

IaaS・PaaS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～

特定非営利活動法人

ASP・SaaS・IoT クラウド コンソーシアム

目次

1. 申請書の記入方法について	1
2. 「事業者」に関わる項目の説明	2
2. 1 開示情報の時点	2
2. 2 事業所・事業	2
2. 3 人材	3
2. 4 財務状況	4
2. 5 資本関係・取引関係	5
2. 6 コンプライアンス	6
3. 「サービス」に関わる項目の説明	9
3. 1 サービス基本特性	9
3. 2 システム運用（システム基盤運用、セキュリティ等）	20
3. 3 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	26
3. 4 サービスサポート	31

（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。

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、必ずご記入ください。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。

なお、認定サービスについては、ASPICホームページにおいて、各必須開示項目に記述された内容をそのまま公表させていただきます。

2) 選択開示項目

選択開示項目については、情報開示される内容を任意でご記入ください。情報されない項目については未記入であっても非認定となることはありません。

なお、認定サービスについては、ASPICホームページにおいて、各選択開示項目に記述された内容をそのまま公表させていただきます。

3) 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、「18号監査（米国ではSAS70や後継のSSAE16）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。

4) 記入時の使用言語

記入時の使用言語は、日本語とします。

2. 「事業者」に関わる項目の説明

株式会社、社団法人等の公益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ご記入下さい。

(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: 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 (西暦) をご記入ください。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】 事業者の正式名称 (商号)

【説明】 貴社の登記上の正式な社名をご記入ください。未記入の場合は非認定となります。

②事業者ホームページ (3: 選択開示項目)

【記述内容】 事業者のホームページのURL

【説明】 貴社のホームページのURLをご記入ください。

③設立年・事業年数 (4: 必須開示項目)

【記述内容】 事業者の設立年 (西暦)

【説明】 貴社の設立年を西暦でご記入ください。未記入の場合は非認定となります。

④事業所 (5: 必須開示項目)

【記述内容1】 事業者の本店住所・郵便番号

【記述内容2】 事業所数（国内、国外）

【説明】 貴社の本店所在地、及び国内と国外の事業所数をご記入ください。

上記2つの記述内容の1つでも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（6：必須開示項目）

【記述内容】 事業者の主要な事業の概要（IaaS・PaaS事業以外も含む）
<100字以内>

【説明】 貴社のIaaS・PaaSに関連している事業以外も含めて、事業概要について100字以内でご記入ください。

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（7：必須開示項目／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（年齢、学歴、業務履歴、資格等）

【説明】 代表者氏名については、未記入の場合は非認定となります。また、代表者の経歴（年齢、学歴、業務履歴、資格等）は選択開示項目ですので、可能な範囲でご記入ください。

②役員（8：選択開示項目）

【記述内容】 役員数

【説明】 貴社の役員数についてご記入ください。

（2）従業員

①従業員数（9：選択開示項目）

【記述内容】 正社員数（単独ベース）

【説明】 貴社の正社員数（単独ベース）をご記入ください。

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（10：必須開示項目）

【記述内容】 事業者全体の売上高（単独ベース）

【説明】 貴社の直近決算期の損益計算書における売上高（単独ベース）を円単位でご記入ください。

未記入の場合は非認定となります。

② 経常利益（11：選択開示項目）

【記述内容】 事業者全体の経常利益額（単独ベース）

【説明】 貴社の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）を円単位でご記入ください。

③ 資本金（12：必須開示項目）

【記述内容】 事業者全体の資本金（単独ベース）

【説明】 貴社の直近決算期の貸借対照表の資本金（単独ベース）を円単位でご記入ください。

未記入の場合は非認定となります。

④ 自己資本比率（13：選択開示項目）

【記述内容】 事業者全体の自己資本の比率（単独ベース）

【説明】 貴社の直近決算期の自己資本比率を下式により算定し、ご記入（単位：％）ください。

$$\text{自己資本比率} = \frac{\text{自己資本}}{\text{総資産}}$$

(2) 財務信頼性

① 上場の有無（14：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】 貴社が株式上場をしているか否かについてご記入ください。また、上場している場合は、その市場名（例：東証1部、JASDAQ）をご記入ください。

② 財務監査・財務データの状況（15：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、以下により選択

- ① 会計監査人による会計監査
- ② 会計参与による監査
- ③ 中小企業会計によるチェックリストに基づく財務データ
- ④ いずれでもない

【説明】 該当する財務監査・財務データの状況を上記、①～④の中から選択し、ご記入ください。

③ 決算公告（16：選択開示項目）

【記述内容】 決算公告の実施の有無

【説明】 貴社の決算公告の実施について、「有り」または「無し」でご記入ください。

2. 5 資本関係・取引関係

(1) 資本関係

①株主構成（17：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】 貴社が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ご記入ください。

