

IaaS・PaaS（IoTクラウドサービス）  
の安全・信頼性に係る情報開示認定制度  
～申請書作成の手引き～

令和4年4月1日

クラウドサービス情報開示認定機関  
一般社団法人日本クラウド産業協会  
(ASPIC)

## 目次

はじめに .....	1
1. 申請書の記入方法について.....	2
2. 「事業者」に関わる項目の説明.....	4
2. 1 開示情報の時点.....	4
2. 2 事業所・事業.....	4
2. 3 人材.....	5
2. 4 財務状況.....	5
2. 5 資本関係・所属団体.....	7
2. 6 コンプライアンス.....	8
3. 「サービス」に関わる項目の説明.....	13
3. 1 センターサービス.....	13
3. 2 提供端末.....	19
3. 3 推奨端末.....	21
3. 4 サービス基本特性.....	22
3. 5 システム運用（システム基盤運用、セキュリティ等）.....	27
3. 6 ハウジング（サーバ設置場所） ※使用データセンター毎に記載.....	32
3. 7 サービスサポート.....	37

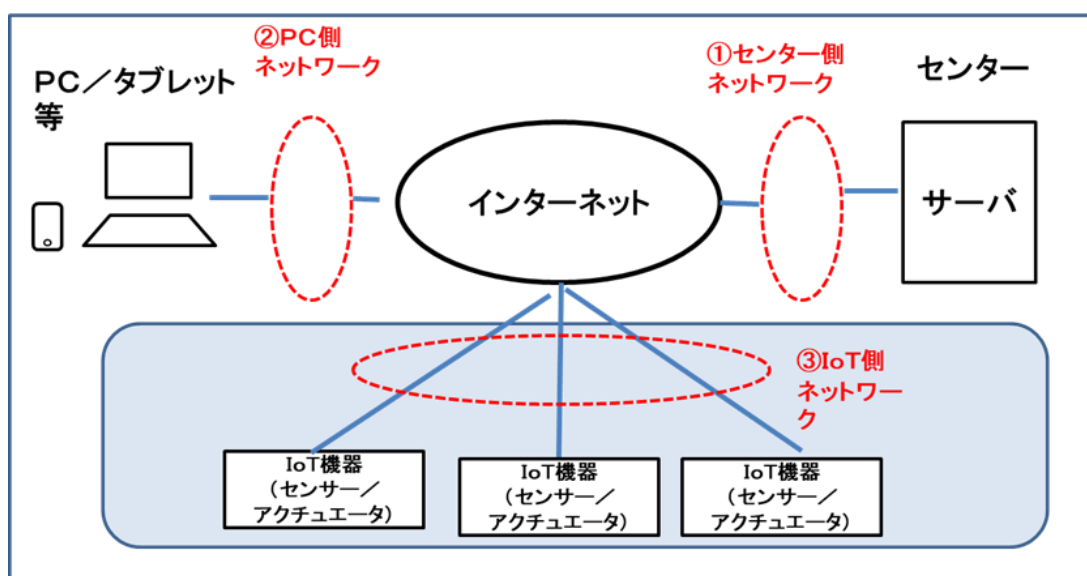
（参考） 本書中に、『「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容』と題して破線テキストボックスで記述した内容は、ASP・SaaSの情報セキュリティ対策に関する研究会から公表された「ASP・SaaSにおける情報セキュリティ対策ガイドライン」（平成20年1月30日）の関連記述を引用しています。

## はじめに

本認定制度は、IoTクラウドサービス情報開示指針にしたがって制定しています。

「IoT クラウドサービス」とは、IoT 機器(センサーやアクチュエータ)を使ったクラウドサービスのことを言います。

IoTクラウドサービス情報開示指針は、IoTクラウドサービスの想定モデルをもとに作成されています。想定モデルを下図に、考え方を以下に示します。



なお、IoTクラウドサービスは、発展途上にあるので、想定以外のモデル、パターンが出現することが想定されます。このような場合は、認定事務局にご相談ください。

### (1) IoTクラウドサービスでの開示情報の拡張

従来の ASP・SaaS 情報開示指針では、センター(サーバ)、ネットワーク(①センター側ネットワーク、②PC 側ネットワーク)の安全性・信頼性に係る情報開示項目が中心でしたが、IoTクラウドサービスでは IoT 機器(センサー/アクチュエータ)、③IoT 側ネットワークに情報開示項目を拡張しました。

今回、IoTクラウドサービスに拡張する際に、IoT の特性を踏まえ、特に「性能」、「セーフティ」及び「データの権利」に着目しました。

例えば、

- 性能は、大量データにより性能不足になる場合等
- セーフティは、アクチュエータが人に危害を及ぼす等
- データの権利は、プライバシーに関わるデータ等

です。

## (2) 情報の開示元と開示先

IaaS・PaaS(IoTクラウドサービス)は、IaaS・PaaS 事業者が情報の開示元、ユーザ(ASP・SaaS 事業者またはエンドユーザ)が開示先となります。

## (3) 想定するサプライチェーンについて

IoT機器およびIoT側のネットワークの調達については、以下のパターンを想定します。

- ① IaaS・PaaS 事業者が調達する場合
- ② ユーザ(ASP・SaaS 事業者又はエンドユーザ)が調達する場合

- ① IoT機器およびIoT側ネットワークを IaaS・PaaS 事業者が調達する場合は、IaaS・PaaS 事業者は、IoT機器およびIoT側ネットワークをユーザ(ASP・SaaS 事業者又はエンドユーザ)に「提供」します。
- ② IoT機器およびIoT側ネットワークをユーザ(ASP・SaaS 事業者又はエンドユーザ)が調達する場合は、IaaS・PaaS 事業者は、IoT機器およびIoT側ネットワークをユーザ(ASP・SaaS 事業者又はエンドユーザ)に「推奨」します。

## 1. 申請書の記入方法について

### 1) 必須開示項目

必須開示項目については、必ず記述してください。必須開示項目に未記入の項目がある場合は、非認定となります。

対策や措置の有無が聞かれている項目で、対策や措置を実施していない場合、「無し」と記述しても非認定とはなりません。

### 2) 一定の要件を考慮すべき項目

必須開示項目で、一定の要件を考慮すべき項目とされたものは、記述内容は認定機関 が設定する一定水準を上回っている必要があります。その水準に満たない場合は、非認定となります。

ただし、一定の水準を下回る場合であっても、サービスの特性上やむを得ない場合、記入欄にその理由等を記述してください。

### 3) 選択開示項目

選択開示項目については、任意で記述してください。未記入であっても非認定となることはありません。

#### 4) 記入時の注意事項

本認定制度以外で取得されている認定制度や監査制度等と重複する審査対象項目であっても、「監査基準委員会報告書第18号監査（米国では監査基準SSAE16、国際監査基準IASE3402）取得済み」等の記述は行わず、手引きの指示通りに記述してください。

#### 5) 記入時の使用言語

記入時の使用言語は、日本語とします。

#### 6) 認定サービスの公表

認定サービスについては、認定機関ホームページにおいて、申請内容欄に記述された内容をそのまま公表させていただきます。添付書類等欄の記述は公表されません。

## 2. 「事業者」に関わる項目の説明

株式会社、社団法人等の団体については、「事業者」に関わる項目のうち必須開示項目をすべて記述してください。個人の場合は、必須開示項目についても記入可能なもののみ、記述し、可能でないものについては「個人事業であるため回答できない。」等と記述してください。

