# ASP・SaaS 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

目　次



（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。

変更履歴:

平成20年5月15日:
節3.1(4)④認証取得・監査実施: ITSMSの例示のJIS番号を訂正しました。
節3.2(3)⑤記録(ログ): (参考)内のセキュリティ対策ガイドライン引用先、引用内容を訂正しました。

平成21年2月17日:
節3.2(3)①死活監視:【説明】説明文書を追加しました。
節3.2(3)④ウイルスチェック:【説明】説明文書を追加しました。
節3.2(3)⑤記録(ログ等):【説明】説明文書を追加しました。
節3.2(3)⑥セキュリティパッチ管理:【説明】説明文書を追加しました。
節3.4(5)①十分な空調設備:必須を選択に訂正しました。

平成24年4月1日
全般 財団法人を一般財団法人へ変更しました。
全般 法人名略称をセンターから財団に変更しました。

平成24年8月31日
全般 文字タイプを整理しました。

平成29年10月1日
節1 一般財団法人マルチメディア振興センターを認定機関に変更しました。

令和元年6月1日
1. 申請書の記入方法について 3)選択開示項目 について申請書Bの“申請内容”欄は申請者が記述した内容をそのまま公表することに変更しました。

令和2年4月1日
クラウドサービス情報開示認定機関を特定非営利活動法人 ASP・SaaS・IoT クラウド コンソーシアムからに一般財団法人 ASP・SaaS・AI・IoT クラウド産業協会に変更しました。

令和4年4月1日
クラウドサービス情報開示認定機関の法人名称を一般財団法人ASP・SaaS・AI・IoT クラウド産業協会から「一般社団法人日本クラウド産業協会」に変更しました。

## 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。

### 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ご記入ください。

### 3）選択開示項目

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

なお、認定機関ホームページにおいて、申請書 B の“申請内容”欄については申請者が記述した内容をそのまま公表します。添付書類等”欄については公表しません。

### 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、「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。

### 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。

## 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。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、記入し、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。」等とご記入ください。

（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: 必須開示項目)

【記述内容】　開示情報の年月日

【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設立年・事業年数(3: 必須開示項目)

【記述内容1】 事業者の設立年(西暦)

【説明1】 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。

【記述内容2】 設立後の事業年数

【説明2】 設立後の事業年数をご記入ください。なお、1年に満たない事業年数は月数でご記入下さい。

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】 事業者の本店住所・郵便番号

【記述内容2】 事業所数

【記述内容3】 主な事業所の所在地

【説明】 貴社の本店所在地、国内と国外の事業所数、及び主な事業所の所在地をご記入下さい。
上記3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（5: 必須開示項目）

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

【説明】 貴社の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（6: 代表者氏名は必須開示項目、他は選択開示項目）

【記述内容1】 代表者氏名

【記述内容2】 代表者の写真

【記述内容3】 年齢

【記述内容4】 経歴（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、代表者の写真・年齢・経歴（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（7: 選択開示項目）

【記述内容1】 役員数

【記述内容2】 役員氏名及び役職名

【説明】 貴社の役員について、役員数、氏名及び役職名をご記入ください。

(2)従業員

①従業員数(8: 選択開示項目)

【記述内容】 正社員数

【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(9: 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。また、決算期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経常利益(10: 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。また、決算期を記入してください。

③資本金(11: 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。また、決算期を記入してください。
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、ご記入ください。

また、決算期を記入してください。

自己資本比率＝[自己資本]／[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】 事業者全体のキャッシュ・フロー対有利子負債比率(単独ベース)

【説明】 貴社の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、ご記入ください。また、決算期を記入してください。

キャッシュ・フロー対有利子負債比率

＝[有利子負債]／[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】 事業者全体のインタレスト・カバレッジ・レシオ(単独ベース)

【説明】 貴社の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、ご記入ください。また、決算期を記入してください。

インタレスト・カバレッジ・レシオ

＝[営業キャッシュ・フロー]／[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、株式上場の場合は市場名

【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(16: 選択開示項目)

【記述内容】 会計監査人による会計監査、会計参与による監査、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、いずれでもない、の中から該当状況を選択

【説明】 貴社の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、ご記入ください。

①会計監査人による会計監査に基づく財務データ

②会計参与による監査に基づく財務データ

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いずれでもない財務データ

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】 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（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】 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大口取引先（19: 選択開示項目）

【記述内容】 大口取引先の名称

【説明】 貴社の主要な取引先の名称（会社名、機関名等）をご記入ください。

②主要取引金融機関（20: 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。

③所属団体（21: 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コンプライアンス担当役員（22: 選択開示項目）

【記述内容】 コンプライアンス担当の役員氏名

【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、その氏名をご記入ください。

なお、ここでの役員は、会社法で規定されている取締役、執行役だけでなく、執行役員も含みます。

②専担の部署・会議体（23: 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

（24: 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、また、経営陣の承認を得た情報セキュリティに関する基本方針・規程・マニュアル等のいずれかを有する水準に満た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、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勧誘・販売に関する規定等の整備（25: 選択開示項目）

【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、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】 勧誘・販売に関する基本方針・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、これらの勧誘・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とします。

③ASP・SaaSの苦情対応に関する規程等の整備（26: 必須開示項目）

【記述内容1】 ASP・SaaS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】 ASP・SaaS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ASP・SaaS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.「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）サービス内容

①サービス名称（27: 必須開示項目）

【記述内容】 申請したASP・SaaSのサービス名称

【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（28: 必須開示項目）

【記述内容1】 申請したASP・SaaSのサービス開始年月日（西暦）

【記述内容2】 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実施の有無と、行われた場合はリニューアル年月日（西暦）

