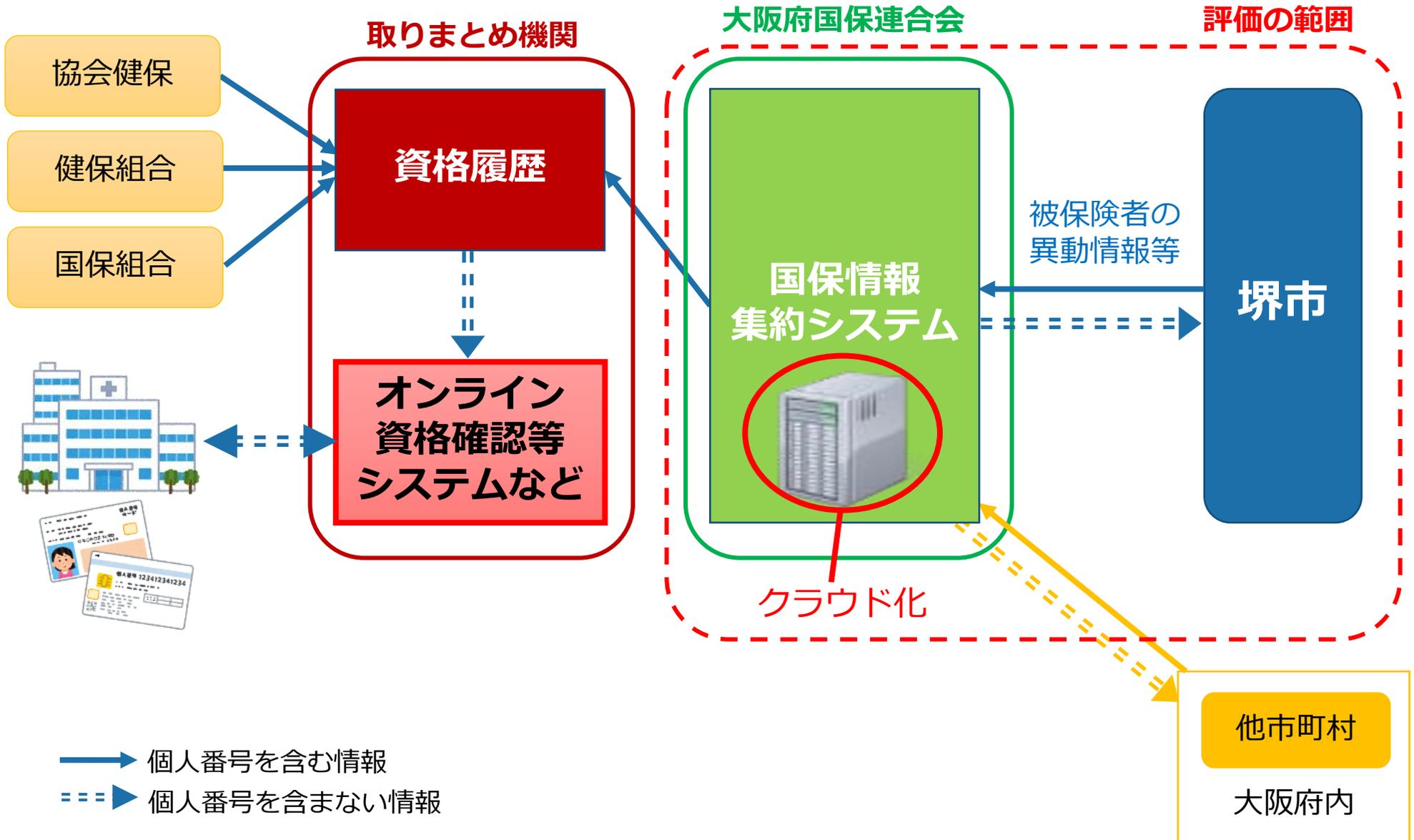


# 国保情報集約システムのクラウド化（イメージ）



事 務 連 絡  
令和 4 年 12 月 14 日

都道府県民生主管部（局）  
国民健康保険主管課（部）御中

厚生労働省保険局国民健康保険課

市町村国保が実施する特定個人情報保護評価(PIA)および個人情報ファイル簿の  
テンプレートの送付について

国民健康保険制度の運営につきましては、平素より格別の御高配を賜り、厚く御礼  
申し上げます。

さて、令和 6 年 4 月に予定している国保情報集約システムの機器更改についてはク  
ラウド環境において実施されることに伴い、市町村国保の特定個人情報保護評価（以  
下「P I A」という。）の再実施が必要となるところです。

また、令和 5 年 4 月から施行される個人情報保護法改正において、個人情報ファイ  
ル簿の作成、公表が義務づけられております。

今般、各市町村国保における P I A 及び個人情報ファイル簿の作成の一助として、  
特定個人情報保護評価書に機器更改を反映させた P I A 及び国保情報集約関連情報フ  
ァイルにおける個人情報ファイル簿のテンプレートを作成いたしましたので、参考と  
して提供いたします。

## 記

### 1 概要

別添「PIA テンプレートおよび個人情報ファイル簿の概要」を参照。

### 1 送付資料

- （1）【別添 1】市町村事務処理標準システムテンプレート（全項目評価書）
- （2）【別添 2】市町村国保システムテンプレート（全項目評価書）
- （3）【別添 3】国保情報集約システム\_個人情報ファイル簿テンプレート

連絡先：

厚生労働省保険局国民健康保険課 寺本・佐藤・雨宮

電話：03 (5253) 1111（内線 3265・3264）

Mail：[kokuho@mhlw.go.jp](mailto:kokuho@mhlw.go.jp)