(注) 各審査対象項目の末尾の( )内には、申請書上の審査項目の通番と、必須/選択開示項目の区分を示します。

### 2. 1 開示情報の時点

#### (1) 開示情報の日付

##### ① 開示情報の日付(1: 必須開示項目)

【記述内容】 開示情報の年月日(西暦)

【説明】 申請に伴い記入される審査対象項目の全てについて、申請者が情報開示していることを確認した年月日を西暦で記述してください。基本的には申請日現在で貴社が情報開示されている内容に基づいて申請してください。未記入の場合は非認定となります。

### 2. 2 事業所・事業

#### (1) 事業所等の概要

##### ① 事業者名(2: 必須開示項目)

【記述内容1】 事業者の正式名称(商号)

【記述内容2】 法人番号

【説明】 貴社の登記上の正式な社名と法人番号を記述してください。未記入の場合は非認定となります。

##### ② 設立年月日(3: 必須開示項目)

【記述内容】 事業者の設立年月日(西暦)

【説明】 貴社の設立年月日を西暦で記述してください。未記入の場合は非認定となります。

##### ③ 事業所(4: 必須開示項目)

【記述内容1】 事業者の本店所在地

【記述内容2】 事業者ホームページ

**【説明】** 事業者の本店所在地及びホームページのURLを記述してください。  
上記いずれかの記述内容が未記入の場合は非認定となります。

## (2) 事業の概要

### ① 主な事業の概要(5: 必須開示項目)

**【記述内容】** 事業者の主な事業の概要(ASP・SaaS以外も含む) <100字以内>

**【説明】** ASP・SaaSに関連している事業以外も含めて、事業概要について100字以内で記述してください。

未記入の場合は非認定となります。

## 2. 3 人材

### (1) 経営者

#### ① 代表者(6: 代表者氏名は必須開示項目、代表者経歴は選択開示項目)

**【記述内容1】** 代表者氏名

**【記述内容2】** 代表者経歴(生年月日、学歴、業務履歴、資格等)

**【説明】** 代表者氏名が未記入の場合は非認定となります。

また、代表者の経歴(生年月日、学歴、業務履歴、資格等)を可能な範囲で記述してください。

#### ② 役員(7: 選択開示項目)

**【記述内容】** 役員数

**【説明】** 役員について、役員数を記述してください。なお、ここで言う役員とは、会社法で規定されている取締役、執行役だけでなく、執行役員も含まれます。

### (2) 従業員

#### ③ 従業員数(8: 必須開示項目)

**【記述内容】** 正社員数(単独ベース)

**【説明】** 単独ベースでの正社員数を記述してください。

未記入の場合は非認定となります。

## 2. 4 財務状況

### (1) 財務データ

財務データは、株主総会で承認された直近のものを用いてください。提出いただきます書類も、株主総会で承認された直近のものでお願いします。公益法人の場合は、株式会社の株

主総会に相当する機関(社団法人であれば社員総会)により承認されたものを用いてください。

① 売上高(9: 必須開示項目)

【記述内容】 事業者の売上高(単独ベース)

【説明】 直近決算期の損益計算書における売上高(単独ベース)を円単位で記述してください。また、決算期も記述してください。  
未記入の場合は非認定となります。

② 経常利益(10: 選択開示項目)

【記述内容】 事業者の経常利益額(単独ベース)

【説明】 直近決算期の損益計算書における経常利益額(単独ベース)を円単位で記述してください。また、決算期も記述してください。

③ 資本金(11: 必須開示項目)

【記述内容】 事業者の資本金(単独ベース)

【説明】 直近決算期の貸借対照表の資本金(単独ベース)を円単位で記述してください。また、決算期も記述してください。  
未記入の場合は非認定となります。

④ 自己資本比率(12: 選択開示項目)

【記述内容】 事業者の自己資本の比率(単独ベース)

【説明】 直近決算期の自己資本比率を下式により算定し、記述してください。また、決算期も記述してください。

$$\text{自己資本比率} = [\text{自己資本}] / [\text{総資産}]$$

⑤ キャッシュフロー対有利子負債比率(13: 選択開示項目)

【記述内容】 事業者のキャッシュフロー対有利子負債比率(単独ベース)

【説明】 直近決算期のキャッシュフロー対有利子負債比率を下式により算定し、記入ください。また、決算期も記述してください。

$$\text{キャッシュフロー対有利子負債比率} = [\text{有利子負債}] / [\text{営業キャッシュフロー}]$$

⑥ インタレスト・カバレッジ・レシオ(14: 選択開示項目)

【記述内容】 事業者のインタレスト・カバレッジ・レシオ(単独ベース)

【説明】 直近決算期のインタレスト・カバレッジ・レシオを下式により算定し、記入ください。



また、決算期も記述してください。

$$\text{インタレスト・カバレッジ・レシオ} = [\text{営業キャッシュフロー}] / [\text{利払い}]$$

## (2) 財務信頼性

### ① 上場の有無 (15: 選択開示項目)

【記述内容】 株式上場の有無と、「有り」の場合は市場名

【説明】 株式上場をしているか否かについて記述してください。

また、上場している場合は、その市場名 (例: 東証1部、JASDAQ) も記述してください。

### ② 財務監査・財務データの状況 (16: 選択開示項目)

【記述内容】 該当する財務監査・財務データの状況を、以下より選択する。

①会計監査人による会計監査、②会計参与による計算書類等の作成、③「中小企業会計要領」の適用に関するチェックリストの活用、④監査役による監査、⑤いずれでもない

【説明】 財務データの正確性を確保するために講じている措置として該当するものを次の中から選び、記述してください。

- ①会計監査人による会計監査
- ②会計参与による監査
- ③「中小企業会計要領」の適用によるチェックリストの活用
- ④監査役による監査
- ⑤いずれも非該当

### ③ 決算公告 (17: 選択開示項目)

【記述内容】 決算公告の実施の有無

【説明】 決算公告の実施について、「有り」または「無し」を記述してください。

## 2. 5 資本関係・所属団体

### (1) 資本関係

#### ① 株主構成 (18: 選択開示項目)

【記述内容】 大株主の名称 (上位5株主程度)、及び各々の株式保有比率

【説明】 発行した株式の保有数上位5株主程度の株主の名称、及び各々の保有比率について記述してください。

(2) 所属団体

① 所属団体(19: 選択開示項目)

【記述内容】 所属している業界団体、経済団体等の名称

【説明】 現在所属している主な業界団体、経済団体等の名称を記述してください。

## 2. 6 コンプライアンス

(1) 組織体制

① コンプライアンス担当役員(20: 選択開示項目)

【記述内容1】 コンプライアンス担当役員の氏名

【説明】 役職員が関連法令を遵守して事業を遂行することを指導・監督する役割を担う役員(コンプライアンス担当役員)が任命されている場合には、その氏名を記述してください。

なお、ここでの役員には、会社法で規定されている取締役、執行役だけでなく、執行役員も含まれます。

(参考)「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の「組織的安全管理対策」「運用管理規程等」に記載されている対策内容

「経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。自社で定める情報セキュリティに関する組織的取組における基本方針が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること」

② 専担の部署・会議体、(21: 選択開示項目)

【記述内容】 コンプライアンスを担当する社内の部署・会議体の有無と、「有り」の場合は社内の部署名・会議名

【説明】 役職員が関連法令を遵守して事業を遂行することを指導・監督する役割を担う部署(例:コンプライアンス部、法務部)や会議体(例:コンプライアンス委員会、リスク管理委員会)の「有り」または「無し」を記述してください。また、有る場合は、その名称を記述してください。

