という選択肢は通常想定し難いものであること。

③ 「(3)外部との接続」

「通信の暗号化」を「していない」という選択肢は通常想定し難いものであること
(フリーWiFiを経由するような通信環境しか考えられない。)

④ 「(4) アクセス制限」

「ID・パスワード付与によるアクセス制限を実施していない」という選択肢は通常想定し難いものであること。

⑤ 「(5) 不正アクセスを検知するシステムの有無」

「なし」という選択肢は通常想定し難いものであること。

たとえばWindowsに標準搭載されている「Windows Defender」のみを有効としている場合には、その旨の記載とともに「あり」を選択すること。

⑥ 「(6) マルウェアを検知するシステムの有無」

「なし」という選択肢は通常想定し難いものであること。

たとえばWindowsに標準搭載されている「Windows Defender」のみを有効としている場合には、その旨の記載とともに「あり」を選択すること。

⑦ 「(7) OS・ソフトウェアの更新」

たとえば受託者において管理者や責任者を設けて、事業所内のWindowsのアップデートを一括管理しているような場合には、その旨の記載とともに「その他」を選択すること。

⑧ 「(9) 停電時のデータ消去防止対策」

「なし」という選択肢は通常想定し難いものであること。

たとえばノートパソコンにバッテリーを標準装備しているような場合には、その旨の記載とともに「その他」を選択すること。

⑨ 「(10) 外国における個人情報の取扱いの有無」

業務のために用いる個人情報を含むファイルをクラウドサービスに保存しているだけでなく、当該クラウド上で編集作業等も行うような場合には、「外国のサーバ上で個人情報が保存されており、外国のサーバ上で保存以外の個人情報の取扱いがある」を選択すること。この場合には、「① 個人情報の取扱いがある外国の名称」及び「② 当該外国における個人情報の制度・保護措置等」の付記が必要となるので、次の情報等を参考にしながら適宜付記を行うこと。

個人情報保護委員会公式ウェブサイト（諸外国・地域の法制度）

<https://www.ppc.go.jp/enforcement/infoprovision/laws/>

(参考) 外国のサーバを利用しているクラウドサービスの例

○Google Cloud（日本のユーザーへの法定表示事項）

<https://policies.google.com/privacy/additional>

○Microsoft Azure（プライバシーステートメント）

<https://www.microsoft.com/ja-jp/privacy/privacystatement>

○Amazon Web Services（日本のデータプライバシー）

<https://aws.amazon.com/jp/compliance/japan-data-privacy/>

なお、全体に共通する留意事項として、全ての項目が埋まらないといけないということではなく、受託者における安全管理措置体制の現況を先ずはありのまま把握させていただくためのものです。

【お問合せ】

- 個人情報・死者情報の取扱いに係る特記事項（特記仕様書）については
鳥取県 地域社会振興部 県民課 情報公開担当（電話 0857-26-7753）まで
- 個別の契約内容については、各委託事業の担当課まで