# 市町村国保が実施するPIAテンプレート および個人情報ファイル簿について

---

# 1. PIAテンプレート

---

- 令和3年個人情報保護委員会告示第1号により、「第9 特定個人情報保護評価の評価項目」において、「技術の進歩に伴うクラウドサービス等の新たなサービス、開発手法等を導入する場合には、当該サービス、開発手法等の特性を考慮した上で、適切な安全管理措置を講ずるものとする。」と明記されました。
- 今般、国保情報集約システムをクラウドに移行するに伴い、クラウドサービス事業者に求めるセキュリティ対策等について加筆したうえで、PIAの再実施と再委託に関する許諾が全ての市町村で必要となります。
- この度は、厚生労働省保険局国民健康保険課より、PIAの概要について次ページ以降にお示しするとともに、「PIAテンプレート」を提供します。
- なお、国保情報集約システムにおける運用テストの開始前（令和6年1月）までに全市町村がPIAを実施する必要があります。

# 1. PIAテンプレート

## ○ 概要

令和3年個人情報保護委員会告示第1号により、以下表の内容が明記されました。

これにあわせて「特定個人情報保護評価指針の解説」が更新され、

- クラウドサービスに関する定義
- クラウドサービスを利用する場合及びアジャイル型開発を採用する場合の特定個人情報保護評価の実施時期
- クラウドサービスの種類に対応したリスク識別、リスク評価、リスク対策
- クラウド環境への移行の際におけるリスク識別、リスク評価、リスク対策
- クラウドサービス事業者の情報セキュリティについて

に関する解説が記載されました。

「令和3年個人情報保護委員会告示第1号」

[https://www.ppc.go.jp/files/pdf/hogohyoka\\_shishin\\_shinkyuu.pdf](https://www.ppc.go.jp/files/pdf/hogohyoka_shishin_shinkyuu.pdf)