③ 情報セキュリティに関する組織体制の状況(22: 必須開示項目)

【記述内容1】情報セキュリティに関する責任者の有無と、「有り」の場合は責任者名・役職

【記述内容2】情報セキュリティに関する組織体制の有無

【説明】 情報セキュリティに関するコンプライアンス責任者の有無について、「有り」または、

「無し」を記述してください。また、「有り」の場合は、責任者氏名・役職を記述してください。

情報セキュリティに関する組織体制の有無について、「有り」または、「無し」を記述してください。

上記いずれかの記述内容が未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

II.1.1.1「経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。

II.2.1.3(情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合(組織環境、業務環境、法的環境、技術的環境等)に見直しを行うこと。

## (2) 個人情報

### ① 個人情報の取扱い(23: 必須開示項目)

【記述内容】 個人情報の取扱いに関する規程の有無と、「有り」の場合は記載箇所

【説明】 個人情報の取扱いに関する規程等の有無について「有り」または、「無し」を記述してください。また、「有り」の場合は、記載されている箇所(契約書等)について記述してください。

未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

III.5.1.2「個人情報は関連する法令に基づいて適切に取り扱うこと。」

## (3) 守秘義務

### ① 守秘義務契約(24: 必須開示項目)

【記述内容1】 守秘義務に係る契約又は条項の有無

【記述内容2】 守秘義務違反があった場合のペナルティ条項の有無

【説明】 守秘義務に係る契約または条項の有無について、「有り」または、「無し」で記述してください。

守秘義務違反があった場合のペナルティ条項の有無について、「有り」または、「無し」を記述してください。

上記いずれかの記述内容が未記入の場合は非認定となります。

(4) 従業員教育等

① 従業員に対するセキュリティ教育の実施状況(25:必須開示項目)

【記述内容1】 従業員に対するセキュリティ教育実施に関する取組の有無

【記述内容2】 従業員に対するセキュリティ教育実施に関する取組状況の開示の可否と、可能な場合の条件等

【説明】 従業員に対するセキュリティ教育の実施の取組みについて、「有り」または、「無し」で記述してください。

取組状況の開示の可否について、「可」または、「否」で記述してください。また、開示が可能な場合の条件等がある場合は、その内容も記述してください。

上記いずれかの記述内容が未記入の場合も非認定となります。

② 従業員に対する守秘義務等の状況(26:必須開示項目)

【記述内容1】 従業員に対する守秘義務対応の取組状況

【記述内容2】 従業員に対する守秘義務対応状況の情報開示の可否と、可能な場合の条件等

【説明】 従業員に対する守秘義務対応の実施の有無について、「有り」または、「無し」で記述してください。

対応状況の開示の可否について、「可」または、「否」で記述してください。また、開示が可能な場合の条件等がある場合は、その内容も記述してください。

上記いずれかの記述内容が未記入の場合も非認定となります。

(5) 委託

① 委託情報に関する開示(27:必須項目)

【記述内容】 サービス提供に係る委託先(再委託先)の情報開示の可否と、可能な場合の条件等

【説明】 委託先(再委託先)に関する情報開示の可否について、「可」または、「否」で記述してください。また、情報開示が「可」の場合に、条件等がある場合は、その内容も記述してください。

未記入の場合も非認定となります。

② 委託先に対する管理状況(28:必須開示項目)

【記述内容1】 自社の個人情報保護指針に対する遵守規定の有無

【記述内容2】 委託先(再委託先)に係る個人情報保護等の状況に関する情報提供の可

否と、可能な場合の条件等

【記述内容3】 委託先(再委託先)との守秘義務対応状況

【説明】 委託先に対し、自社の個人情報保護指針を遵守する規定が有るか、否かについて、「有り」または、「無し」で記述してください。

委託先(再委託先)との守秘義務契約の有無について、「有り」または、「無し」で記述してください。

委託先(再委託先)との守秘義務契約の有無について、「有り」または、「無し」で記述してください。

上記いずれかの記述内容が未記入の場合も非認定となります。

## (6) 文書類

### ① 情報セキュリティに関する規程等の整備

(29 必須開示項目 / 一定の要件を考慮すべき項目)

【記述内容1】 情報セキュリティに関する基本方針・規程・マニュアル等の状況と文書名

【説明1】 情報セキュリティに関する基本方針・規程・マニュアル等の有無について、「有り」または、「無し」で記述してください。「有り」の場合には、文書名を記述してください。

未記入の場合もしくは情報セキュリティに関する基本方針・規程・マニュアル等の文書類が無い場合は非認定となります。

なお、これらの情報セキュリティに関する基本方針・規程・マニュアル等とは、情報の漏洩や不必要な消失等を防止するための組織体制、管理のためのプロセス等が記述されている文書類です。

【記述内容2】 情報セキュリティに係る規程等に関する情報提供の可否と、可能な場合の条件等

【説明2】 情報提供の可否について、「可」または、「否」で記述してください。また、情報提供が「可」の場合に、条件等がある場合は、その内容も記述してください。

未記入の場合は非認定となります。

### ② 事業継続に関する規程の整備(30:必須項目)

【記述内容1】 事業継続に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名

【記述内容2】 BCP対応計画及び運用手順書等の開示の可否と、可能な場合の条件等

【説明】 事業継続に関する基本方針・規程・マニュアル等の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、文書名を記述してください。

い。

BCP対応計画及び運用手順書等に関する情報開示の可否について、「可」または、「否」で記述してください。情報開示が「可」の場合に、条件等がある場合は、その内容を記述してください。

上記いずれかの記述内容が未記入の場合は非認定となります。

③ リスク管理に関する規程等の整備(31: 必須項目)

【記述内容】 リスク管理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名

【説明】 リスク管理に関する基本方針・規程・マニュアル等の文書類の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、文書名を記述してください。

未記入の場合は非認定となります。

④ 勧誘・販売・係争に関する規程等の整備(32: 必須開示項目)

【記述内容1】 勧誘・販売に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名

【記述内容2】 係争に関する規程・管轄裁判所等、係争が生じた際の対応に関する情報を含む文書類の有無と、「有り」の場合は文書名

【説明】 勧誘・販売に関する基本方針・規程・マニュアル等の文書類について、「有り」または、「無し」を記入してください。また、「有り」の場合は、文書名を記述してください。

係争が生じた際の対応や管轄裁判所等を記載した文書類について、「有り」または、「無し」を記述してください。また、「有り」の場合は、文書名を記述してください。なお、勧誘・販売に関する基本方針・規程・マニュアル等とは、サービスに関する重大な付帯条件を説明せずに勧誘することの禁止、ユーザがサービスを十分に理解していない段階での強引な契約の禁止等、勧誘・販売の進め方の方針や禁止行為等が記述されている文書類です。また、係争に関する文書類とは、係争が生じた際にユーザとの係争を円滑に処理するための基本方針や管轄裁判所等が明記されている文書類です。

上記いずれかの記述内容が未記入の場合は非認定となります。

⑤ IaaS・PaaSの苦情対応に関する規程等の整備(33: 必須開示項目)

【記述内容1】 IaaS・PaaSの苦情処理に関する基本方針・規程・マニュアル等の有無

と、「有り」の場合は文書名

【記述内容2】 IaaS・PaaS事業者の事故責任の範囲と補償範囲が記述された文書の有無と、「有り」の場合は文書名

【説明】 IaaS・PaaSのサービスの苦情処理に関する基本方針・規程・マニュアル等について、「有り」または、「無し」を記入してください。また、「有り」の場合は、文書名を記述してください。