(2) 取引関係

①主要取引金融機関（18：選択開示項目）

【記述内容】 主要取引金融機関の名称

【説明】 貴社の主要な取引金融機関の名称（銀行名、信用金庫名等）をご記入ください。

②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】 貴社が現在所属している主な業界団体、経済団体等の名称をご記入

ください。

2. 6 コンプライアンス

(1) 組織体制

① 専担の部署・会議体 (20: 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、部署等がある場合には社内の部署名・会議名

【説明】 貴社の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) がある場合には、その名称をご記入ください。

(2) 文書類

① 情報セキュリティに関する規程等の整備 (21: 必須開示項目)

【記述内容1】 情報セキュリティに関する基本方針・規程・マニュアル等文書類の名称

【記述内容2】 上記の文書類の経営陣による承認の有無

【説明】 情報セキュリティに関する基本方針・規程・マニュアル等の名称、及び経営陣による承認の有無をご記入ください。上記2つの記述内容が1つでも未記入の場合は非認定となります。情報セキュリティに関する規程等の整備がされていない場合は、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、セキュリティ対策 (ネットワーク等外部侵入対策、ウイルス対策、情報漏洩対策を含む) 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とします。

(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 IaaS・PaaSサービスの苦情対応に関する規程等の整備（22：必須開示項目）

【記述内容1】 IaaS・PaaSサービスの苦情処理に関する基本方針・規程・マニュアル等の有無と、文書類がある場合はそれらの文書名

【記述内容2】 上記の文書類の経営陣による承認の有無

【説明】 IaaS・PaaSのサービスの苦情処理に関する基本方針・規程・マニュアル等がある場合、その名称及び経営陣による承認の有無をご記入ください。

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とします。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類があるか否かを記述していただきます。

上記2つの記述内容が1つでも未記入の場合は非認定となります。

③ 事業継続に関する規定等の整備（23：必須開示項目）

【記述内容1】 事業継続に関する基本方針、計画、マニュアル等の文書類の有無と、有りの場合は文書類の名称

【記述内容2】 上記の文書類の経営陣による承認の有無

【説明】 事業継続に関する規程等の整備状況についてご記入ください。

なお、ここでいう事業継続に関する基本方針、計画、マニュアル等とは、危機・災害等の不測の事態が発生した際に事業継続を行うための、組織体制、事前準備、災害発生時の対応方法などを規定した実行計画が記述されている文書類とします。

上記2つの記述内容が1つでも未記入の場合は非認定となります。

④ リスク管理に関する規程等の整備（24：必須開示項目）

【記述内容1】 リスク管理に関する基本方針、計画、マニュアル等の文書類の有無と、有りの場合は文書類の名称

【記述内容2】 上記の文書類の経営陣による承認の有無

【説明】 リスク管理に関する規程等の整備状況について、ご記入ください。

なお、ここでいうリスク管理に関する基本方針、計画、マニュアル等とはリスク管理を行うための、組織体制、事業遂行に関わる管理すべきリスクとリスク対策に係る行動計画等が記述されている文書類とします。

上記2つの記述内容が1つでも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 サービス基本特性

(1) サービス概要

① サービス名称 (25: 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 (26: 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 (27: 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400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 サービスの基本タイプ (28: 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）

⑤ サービスのカスタマイズ範囲（29：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。

⑥ 提供回線・帯域（30：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（31：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 (32: 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 (33: 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 管理者接続用ネットワーク提供サービス (34: 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。

⑤ バックアップ・リストアサービス (35: 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。

⑥ その他サービス (36: 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 (37: 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（38：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（39：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（40：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（41：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（42：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（43：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（44：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（45：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（46：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（47：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（48：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 その他サービス（49：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。

（7） サービス品質

① サービス稼働設定値（50：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。

○サービス提供時間＝[契約サービス時間]
－[事前通知された定期保守によるサービス停止時間]

○サービス稼働時間＝[サービス提供時間]
－[事前通知のないサービス停止時間]

○サービス稼働率＝[サービス稼働時間]／[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。

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、認定取得日以降から更新申請日まで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 DR (Disaster Recovery) への対応 (51: 必須開示項目)

【記述内容1】 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）

【説明1】 未記入の場合は非認定となります。なお、記述内容1では、データのみバックアップを行っている場合についてご記入ください。データを含むシステムのバックアップを行っている場合は、記述内容2にご記入ください。

(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

【記述内容2】 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2】 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

③ サービスパフォーマンスの管理 (52: 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。」

④ サービスパフォーマンスの増強（53：選択開示項目）

【記述内容】 ネットワーク・機器等の増強判断基準あるいは計画の有無、判断基準や計画がある場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要