特定個人情報保護評価指針(令和3年個人情報保護委員会告示第1号)(抄)

| 改正後  | 改正前   |
|--|---|
| <p>第9 特定個人情報保護評価の評価項目</p> <p>1 基本的な考え方</p> <p>特定個人情報保護評価を実施するに当たって、評価実施機関は、特定個人情報ファイルを取り扱う事務の特性を明らかにした上で、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクについて認識又は分析し、このようなリスクを軽減するための適切な措置を講じていることを確認の上、特定個人情報保護評価書において宣言するものとする。</p> <p>評価実施機関は、リスクを軽減するための措置を検討する際には、特定個人情報の安全管理に関する基本方針、特定個人情報の取扱規程等を策定することが望ましい。また、リスクを軽減するための措置には、物理的安全管理措置、技術的安全管理措置、組織的安全管理措置及び人的安全管理措置があり、評価実施機関は、基本方針、取扱規程等を踏まえ、評価実施機関の規模及び事務の特性に応じた適切な措置を講ずるものとする。</p> <p>なお、技術の進歩に伴うクラウドサービス等の新たなサービス、開発手法等を導入する場合には、当該サービス、開発手法等の特性を考慮した上で、適切な安全管理措置を講ずるものとする。</p> <p>2 (略)</p> | <p>第9 特定個人情報保護評価の評価項目</p> <p>1 基本的な考え方</p> <p>特定個人情報保護評価を実施するに当たって、評価実施機関は、特定個人情報ファイルを取り扱う事務の特性を明らかにした上で、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクについて認識又は分析し、このようなリスクを軽減するための適切な措置を講じていることを確認の上、特定個人情報保護評価書において宣言するものとする。</p> <p>2 (略)</p> |

# 1. PIAテンプレート

## I . 「特定個人情報保護評価指針の解説」の更新について

### ○ クラウドサービスに関する定義（1/2）

クラウドサービスとは、「事業者等によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」と定義されました。

「特定個人情報保護評価指針の解説」  
[https://www.ppc.go.jp/files/pdf/kaisetsu\\_shishin.pdf](https://www.ppc.go.jp/files/pdf/kaisetsu_shishin.pdf)

特定個人情報保護評価指針の解説(抄)

#### 第2 定義

(解説)

番号法、規則及びこの指針において規定されている主な定義・用語は、次のとおりです。

| 用語       | 定義   |
|----------|--|
| クラウドサービス | 事業者等によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの |

# 1. PIAテンプレート

## I . 「特定個人情報保護評価指針の解説」の更新について

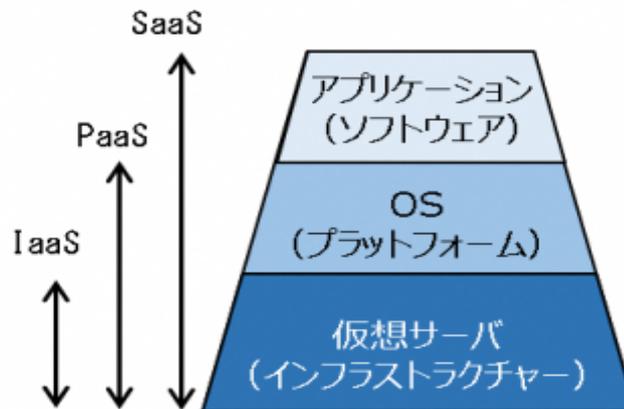
### ○ クラウドサービスに関する定義 (2/2)

クラウドサービスには、クラウドサービス事業者とクラウドサービス利用者の役割分担により、IaaS、PaaS、SaaSの3種に分類されます。

システムの階層を3層で捉えた場合、1段目までクラウドサービス事業者任せるのがIaaS、2段目まで任せのがPaaS、3段目まで任せのがSaaSということになり、クラウドサービスの種類によって、クラウドサービス事業者の構築・管理の範囲が異なります。

特定個人情報保護評価指針の解説(抄)