なお、ここでいうIaaS・PaaSのサービスの苦情処理に関する基本方針・規程・マニュアル等とは、苦情処理部署の設置、苦情処理の手順(苦情の記録、苦情処理の担当部署への報告、サービス部門との事実確認等)の方針等が記述されている文書類です。苦情の範囲・レベルに関係なく、外部からの問合せ等に対してどのように対応するかを明文化した何らかの社内文書があるか否かを記述してください。

IaaS・PaaS事業者の事故責任の範囲と補償範囲が記述された文書について、「有り」または、「無し」を記入してください。また、「有り」の場合は、文書名を記述してください。

上記いずれかの記述内容が未記入の場合は非認定となります。

### 3. 「サービス」に関わる項目の説明

(注) 各審査対象項目の末尾の( )内には、申請書上の審査項目の通番と、必須/選択開示項目の区分を示します。

#### 3. 1 センターサービス

##### (1) サービス内容

###### ① サービス名称 (34: 必須開示項目)

【記述内容】 情報開示した IaaS・PaaSの名称

【説明】 未記入の場合は非認定となります。

###### ② サービス開始時期 (35: 必須開示項目)

【記述内容】 情報開示した IaaS・PaaSサービスのサービス開始年月日(サービス開始から申請時までの間に大きなリニューアル等が行われた場合は、その年月日も記述)

【説明】 未記入の場合は非認定となります。

###### ③ サービスの概要 (36: 必須開示項目)

【記述内容】 申請したサービスの内容

【説明】 申請したサービスの内容を500文字以内でご記入ください。未記入の場合は非認定となります。

④ I o Tクラウドサービス基本事項（37：必須開示項目）

【記述内容】 I o Tクラウドサービスに対する基本的な考え方、安全性（セーフティ）、連携内容、資産の管理方法、セキュリティ・バイデザイン、調達管理などを記述

【説明】 I o Tクラウドサービスに対する基本的な考え方を、記述内容に列挙したような観点からご記入ください。未記入の場合は非認定となります。

⑤ サービスの基本タイプ（38：必須開示項目）

【記述内容】 システム基盤サービス、開発・実行基盤サービス、アプリ基盤サービス、ハード基盤サービス、ネットワーク基盤サービスの中から該当タイプを選択（複数選択可）。

【説明】 申請したサービスが以下のどのタイプに該当するか（複数選択可）をご記入ください。未記入の場合は非認定となります。

○システム基盤サービス

アプリケーションのASP・SaaS化に必要な課金・認証等の付加機能を提供するサービス（例：認証、決済・課金、セキュリティ、タイムスタンプ等）、バックアップ・リストアサービス等

○開発・実行基盤サービス

アプリケーション、システム等の開発・実行環境を提供するサービス（例：OS、ミドルウェア、開発キット等、各種ソフトウェア開発環境の提供等）

○アプリ基盤サービス

メールサービス、Webサービス等のアプリケーションの基盤を提供するサービス

○ハード基盤サービス

ASP・SaaSの提供に必要なハードウェア資源をネットワーク経由で提供するサービス（例：サーバ提供、ストレージ提供等）

○ネットワーク基盤サービス

ルーター、スイッチ等のネットワーク機器を提供するサービス（例：ロードバランサ、ネットワーク機器提供等）



⑥ サービスのカスタマイズ範囲（39：必須開示項目）

【記述内容】 サービスのカスタマイズの範囲（特に決まっていない、相談に応じて決める等の場合は、その旨を記述）

【説明】 未記入の場合は非認定となります。

⑦ 提供回線・帯域（40：選択開示項目）

【記述内容1】 専用線（VPNを含む）、インターネット等の回線の種類、提供帯域の種類、帯域保証がある場合にはその内容。

【説明1】 可能な範囲でご記入ください。

【記述内容2】 提供回線が別契約（有償）回線か、基本料金にバンドルされているか、の区別。

【説明2】 可能な範囲でご記入ください。

（2）サービス構成（システム基盤サービス）

① 提供OS（41：必須開示項目）

【記述内容】 仮想化ソフト（ハイパーバイザ）の提供の有無、ゲストOSとして動くOS（Windows、Unix、Linux等）及びそのバージョンを記述

【説明】 提供OSについてご記入ください。未記入の場合は非認定となります。

② サーバ管理（42：必須開示項目）

【記述内容】 サーバOS初期化、OSに関するパッチアップデート等のサービス内容

【説明】 サーバ管理サービスの内容についてご記入ください。

未記入の場合は非認定となります。

③ ASP・SaaS支援サービス（43：必須開示項目）

【記述内容】 検索、認証、決済・課金、セキュリティ、位置情報、タイムスタンプ、メディア、言語変換等のサービス内容

【説明】 ASP・SaaS支援サービスの内容についてご記入ください。未記入の場合は非認定となります。

④ IoT支援サービス（44：必須開示項目）

【記述内容】 IoTシステムの構築を支援するサービスの内容（データ集約、プ

ロトコル変換、アクセスコントロールなど)

【説明】 IoT支援サービスの内容についてご記入ください。未記入の場合は非認定となります。

⑤ 管理者接続用ネットワーク提供サービス (45: 必須開示項目)

【記述内容】 リモートデスクトップ、SSH等の接続手段の内容

【説明】 管理者接続用ネットワーク提供サービスの内容についてご記入ください。

未記入の場合は非認定となります。

⑥ バックアップ・リストアサービス (46: 必須開示項目)

【記述内容】 バックアップサービス、障害時のリストアサービス等の内容

【説明】 バックアップ・リストアサービスの内容についてご記入ください。

未記入の場合は非認定となります。

⑦ その他サービス (47: 必須開示項目)

【記述内容】 上記に該当しないその他サービスの内容

【説明】 上記に該当しないその他のサービス (各種申請代行、決済代行、業務代行、コンサルティング等) があればそのサービス内容についてご記入ください。

未記入の場合は非認定となります。

(3) サービス構成 (開発・実行基盤サービス)

① ソフトウェア開発環境支援サービス (48: 必須開示項目)

【記述内容】 Java、Servlet、Perl、PHP、Ruby、C/C++、その他のオープンソースの開発環境の提供等

【説明】 アプリケーション、システム等の開発・実行環境を提供するサービス (プログラミング言語、開発支援環境等) の内容についてご記入ください。

未記入の場合は非認定となります。

(4) サービス構成 (アプリ基盤サービス)

① ドメイン等管理サービス (49: 必須開示項目)

**【記述内容】** IPアドレス管理、ドメイン取得・管理、DNSサーバ等のサービス内容

**【説明】** ドメイン等管理サービスの内容についてご記入ください。  
未記入の場合は非認定となります。

② メールサービス (50: 必須開示項目)

**【記述内容】** Webメール、メーリングリスト等のサービス内容

**【説明】** メールサービスの内容についてご記入ください。  
未記入の場合は非認定となります。

③ Webサービス (51: 必須開示項目)

**【記述内容】** Webサーバ、FTPサーバ、Webアカウント、アクセス制御、アクセスログ解析、アクセスログ取得、ブログ、掲示板などのサービス内容

**【説明】** Webサービスの内容についてご記入ください。  
未記入の場合は非認定となります。

④ その他サービス (52: 必須開示項目)