【説明】 可能な範囲でご記入ください。

⑤ 認証取得、監査実施（54：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。

⑥ 個人情報の取扱い（55：必須開示項目）

【記述内容】 個人情報を収集する際の利用目的の明示

【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.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。」

⑦ 脆弱性診断（56：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。」

⑧ バックアップ対策 (57: 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。」

⑨ バックアップ管理 (58: 必須開示項目)

【記述内容】 バックアップ確認のインターバル

【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.2.3.2「バックアップをされた情報が正常に記録され、正しく読みだすことができるかどうかについて定期的に確認すること。」

⑩ 受賞・表彰歴 (59: 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。

⑪ SLA (サービスレベル・アグリーメント) (60: 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。

(8) 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（61：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（62：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 サービス（事業）変更・終了に係る問合せ先（63：必須開示項目）

- 【記述内容】 問合せ先（通常の苦情等の問合せ窓口も含む）の有無、問合せ先がある場合は名称・受付時間
- 【説明】 未記入の場合は非認定となります。

(9) サービス料金・解約

① 課金方法 (64: 必須開示項目)

【記述内容】 従量部分、固定部分別の課金方法

【説明】 申請したサービスの利用者への課金方法について、従量部分と固定部分に分けて、具体的にわかりやすく記入してください。なお、該当する課金方法がない場合は、その旨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 料金体系・金額 (65: 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。

③ 支払方法 (66: 必須開示項目)

【記述内容】 クレジットカード決済、電子マネー決済等の支払い方法

【説明】 支払方法をご記入ください。未記入の場合は非認定となります。

④ 解約時ペナルティ (67: 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。

⑤ 利用者からの解約事前受付期限 (68: 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。

(10) サービス利用量

① 利用者数 (69: 選択開示項目)

【記述内容】 情報開示したIaaS・PaaSサービスの利用者ライセンス数（同時接続利用者数か、実利用者数かも明示）

【説明】 可能な範囲でご記入ください。

② 代理店数（70：選択開示項目）

【記述内容】 情報開示したIaaS・PaaSサービスの取扱い代理店数

【説明】 可能な範囲でご記入ください。

（1 1）データ管理

① データの所在（71：必須開示項目）

【記述内容】 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（72：必須開示項目）

【記述内容】 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. 2 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）（73：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）（74：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.1.1.1.2「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（75：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（76：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（77：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 記録（ログ等）（78：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。」

④ ID・パスワードの運用管理（79：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。」

⑤ セキュリティパッチの管理（80：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（81：必須開示項目）

【記述内容】 ファイアウォールの有無

【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）を講ずること。」

② ネットワーク不正侵入検知（不正パケット、サーバへの不正侵入）

（82：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）を講ずること。」

③ ネットワーク監視（83：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（84：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（85：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 記録（ログ等）（86：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。

（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。」

⑦ なりすまし対策（事業者サイド）（87：必須開示項目）

【記述内容】 第三者による自社を装ったなりすましに関する対策の実施の有無、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。」

⑧ その他セキュリティ対策（88：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. 3 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) 建物

① データセンター識別名（89：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（90：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 建物専用形態（91：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（92：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（93：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) 電源設備

① 無停電電源(94: 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(95: 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（96：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じること。」

（3）消火設備

① サーバルーム内消火設備（97：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（98：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ールームに火災検知・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ールームには、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 (99：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 (100：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 (101：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 (102: 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 (103: 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（104：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. 4 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 営業日・時間（105：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。

② サポート範囲・手段（106：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) サービス保証・継続

① 事故発生時の責任と補償範囲（107：必須開示項目）

【記述内容】 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、有る場合はその文書名称

【説明】 未記入の場合は非認定となります。

(3) 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（108：必須開示項目）

【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】 上記記述（記述内容1）よりも短い告知時期での緊急メンテナンスの有無

【説明】 メンテナンス等により一時的にサービスを停止する場合に、利用者へ事前に通知する時期及び通知方法（書面、メール等）、並びに緊急メンテナンスの有無についてご記入ください。

上記3項目のうち、1つでも未記入の場合は非認定となります。また、メンテナンス等の一時的サービス停止時の事前告知がない場合は非認定となります。

② 障害・災害発生時の通知（109：必須開示項目）

【記述内容】 障害発生時通知の有無

【説明】 未記入の場合は非認定となります。サービスの停止等、利用者へ大きな影響を及ぼす障害発生時に通知がない場合は非認定となります。

③ 定期報告（110：必須開示項目）

【記述内容】 利用者への定期報告の有無

【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.1.1.7「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。」