システムの階層とクラウドサービス事業者任せの範囲



1. クラウドサービス事業者とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいいます。
2. IaaS(Infrastructure as a Service)とは、利用者に、CPU機能、ストレージ、ネットワークその他の基礎的な情報システムの構築に係るリソースが提供されるものをいいます。利用者は、そのリソース上にOSや任意機能(情報セキュリティ機能を含む。)を構築することが可能です。
3. PaaS(Platform as a Service)とは、IaaSのサービスに加えて、OS、基本的機能、開発環境や運用管理環境等もサービスとして提供されるものをいいます。利用者は、基本機能等を組み合わせることにより情報システムを構築することが可能です。
4. SaaS(Software as a Service)とは、利用者に特定の業務系のアプリケーション、コミュニケーション等の機能がサービスとして提供されるものをいいます。具体的には、政府外においては、安否確認、ストレスチェック等の業務系のサービス、メールサービスやファイル保管等のコミュニケーション系のサービス等があります。政府内においては、府省共通システムによって提供される諸機能や、政府共通プラットフォーム上で提供されるコミュニケーション系のサービス・業務系のサービスが該当します。

# 1. PIAテンプレート

## I . 「特定個人情報保護評価指針の解説」の更新について

### ○ 特定個人情報保護評価の実施時期

特定個人情報ファイルを取り扱うシステムを改修し、クラウドサービスを利用する場合にも、特定個人情報保護評価の実施時期については、基本的にはこれまでの考え方と変わりません(次期環境において本番データを利用する(テスト等も含む)までに実施する必要がある)。そのため、本番データを移行する前日までにPIAを終えておく必要があります。

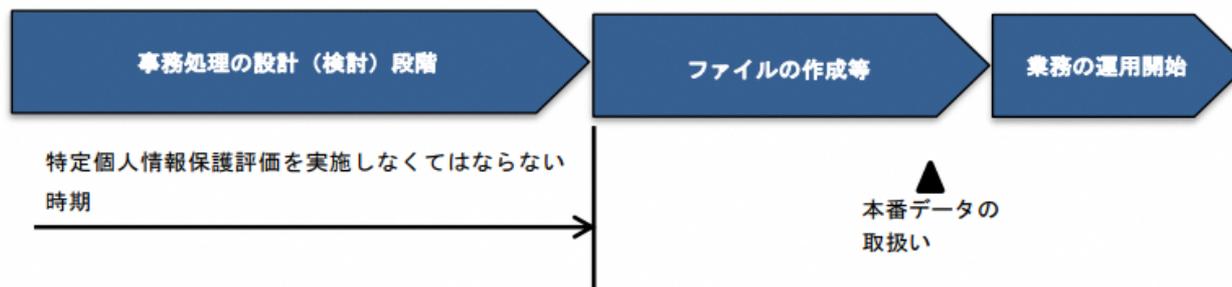
特定個人情報保護評価指針の解説(抄)

- クラウドサービス利用者側でアプリケーション等を構築・管理できるIaaSのクラウドサービスへの移行する場合には、例えば、クラウド環境への移行にあたり、クラウドサービス利用者が既存システムのアプリケーション等について、特定個人情報の取扱いに関する機能の改修を行い移行する場合と改修を行わず移行する場合が考えられます。
- 特定個人情報の取扱いに関する機能の改修を行い移行する場合は、システム開発を行いますので、「指針第6の2(2)ア システム開発を伴う場合の実施時期」に従い、プログラミング開始前の適切な時期に特定個人情報保護評価を行う必要があります。
- 特定個人情報の取扱いに関する機能の改修を行わず移行する場合は、「指針第6の2(2)イ システム開発を伴わない又はその他の電子ファイルを保有する場合の実施時期」に従って適切な時期に特定個人情報保護評価を行う必要があります。

(中略)