**【記述内容】** 上記に該当しないその他サービスの内容

**【説明】** 上記に該当しないその他のサービス (DBサーバ等) があればそのサービス内容についてご記入ください。  
未記入の場合は非認定となります。

(5) サービス構成 (ハード基盤サービス)

① サーバ提供サービス (53: 必須開示項目)

**【記述内容】** 共用サーバ、専用サーバ等のサービス内容

**【説明】** サーバ提供サービスの内容についてご記入ください。  
未記入の場合は非認定となります。

② ストレージ提供サービス (54: 必須項目)

【記述内容】 ストレージ提供サービスの内容

【説明】 ストレージ提供サービスの内容についてご記入ください。  
未記入の場合は非認定となります。

③ レンタル機器サービス (55: 必須開示項目)

【記述内容】 レンタル機器類の障害時対応サービス、定期運用サービス、運用・保守支援サービスの有無と、有りの場合にはその内容

【説明】 レンタル機器サービスの内容についてご記入ください。  
未記入の場合は非認定となります。

④ 統合リソース提供サービス (56: 必須開示項目)

【記述内容】 仮想リソース群（仮想マシン、サーバ、ストレージ、ネットワーク等）を統合して提供するサービスの内容

【説明】 統合リソース提供サービスの内容についてご記入ください。  
未記入の場合は非認定となります。

⑤ その他サービス (57: 必須開示項目)

【記述内容】 上記に該当しないその他サービスの内容

【説明】 上記に該当しないその他サービスがあれば、そのサービス内容についてご記入ください。

未記入の場合は非認定となります。

(6) サービス構成 (ネットワーク基盤サービス)

① ロードバランサーサービス (58: 必須開示項目)

【記述内容】 ロードバランサーサービスの内容

【説明】 未記入の場合は非認定となります。

② ネットワーク機器提供サービス (59: 必須開示項目)

【記述内容】 ルーター、スイッチ等のネットワーク機器提供サービスの内容

【説明】 未記入の場合は非認定となります。

③ IoT側ネットワークサービス（60：必須開示項目）

【記述内容】 提供又は推奨するIoT側ネットワークの回線、帯域など

【説明】 未記入の場合は非認定となります。

④ その他サービス（61：必須開示項目）

【記述内容】 上記に該当しないその他サービスの内容

【説明】 上記に該当しないその他サービスがあれば、その内容をご記入ください。

未記入の場合は非認定となります。

### 3. 2 提供端末

提供する端末が複数種類ある場合は、端末ごとに記入してください。

(1) IoT機器（センサー、アクチュエータ）

① 機器（62：必須開示項目）

【記述内容1】 提供する機器の有無。「有り」の場合は、機器の種類、製品名などを記入ください。「無し」の場合は「無し」と記入してください。

【記述内容2】 機器の主な機能

【記述内容3】 機器のセキュリティレベル、認証取得状況等

【説明】 未記入の場合は非認定となります。

② 接続条件（63：必須開示項目）

【記述内容】 接続数、設置条件などの制約

【説明】 例えば「センサーとアクチュエータの同時接続数〇〇万台まで」、「日本国海道、沖縄を除く」のように記述してください。

未記入の場合は非認定となります。

③ 使用条件（64：必須開示項目）

【記述内容】 IoT機器の目的外使用の禁止などの使用条件

【説明】 例えば「目的外使用の免責」、「提供外機器使用の免責」などを記述してください。

未記入の場合は非認定となります。

④ ソフトウェア (65 : 必須開示項目)

【記述内容】 IoT機器組み込みソフト

【説明】 未記入の場合は非認定となります。

⑤ 物理的セキュリティ (66 : 必須開示項目)

【記述内容】 推奨(提供)する盗難防止策など

【説明】 例えば、「センサーは目隠し湯カバーを設置」、「鍵のかかる部屋に設置」  
などのように記述してください。

未記入の場合は非認定となります。

⑥ 保守・管理 (67 : 必須開示項目)

【記述内容】 保守体制、管理手法など

【説明】 例えば、「全国に拠点を持つ保守会社と契約」、「契約更新時に保守状  
況を確認」などのように記述してください。

未記入の場合は非認定となります。

⑦ セキュリティ対策 (68 : 必須開示項目)

【記述内容】 IoT機器のセキュリティ対策(初期パスワードの変更、OS等の最新化、  
エッジコンピュータ、ゲートウェイの導入等)

【説明】 未記入の場合は非認定となります。

(2) GW/エッジコンピュータなど

① 機器 (69 : 必須開示項目)

【記述内容1】 機器の種類、製品名など

【記述内容2】 機器の主な機能

【記述内容3】 機器のセキュリティレベル、認証取得状況等

【説明】 未記入の場合は非認定となります。

② 接続条件 (70 : 必須開示項目)

【記述内容】 接続数、設置条件などの制約

【説明】 例えば「1サイトに1ゲートウェイ」「ゲートウェイ1台あたり、センサー〇〇

○台まで」、「日本国内(北海道、沖縄を除く)」のように記述してください。

未記入の場合は非認定となります。

③ 使用条件 (71: 必須開示項目)

【記述内容】 目的外使用の禁止などの使用条件

【説明】 例えば「目的外使用の免責」などを記述してください。

未記入の場合は非認定となります。

④ 物理的セキュリティ (72: 必須開示項目)

【記述内容】 盗難防止策など

【説明】 例えば、「ゲートウェイは専用のマシン室に設置」、「入退室管理は利用者側で実施」などのように記述してください。

未記入の場合は非認定となります。

⑤ 保守・管理 (73: 必須開示項目)

【記述内容】 保守体制、管理手法など

【説明】 例えば、「ゲートウェイのメーカーと保守契約」、「契約更新時に保守状況を確認」などのように記述してください。

未記入の場合は非認定となります。

### 3. 3 推奨端末

① PC等 (操作端末) (74: 必須開示項目)

【記述内容1】 パソコン、スマホ、タブレット、シンクライアント等の端末の種類、OS等

【記述内容2】 利用するブラウザの種類

【説明1,2】 操作端末の概要を記入してください。

未記入の場合は非認定となります。

② IoT機器 (センサー、アクチュエータ) (75: 必須開示項目)

【記述内容1】 推奨機器の「有無」。「有り」の場合は、その種類、製品名などを記入してください。「無し」の場合は「無し」と記入してください。

【記述内容2】 推奨機器の主な機能

【記述内容3】 推奨機器のセキュリティレベル、認証取得状況等

【説明】 未記入の場合は非認定となります。

③ GW/エッジコンピュータなど（76：必須開示項目）

【記述内容1】 推奨機器の「有無」。「有り」の場合は、その種類、製品名などを記入してください。「無し」の場合は「無し」と記入してください。

【記述内容2】 推奨機器の主な機能

【記述内容3】 推奨機器のセキュリティレベル、認証取得状況等

【説明】 未記入の場合は非認定となります。

### 3. 4 サービス基本特性

#### (1) サービス品質

##### ① サービス稼働設定値（77：必須開示項目）

【記述内容1】 サービス稼働率の目標値

【記述内容2】 サービス稼働率の実績値

【説明1,2】 申請したサービスについてのサービス稼働率について、次の式により算出しご記入ください。

$$\begin{aligned} \text{○サービス提供時間} &= [\text{契約サービス時間}] \\ &\quad - [\text{事前通知された定期保守によるサービス停止時間}] \end{aligned}$$

$$\begin{aligned} \text{○サービス稼働時間} &= [\text{サービス提供時間}] \\ &\quad - [\text{事前通知のないサービス停止時間}] \end{aligned}$$

$$\text{○サービス稼働率} = [\text{サービス稼働時間}] / [\text{サービス提供時間}]$$

なお、事前通知のないサービス停止時間とは、システム障害等によってサービス提供が停止した時間を指します。

・新規申請時は、直近1年間（サービス開始から1年未満の場合は、サービス開始後から申請日まで）の稼働率実績をご記入ください。

・更新申請時は、直近1年間の稼働率実績値をご記入ください。

未記入の場合は非認定となります。

【記述内容3】 サービス停止の事故歴

【説明2】 サービス停止の事故歴については、申請時期や区分により以下のように記述してください。ここでいうサービス停止事故とは、大規模な性能劣化または何らかの障害によりサービスの停止と事業者