<その他の電子ファイルを保有する場合の実施時期>

事務処理の検討段階(特定個人情報ファイルの保有前)で特定個人情報保護評価を実施する必要があります。



# 1. PIAテンプレート

## I . 「特定個人情報保護評価指針の解説」の更新について

### ○ クラウドサービスを利用する場合に特定個人情報保護評価で考慮すべきこと

クラウドサービス事業者が委託業務の範囲内で個人番号をその内容に含む電子データを取り扱わない場合は、そもそも、個人番号関係事務又は個人番号利用事務の全部又は一部の委託を受けたとみることはできません。

そのため、番号法上の委託には該当しませんが、その場合は、契約によって当該事業者が個人番号をその内容に含む電子データを取り扱わない旨が定められており、適切にアクセス制御を行う等の措置が講じられていることを確認し、必要に応じて、その内容を特定個人情報保護評価書に記載します。

特定個人情報保護評価指針の解説(抄)

一般的に、クラウドサービス事業者への委託については、番号法の委託に該当するか否かという点で特定個人情報保護評価書に記載が必要なリスク対策が異なります。また、番号法の委託に該当するか否かは、クラウドサービス事業者が当該契約内容を履行するに当たって個人番号をその内容に含む電子データを取り扱うかどうかが基準となります。

例えば、クラウドサービス事業者が提供するIaaSを利用し、当該事業者が委託業務の範囲内で個人番号をその内容に含む電子データを取り扱わない場合は、そもそも、個人番号関係事務又は個人番号利用事務の全部又は一部の委託を受けたとみることはできないため、番号法上の委託には該当しません。

ただし、契約によって当該事業者が個人番号をその内容に含む電子データを取り扱わない旨が定められており、適切にアクセス制御を行う等の措置が講じられていることを確認し、必要に応じて、その内容を特定個人情報保護評価書に記載することが考えられます。

また、クラウドサービス事業者が提供するPaaS、SaaSを利用する場合には、当該事業者がアプリケーションやOS等の保守サービスもクラウドサービスの一環として行うことが考えられます。この場合、サービス内容の全部又は一部として個人番号をその内容に含む電子データを取り扱う場合には、個人番号利用事務又は個人番号関係事務の一部の委託に該当します。そのため、委託内容に対応したリスクを識別・評価し、リスクを軽減させるために講ずる措置を特定個人情報保護評価書に記載する必要があると考えられます。

〔クラウドサービス事業者が保守サービスの中で個人番号を取り扱う典型的な例〕

- ・ 個人番号を用いて情報システムの不具合を再現させ検証する場合
- ・ 個人番号をキーワードとして情報を抽出する場合

---

# 1. PIAテンプレート

---

## I . 「特定個人情報保護評価指針の解説」の更新について

○ クラウドサービス環境への移行に関して特定個人情報保護評価で考慮すべきこと

また、クラウド環境への移行の際に、既存のシステム環境から特定個人情報ファイルを抽出し、クラウド環境へデータを移し替える作業や、既存のシステム環境に保管されていた特定個人情報の消去、機器の廃棄に係るリスクを軽減させるために講じる措置を特定個人情報保護評価書に記載します。

特定個人情報保護評価指針の解説(抄)

### 【その他】

- クラウドサービスの種類がIaaS、PaaS、SaaSのどの分類であっても、オンプレミス環境にある既存システムからクラウド環境に移行し、特定個人情報ファイルを取り扱うシステム等の場所が変わる場合、従来、職員が業務で利用していたパソコン等の操作端末からクラウドサービスに存在するシステムへ接続する通信経路やアクセス制御等に変更が生じる可能性があります。それらの変更に対応したリスクを識別・評価し、リスクを軽減させるために講ずる措置を特定個人情報保護評価書に記載する必要があります。
- また、クラウド環境への移行の際に、既存のシステム環境から特定個人情報ファイルを抽出し、クラウド環境へデータを移し替える作業や、既存のシステム環境に保管されていた特定個人情報の消去、機器の廃棄に係るリスクについても、漏えい、滅失等が起こらないように特定個人情報保護評価を実施しているか注意が必要です。

# 1. PIAテンプレート

## I . 「特定個人情報保護評価指針の解説」の更新について

### ○ クラウドサービス事業者の情報セキュリティについて

クラウドサービスの選定時において、適切に情報セキュリティが確保されているサービスを利用することが重要となります。また、特定個人情報ファイルの保管等については、各クラウドサービスが提供する監査報告書を利用して把握すること等が必要になります。

特定個人情報保護評価指針の解説(抄)

#### 【クラウドサービスの選定における留意事項】

- 行政機関においては、「政府情報システムにおけるクラウドサービス利用に係る基本方針(デジタル社会推進会議幹事会決定)」の要件を満たすクラウドサービスの選定、「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からのクラウドサービスの選定を行う等、サービスの選定時において、適切に情報セキュリティが確保されているサービスを利用することが重要です。
- 行政機関以外の評価実施機関においても、「政府情報システムにおけるクラウドサービス利用に係る基本方針」、「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、「地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省)」等を参考に、行政機関同様に情報セキュリティが確保されているサービスを適切な選定プロセスを経て、利用する必要があります。

#### 【クラウドサービス事業者の情報セキュリティの管理体制の把握】

- クラウドサービス事業者の特定個人情報ファイルを保管するサーバ設置場所への入退室管理等の物理的対策、特定個人情報ファイルの廃棄・消去の実態等について、直接、委託元が詳細に把握することは困難だと思われます。そのため、第三者による認証や各クラウドサービスが提供する監査報告書を利用し把握することが考えられます。
- 特定個人情報保護評価書のリスク対策等の記載においては、クラウドサービスを選定する際の基準を記載し、基準に合致したものを利用すること、また、特定個人情報の取扱いの実態については、各クラウドサービスが提供する監査報告書等のレポートを利用し、実態の把握に努める等、リスク対策を担保するために実施する内容を記載することが望まれます。

# 1. PIAテンプレート

## Ⅱ . 「国保情報集約システム」のクラウド化に伴うPIAについて

### ○特定個人情報保護評価書テンプレートの前提条件

「国保情報集約システム」のクラウド化に関する特定個人情報保護評価書の記載において、前提事項(契約と位置関係、その他)について以下に記載します。

#### 【契約と位置関係の整理】

中間サーバーにおける契約事例を基に想定した。

(実際には今後、国保中央会にて検討のうえ、示されるものである予定)

#### ○ クラウドサービスを提供する事業者：国保中央会からクラウド事業者へ委託



この一連の委託は特定個人情報の委託に該当しない想定(委託事項5のクラウド事業者)。

#### ○ クラウドサービスを用いて情報システムを開発・運用する事業者：国保中央会(集約機関)から事業者へ委託

国保中央会(集約機関)は、標準システムに係るアプリケーション保守業務(アプリケーション改修、データパッチ実施等及びシステム運用事務バックアップ取得、システム障害等発生時のデータ復旧等)を行う



この一連の委託は特定個人情報の委託に該当しない(委託事項5)。

#### ○ システム運用者：国保連から運用事業者へ委託



この一連の委託は特定個人情報の委託に該当する。

この委託に関しては、従来から変更がない(委託事項1)

# 1. PIAテンプレート

## Ⅱ . 「国保情報集約システム」のクラウド化に伴うPIAについて

### 【その他の前提事項】

- クラウド事業者が提供するクラウドサービスは、クラウド事業者が提供するPaaSを想定。
- クラウド事業者を選定する際の調達要件として、当該クラウドサービスが政府情報システムのためのセキュリティ評価制度に基づくクラウドサービスリストに掲載されている事業者であることを想定。
- クラウドサービスを提供する事業者とは、契約条項によって事業者が個人番号をその内容に含む電子データを取り扱わない旨を定め、適切にアクセス制御を行うこととしており、番号法上の特定個人情報の委託関係にならない想定。
- クラウドサービスを用いて情報システムを開発・運用する集約機関(国保中央会)とは、契約条項によって事業者が個人番号をその内容に含む電子データを取り扱わない旨を定め、適切にアクセス制御を行うこととしており、番号法上の特定個人情報の委託関係にならない想定。
- クラウド化に伴い、従来の操作端末からクラウドサービスに存在するシステムへ接続する通信経路やアクセス制御等に関しては、集約システムの設置場所が変わるため通信サービスに関する契約変更は生じる可能性があるが、通信に求めるセキュリティレベルは変更せず、アクセス制御に関しても変更しない想定。