が判断したものを指します。

- ・新規申請時は、直近1年間（サービス開始から1年未満の場合は、サービス開始後から申請日まで）のサービス停止事故件数と事故の概要をご記入ください。
- ・更新申請時は、直近1年間のサービス停止事故件数と概要についてご記入ください。

未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.2.1.1「ASP・SaaS サービスを利用者に提供する時間帯を定め、この時間帯における ASP・SaaS サービスの稼働率を規定すること。また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。

## ② サービスパフォーマンスの管理（78：選択開示項目）

**【記述内容1】** 機器障害やシステム遅延の早期検知方法（検知の場所、検知のインターバル、画面の表示チェック等の検知方法）

**【説明1】** 可能な範囲でご記入ください。

**【記述内容2】** サービスのパフォーマンス把握方法（検知の場所、検知のインターバル、画面の表示チェック等の把握方法）

**【説明2】** 可能な範囲でご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.1.1.3「ASP・SaaS サービスを利用者に提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。

また、利用者との取決めに基づいて、監視結果を利用者に通知すること。」

## ③ 認証取得、監査実施（79：選択開示項目）

**【記述内容】** プライバシーマーク、ISMS（JIS Q 27001など）、ITSMS（JIS Q 20000-1など）、18号監査（米ではSAS70や後継のSSAE16）の監査報告書作成の有無と、有りの場合は認証名あるいは監査の名称

**【説明】** 可能な範囲でご記入ください。

④ 脆弱性診断 (80: 選択開示項目)

【記述内容】 脆弱性診断の有無と、有りの場合は評価基準、対策手順の有無等の整備備状況、対策の実施状況などの概要

【説明】 可能な範囲でご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.2.1.4「ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的に脆弱性診断を行い、その結果に基づいて対策を行うこと。」

⑤ バックアップ対策 (81: 必須開示項目)

【記述内容】 バックアップ実施インターバル、及び 世代バックアップ (何世代前までかを記述)

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.2.3.1「利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。」

⑥ サービス継続 (82: 必須開示項目)

【記述内容1】 サービスが停止しない仕組み (冗長化、負荷分散等)

【記述内容2】 他データセンターへのデータのバックアップの有無と、「有り」の場合は当該データセンターの場所 (国内の場合は、地域ブロック名、国外の場合は設置国)

【記述内容3】 他データセンターへのシステム (データを含む) のバックアップの有無と、「有り」の場合は当該データセンターの場所 (国内の場合は、地域ブロック名、国外の場合は設置国)

【説明】 冗長化、負荷分散等サービスが停止しない仕組みについて記述してください。  
他データセンターへのデータのバックアップの有無と、「有り」の場合は当該データセンターの場所 (国内の場合は、地域ブロック名、国外の場合は設置国) について記述してください。  
他データセンターへのシステム (データを含む) のバックアップの有無と、「有り」の場合は当該データセンターの場所 (国内の場合は、地域ブロック名、国外の場合は設置国) について記述してください。

未記入の場合は非認定となります。

上記いずれかの記述内容が未記入の場合は非認定となります。

⑦ 受賞・表彰歴（83：選択開示項目）

【記述内容】 IaaS・PaaS サービスに関連する各種アワード等の受賞歴

【説明】 可能な範囲でご記入ください。

⑧ SLA（サービスレベル・アグリーメント）（84：必須開示項目）

【記述内容】 当該サービスに係る SLA が契約書に添付されているか否か

【説明】 SLA とは、「事業者が独自に顧客との間で取り決めるサービス水準に関する合意事項」を指します。

未記入の場合は非認定となります。

(2) サービスの変更・終了

① サービス（事業）変更・終了時の事前告知（85：必須開示項目）

【記述内容】 利用者への通知時期（●ヶ月前等と記述）、通知方法

【説明】 事業者側の何らかの理由により、申請したサービスの内容が大きく変更となった場合、あるいは事業として停止・終了した場合に、利用者へ事前に通知する時期及び通知方法についてご記入ください。上記2つの記述内容の1つでも記入がない場合は非認定となります。

② サービス（事業）変更・終了後の対応・代替措置（86：必須開示項目）

【記述内容1】 対応・代替措置の基本方針の有無、基本方針がある場合はその概略。

【記述内容2】 契約終了に伴うユーザへの対応策（代替サービスの紹介等）の有無、対応策がある場合はその概略。

【記述内容3】 契約終了時の情報資産（ユーザデータ等）の返却責任の有無。

【説明】 上記3つの記述内容のうち、1つでも記入がない場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.4.1.1「取り扱う核情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。」

(3) 契約の終了等

① 情報の返却・削除・廃棄(87: 必須開示項目)

【記述内容1】 契約終了時等の情報資産(利用者データ等)の返却責任の有無と、受託情報の返却方法・ファイル形式・費用等

【記述内容2】 情報の削除または廃棄方法の開示の可否と、可能な場合の条件等

【記述内容3】 削除又は廃棄したことの証明書等の提供

【説明】 契約終了時等において、利用者のデータ等の情報資産の返却責任の有無について、「有り」または、「無し」を記述してください。また、サービス開始時等において利用者から受託した情報の返却方法・ファイル形式・費用等について記述してください。

情報の削除または廃棄方法の開示の可否について、「可」または「否」を記述してください。また「可」の場合は、条件等について記述してください。

削除または廃棄した際の証明書の提供について「可」または「否」を記述してください。証明書の提供ができない場合は非認定となります。

上記いずれかの記述内容が未記入の場合は非認定となります。

(4) サービス料金・解約

① 料金体系・金額(88: 必須開示項目)

【記述内容】 初期費用額、月額利用額、最低利用契約期間

【説明】 申請したサービスの料金体系について、契約に伴う初期費用額、契約以降継続的に発生する月次利用額、契約によって利用者に課せられる最低利用月額契約期間をご記入ください。

未記入の場合は非認定となります。

② 解約時違約金払いの有無(89: 必須開示項目)

【記述内容】 解約時違約金(ユーザ側)の有無、違約金がある場合はその額

【説明】 利用者側の都合により契約を解約した場合の違約金の有無とその条件、違約金がある場合にはその金額もしくは算定条件をご記入ください。

未記入の場合は非認定となります。

③ 利用者からの解約事前受付期限（90：必須開示項目）

【記述内容】 利用者からのサービス解約の申請時の受付期限の有無、ある場合はその期限（何日・何か月前かを記述）

【説明】 未記入の場合は非認定となります。

(5) 契約者数

① 契約者数（91：選択開示項目）

【記述内容】 本IaaS・PaaSサービスの契約者数等

【説明】 可能な範囲でご記入ください。

(6) データ管理

① データの所在（92：必須開示項目）

【記述内容】 本IaaS・PaaSサービス使用時における顧客データの保存先・所在先（国名）

【説明】 未記入の場合は非認定となります。

② 使用データセンター（93：必須開示項目）

【記述内容】 本IaaS・PaaSサービス使用時における使用データセンターの数

【説明】 未記入の場合は非認定となります。

3. 5 システム運用（システム基盤運用、セキュリティ等）

(1) システム基盤運用

① 死活監視（機器等）（94：必須開示項目）

【記述内容】 死活監視の有無、死活監視を行っている監視の対象（基盤、ストレージ等）、ジ及び死活監視の対象ごとの監視インターバル、監視時間、通知時間

【説明】 監視インターバルは「何分ごとに監視を行っているかの数値（時間間隔）」をご記入ください。また、通知時間は、「死活監視によって停止した後、指定された利用者に通知するまでの時間」をご記入ください。

未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.1.1.1「ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。

② 障害監視（機器等）（95：必須開示項目）

【記述内容】 障害監視の有無

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.1.1.2「ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。

障害を検知した場合は、利用者に速報を通知すること。」

③ 時刻同期（96：必須開示項目）

【記述内容】 システムの時刻同期方法

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.1.1.5「ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。」

(2) セキュリティ（基盤、ストレージ等）

① ウイルス対策（97：必須開示項目）

【記述内容】 ウイルス対策の有無、対策がある場合はパターンファイルの更新間隔（ベンダーリリースからの時間）

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.2.2.1「ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。」

② 管理者認証（98：必須開示項目）

【記述内容】 管理者権限（サービス提供事業者側）の登録・登録削除の正式な手順の有無

【説明】 未記入の場合は非認定となります。

③ ID・パスワードの運用管理（99：必須開示項目）

【記述内容】 IDやパスワードの運用管理方法（サービス提供事業者側）の規程の有無

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.3.1.3「利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方式等により、アクセス制御となりすまし対策を行うこと。

また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。」

④ 記録（ログ等）（100：必須開示項目）

【記述内容】 利用者の利用状況、例外処理及びセキュリティ事象の記録（ログ等）取得の有無、記録（ログ等）がある場合にはその保存期間

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.2.1.3「利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。」

⑤ セキュリティパッチ管理（101：必須開示項目）

【記述内容】 セキュリティパッチの情報取得方法、評価方法、判断基準、更新手順、通常時の更新間隔、緊急時の対処方法などを定めた規程の有無

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.1.1.6「ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。」

(3) セキュリティ (ネットワーク)

① ファイアウォール (102: 必須開示項目)

【記述内容】 ファイアウォール設置等の不正アクセスを防止する措置の有無

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.3.1.4「外部及び内部からの不正アクセスを防止する装置（ファイアウォール、リバースプロキシの導入等）を講じること。」

② ネットワーク不正侵入検知 (103: 必須開示項目)

【記述内容】 不正パケット、非権限者による不正なサーバ侵入に対する検知等の有無と、「有り」の場合は対応方法を記入ください。

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.3.1.3「利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。

また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。」

Ⅲ.3.1.5「不正な通貨パケットを自動的に発見する装置（IDSの導入等）を講じること。」

③ ネットワーク監視 (104: 選択開示項目)

【記述内容】 事業者と契約利用者との間のネットワーク（専用線等）において障害が発生した際の通報時間

【説明】 可能な範囲でご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.3.2.5「外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。」



④ ウイルスチェック（105：必須開示項目）

【記述内容】 メール、ダウンロードファイル、サーバ上のファイルアクセスに対する対処の有無、対処がある場合はパターンファイルの更新間隔（ベンダーリリースからの時間）

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.2.2.1「ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。」

⑤ ユーザ認証（106：必須開示項目）

【記述内容】 利用者に対する認証手段と方法（認証基盤を通じた個人認証、又はID、パスワード等）

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.3.1.3「利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。  
また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。」

⑥ IoT機器認証（107：必須開示項目）

【記述内容】 IoT機器のアクセスを管理するための認証方法、特定の場所及び装置からの情報を認証する方法等

【説明】 ID、パスワードによる認証、デジタル証明書による認証などIoT機器を認証する方法を記述してください。

未記入の場合は非認定となります。

⑦ 記録（ログ等）（108：必須開示項目）

【記述内容】 ネットワークの利用状況、例外処理及びセキュリティ事象の記録

(ログ等) 取得の有無、記録 (ログ等) がある場合にはその保存期間

【説明】 未記入の場合は非認定となります。

- ⑧ (参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.2.1.3「利用者の利用状況、例外処理及び情報セキュリティ事象の記録 (ログ等) を取得し、記録 (ログ等) の保存期間を明示すること。」  
無、対策がある場合は認証の方法

【説明】 未記入の場合は非認定となります。

対策例として、①専用ソフトによるアクセス監視、②他事業者による関連 サービスの利用、③認証局が発行する証明書による確認、④ID・パスワード等運用規程の整備、等をご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.3.2.3「第三社が当該事業者のサーバになりすますこと (フィッシング等) を防止するため、サーバ証明書の取得等の必要な対策を実施すること。」

#### ⑨ その他セキュリティ対策 (110: 選択開示項目)

【記述内容】 情報漏洩対策、データの暗号化等の対策について自由に記述

【説明】 可能な範囲でご記入下さい。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.3.2.2「外部ネットワークを利用し ASP・SaaS 情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。」

### 3. 6 ハウジング (サーバ設置場所) ※使用データセンター毎に記載

#### (1) 施設建築物

##### ① データセンター識別名 (111: 必須開示項目)

【記述内容】 当該データセンターの正式識別名。複数データセンターがある場合は、簡易略照明を追記 (以降の開示項目の記述で使用)

<※> ※簡易略称名とは、「A,B,C...」、「1,2,3...」など

記述例:

x x x データセンター（正式識別名）：A1センター（簡易略称名）

【説明】 未記入の場合は非認定となります。

② データセンター事業開始年（112：必須開示項目）

【記述内容】 当該データセンターの事業開始年（必須開示項目）

【説明】 未記入の場合は非認定となります。

③ 建物形態（113：必須開示項目）

【記述内容】 データセンター専用建物、オフィス建物のいずれに近いかの明示

【説明】 未記入の場合は非認定となります。

④ 所在地（114：必須開示項目／選択開示項目）

【記述内容1】 所在国名、日本の場合は地域ブロック名（例：関東、東北）

【記述内容2】 特筆すべき立地条件上の優位性があれば記述（例：標高、地盤等）

【説明】 記述内容1については、未記入の場合は非認定となります。

（記述例：地域ブロック名）北海道、東北、関東、北陸、東海、  
甲信越、近畿、中国、四国、九州等

記述内容2については、可能な範囲でご記入ください。

⑤ 耐震・免震構造（115：必須開示項目）

【記述内容1】 耐震数値（震度等）

【記述内容2】 地震対策に係る建物構造（免震、制震構造等）

【説明】 耐震数値については、建物の構造（柱や梁）自体がどの程度（耐震数値）の地震に耐えられるような強度で造られているか、についてご記入ください。

（記述例）「震度6弱まで」、「震度6強以上」

また、地震対策に係る建物構造については、制震構造、免震構造についてご記入ください。

免震構造：構造物と地盤との間に積層ゴムなどの特殊な装置を付けた免震層を造ることで、揺れの力を直接伝えな

いようにした構造のこと。

制震構造：建物が揺れ始めたとき振動を吸収し、建物を許容範囲内の振動以下に制御する構造のこと。

上記2つの記述内容のうち、1つでも未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.4.1.1「ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。」