# 1. PIAテンプレート

## Ⅱ . 「国保情報集約システム」のクラウド化に伴うPIAについて

### 【その他の前提事項】(つづき)

- クラウド環境への移行の際に、クラウド環境へデータを移し替える作業や、既存システム環境に保管されていた特定個人情報の消去、機器の廃棄等については、市町村は(運用事業者以外への)委託は行わないという想定。
- クラウド環境への移行の際に、クラウド環境へデータを移し替える作業や、既存システム環境に保管されていた特定個人情報の消去、機器の廃棄に係るリスクについても漏えい、滅失等が起こらないように対策を講じ、評価書に記載したため、移行完了後に再度、当該記載を消す必要があるが、特定個人情報保護評価指針では、「個人のプライバシー等の権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更又は当該リスクを明らかに軽減させる変更は重要な変更には当たらないものとする。」と定義されているため、重要な変更には該当しないと考えられる、との見解を個人情報保護委員会から得ている。
- なお、令和5年4月1日で、市町村の個人情報保護条例を廃止するため、個人情報保護法の罰則等を設けているのは国であり、評価実施機関ではなくなるため、条例よる罰則や目的外利用の禁止規定に関する記載は削除する。

# 1. PIAテンプレート

## 【変更のポイント】

### ○市町村事務処理標準システム

・現時点までの番号法の条文ズレを見直した。

・公金受取口座登録制度が開始されることで、同口座情報に関して情報提供ネットワークシステムを利用し、デジタル庁の公的給付支給等口座登録簿の副本情報を照会することが必要になり、番号法別表第2の121項が根拠となるため、「121」を追記した。

・国保総合(国保集約)システムがクラウドサービス事業者に求めるセキュリティ要求について、医療保険者中間サーバー、後期高齢者医療広域連合標準システムの前例に倣って記載をした。

・オンプレ環境からクラウド環境への特定個人情報の移行の際のリスク対策が必要となることから記載をした。

・デジタル社会形成整備法第51条による個人情報保護法の改正に係る部分(地方関係への同法適用)の施行期日である令和5年4月1日からは、滅失又は毀損の防止等に関する安全確保の措置を義務付けするのは国になるため削除した。

・デジタル社会形成整備法第51条による個人情報保護法の改正に係る部分(地方関係への同法適用)の施行期日である令和5年4月1日からは、個人情報ファイル簿の公開が必須となることから記載をした。

# 1. PIAテンプレート

## 【変更のポイント】

### ○市町村国保システム

・国保総合(国保集約)システムがクラウドサービス事業者に求めるセキュリティ要求について、医療保険者中間サーバー、後期高齢者医療広域連合標準システムの前例に倣って記載をした。

・オンプレ環境からクラウド環境への特定個人情報の移行の際のリスク対策が必要となることから記載をした。

・デジタル社会形成整備法第51条による個人情報保護法の改正に係る部分(地方関係への同法適用)の施行期日である令和5年4月1日からは、滅失又は毀損の防止等に関する安全確保の措置を義務付けするのは国になるため削除した。

・デジタル社会形成整備法第51条による個人情報保護法の改正に係る部分(地方関係への同法適用)の施行期日である令和5年4月1日からは、個人情報ファイル簿の公開が必須となることから記載をした。

変更箇所については、評価書の「(別紙3)変更箇所」を参照