## (2) 非常用電源設備

### ① 無停電電源（116：必須開示項目）

【記述内容】 無停電電源とするための対策（UPS設置等）の有無と、有りの場合は電力供給可能時間

【説明】 未記入の場合は非認定となります。

### ② 給電ルート（117：必須開示項目）

【記述内容】 給電ルート（系統）について、以下より選択してください。

- ① 異なる変電所から給電ルートで2ルート以上確保
- ② 同一変電所から複数の給電ルートを確保
- ③ 同一変電所・単一の給電ルート

【説明】 上記①～③を選択してください。未記入の場合は非認定となります。

### ③ 非常用電源（118：必須開示項目）

【記述内容】 非常用電源（自家発電機）の有無と、有りの場合には以下の項目をご記入ください。

- ・ 停電時から非常用電源の稼働開始までの時間
- ・ 無給油での連続稼働時間
- ・ 非常用電源稼働対策の内容（燃料の連続供給方法等）

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.4.2.1「ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講ずること。」

(3) 消火設備

① サーバルーム内消火設備 (119: 必須開示項目)

【記述内容】 自動消火設備の有無と、有りの場合はガス系消火設備（ハロンガス対応、新ガス対応の別）か否かの明示

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.3.1「サーバルームに設置されている ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。」

② 火災感知・報知システム (120: 必須開示項目)

【記述内容】 火災検知システム、煙検知システムの有無

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.3.2「ASP・SaaS 事業者は、サービス提供用機器を設置するサーバルームに火災検知・通報システム及び消火設備を備えること。ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。」

(4) 避雷対策設備

① 直撃雷対策 (121: 必須開示項目)

【記述内容】 直撃雷対策の有無

【説明】 未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.3.3「情報処理施設に雷が直撃した場合を想定した対策を講じること。」

② 誘導雷対策（122：必須開示項目）

【記述内容】 誘導雷対策の有無と、有りの場合は最大対応電圧の数値（選択）

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.3.4「情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。」

（5）空調設備

① 十分な空調設備（123：必須開示項目）

【記述内容】 空調設備の内容（床吹き上げ空調、コンピュータ専用個別空調、水冷・空冷式、その他の工夫 等）

【説明】 未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.2.2「ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。」

（6）セキュリティ

① 入退館管理等（124：必須開示項目）

【記述内容1】 入退室記録の有無と、有りの場合はその保存期間

【記述内容2】 監視カメラの有無と、有りの場合は監視カメラ稼働時間、映像の保存期間、改ざん防止機能の有無

【記述内容3】 個人認証システムの有無

【説明】 上記3つの記述内容のうち、1つでも未記入の場合は非認定となります。

（参考）「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容  
Ⅲ.4.4.1「重要な物理的セキュリティ境界（カード制御による出入り口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。」  
Ⅲ.4.4.2「重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。」

② 媒体の保管（125：選択開示項目）

【記述内容1】 磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットや保管室の有無

【記述内容2】 保管管理手順書の有無

【説明】 可能な範囲でご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.5.3.1「紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。」

③ その他セキュリティ対策（126：選択開示項目）

【記述内容】 その他特筆すべきセキュリティ対策

【説明】 可能な範囲でご記入ください。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

Ⅲ.4.4.4「重要な物理的セキュリティ境界の出入り口に破壊対策ドアを設置すること。」

Ⅲ.4.4.5「重要な物理的セキュリティ境界に警備員を常駐させること。」

### 3. 7 サービスサポート

(1) サービス窓口（苦情受付、問い合わせ）

① 連絡先(127: 必須開示項目/一定の要件を考慮すべき項目)

【記述内容1】 電話/FAX、Web、電子メール等の連絡先

【記述内容2】 代理店連絡先の有無と、「有り」の場合は、代理店名称、代理店の本店の所在地と連絡先

【記述内容3】 運用体制に係る問合せの可否

【説明】 電話/FAX、Web、電子メール等の連絡先を記述してください。

代理店連絡先の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、代理店名称、代理店の本店の所在地と連絡先についても記述してください。窓口(連絡先)を設置していない場合は非認定となります。

運用体制に係る問合せの可否について、「可」または「否」を記述してください。  
上記いずれかの項目について未記入の場合は非認定となります。

② 営業日・時間（128：必須開示項目）

【記述内容1】 営業曜日、営業時間（受付時間）

【記述内容2】 営業時間外の対応の可否

【説明】 上記2項目のうち、1つでも未記入の場合は非認定となります。

③ サポート範囲・手段（129：必須開示項目）

【記述内容1】 サポート範囲

【記述内容2】 連絡先、連絡手段（電話/FAX、電子メール等）

【説明】 上記2項目のうち、1つでも未記入の場合は非認定となります。  
連絡先が明記されていない場合は非認定となります。

(2) サービス通知・報告

① メンテナンス等の一時的サービス停止時の事前告知

(130: 必須開示項目／一定の要件を考慮すべき項目)

【記述内容1】 利用者への告知時期(1カ月前、3カ月前、6カ月前、12カ月前等の単位で記述)

【記述内容2】 告知方法

【記述内容3】 保守業務実施における事前通知の有無

【記述内容4】 保守業務実施中の緊急問合せの可否

【説明】 メンテナンス等のために一時的にサービスを停止する場合、利用者への事前告知時期及び告知方法について記述してください。事前告知を実施していない場合は非認定となります。

保守業務実施における事前通知の有無について、「有り」または、「無し」を記述してください。

保守業務実施中の緊急問合せの可否について、「可」または「否」を記述してください。

上記いずれかの記述内容が未記入の場合も非認定となります。

② 障害・災害発生時の通知(131: 必須開示項目／一定の要件を考慮すべき項目)



【記述内容1】 障害発生時通知の有無と、「有り」の場合は通知方法、及び利用者への通知時間

【説明1】 障害発生時通知の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、通知方法、及び利用者への通知時間についても記述してください。

障害発生時の通知を実施していない場合は非認定となります。

但し、サービス利用者への影響が無い障害に限り、通知を行わないことによって非認定にはなりません。

未記入の場合は非認定となります。

【記述内容2】 緊急時発生時の通知の有無・方法

【説明2】 緊急時発生時の通知の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は通知方法について記述してください。

未記入の場合は非認定となります。

(参考)「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の「見読目的に応じた応答時間」に記載されている対策内容

「ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視(応答確認等)を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること」

「ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視(サービスのレスポンス時間の監視)を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること」

### ③ セキュリティ・インシデント対応(132: 必須開示項目)

【記述内容】 セキュリティに関するインシデントが発生した場合の対応(通知、被害の拡大防止、暫定対策、本格対処など)

【説明】 セキュリティ・インシデント発生の場合の対応の有無について「有り」または、「無し」を記述してください。「有り」の場合は、対応方法を記述してください。

未記入の場合は非認定となります。

### ④ 定期報告(133: 必須開示項目)

【記述内容】 利用者への定期報告の有無(アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等)

【説明】 利用者への定期報告の有無について「有り」または、「無し」を記述してください。

未記入の場合は非認定となります。

(参考)「ASP・SaaSにおける情報セキュリティ対策ガイドライン」に記載されている対策内容

「ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等(情報セキュリティ対策機器、通信機器等)の監視結果(障害監視、死活監視、パフォーマンス監視)について、定期報告書を作成して利用者等に報告すること。」