【説明】 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サービスの基本タイプ（29: 必須開示項目）

【記述内容】 アプリケーションサービス、ネットワーク基盤サービス、ASP基盤サービス、その他サービスの4つの中から該当タイプを選択

【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をご記入ください。
未記入の場合は非認定となります。

○ アプリケーションサービス
業種別・分野別のアプリケーションを提供するASP・SaaS
（例：受発注、CRM・営業支援、販売支援、人事管理・勤怠管理、経理、eラーニング、ECサポート　等）

○ ネットワーク基盤サービス
VPNやコールセンター機能を、専用ソフト・ハードを使わずに提供するASP・SaaS
（例：VPN、IPセントレックス、コールセンター／コンタクトセンター、音声通話、オンライン支援、統合サービス　等）

○ ASP基盤サービス
社会的な共通アプリケーション（例：ブログ、コンテンツ管理・配信、Web会

議システム等）、個々のアプリケーションを実現する際に必要となる機能（例：認証機能、文書管理機能等）、システムの基盤となる機能（例：ウイルス対策、暗号化、情報漏洩防止等）を提供するASP・SaaS

○ その他サービス

上記のいずれにも属さないASP・SaaS

④サービスの内容・範囲（30: 必須開示項目）

【記述内容1】 申請したASP・SaaSのサービスの内容・特徴＜500字以内で記述＞

【記述内容2】 他の事業者との間でサービス連携を行っていることの有無と、ある場合はその内容　＜前記述と合せて500字以内で記述＞

【説明】 申請したサービスの内容・特徴、他の事業が提供するサービスとの連携の内容等について、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。

⑤サービスのカスタマイズ範囲（31: 必須開示項目）

【記述内容】 アプリケーションのカスタマイズの範囲 （契約内容に依存する場合はその旨記述）＜200字以内で記述＞

【説明】 顧客の要望に応じたアプリケーションのカスタマイズが可能な機能、内容、範囲等について200字以内でご記入ください。「特に決まっていない」、「個別相談に応じて決める」等の場合は、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）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

（32: 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（事前告知の時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）

【記述内容2】告知方法

【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つの記述内容が1つでも未記入の場合は非認定となります。

また、サービス（事業）変更・終了時の利用者への事前告知時期が1ヶ月未満となる

水準の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(33: 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と、基本方針がある場合はその概略

【記述内容2】 基本方針に沿った具体的なユーザへの対応策(代替サービスの紹介等)の有無と、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1つでも記入が無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

II.4.1.1「取り扱う各情報資産について、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
(34: 必須開示項目/一定の要件を考慮すべき項目)

【記述内容】 問合せ先(通常の苦情等の問合せ窓口も含む)の有無と、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。また、サービス(事業)変更・終了に係る問合せ先が無い場合も非認定となります。

(3)サービス料金

①課金方法(35: 必須開示項目)

【記述内容1】 従量部分の課金方法

【記述内容2】 固定部分の課金方法

【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。
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料金体系(36: 必須開示項目)

【記述内容1】 初期費用額

【記述内容2】 月額利用額

【記述内容3】 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契約期間をご記入ください。

上記3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。

③解約時ペナルティ(37: 必須開示項目)

【記述内容】 解約時違約金(ユーザ側)の有無と、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。

④利用者からの解約事前受付期限(38: 必須開示項目)

【記述内容】 利用者からのサービス解約の受付期限の有無と、有りの場合はその期限(何日・何ヶ月前かを記述)

【説明】 未記入の場合は非認定となります。

(4)サービス品質

①サービス稼働設定値(39: 必須開示項目)

【記述内容1】 サービス稼働率のこれまでの実績値、またはやむなき理由により実績値が記載できない場合はその理由と目標値

【説明1】 申請したサービスについてのサービス提供時間、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]

○サービス稼働率 ＝([サービス提供時間]－[事前告知のないサービス停止時間]) ／ [サービス提供時間]

なお、事前告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。

目標値の使用については、実績値を記入できない理由を記入したときのみ認められます。また、更新申請時に目標値を記入することはできません。
未記入の場合は非認定となります。

【記述内容2】 申請したサービスが該当する「情報セキュリティ対策ガイドライン」におけるサービス種別のパターン番号と稼働率の対策参照値

【説明2】 申請したサービスに対し、ASP・SaaSのサービス種別を判定いただき、該当するパターン番号と対応する稼働率の対策参照値をご記入ください。サービス種別は図表1、2等を用いて申請者が確定させていただき、該当するパターン番号に対応する図表3の対策参照値を用いていただきます。ここで、図表1～3は、「ASP・SaaS情報セキュリティ対策ガイドライン」の内容をもとに作成しています。
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3】 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。
- 更新申請時においても、更新申請日までの直近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。

図表１　ASP・SaaS のサービスに対するパターン番号の決定ルール

| パターン | 機密性への要求 | 完全性への要求 | 可用性への要求 |
|---|---|---|---|
| 1 | 高 | 高 | 高 |
| 2 | 高 | 高 | 中 |
| 3 | 高 | 高 | 低 |
| 4 | 低 | 高 | 高 |
| 5 | 低 | 高 | 中 |
| 6 | 低 | 高 | 低 |

（注 1）ASP・SaaS 事業者が提供するサービスは、基幹系業務システムからグループウェアに至るまで多岐に渡っており、その取り扱う情報の違いから、各 ASP・SaaS のサービスに要求される「機密性」「完全性」「可用性」のレベルも必然的に異なってくる。そこで、本ガイドラインでは、ASP・SaaS のサービス種別を「機密性」「完全性」「可用性」の観点から、その特性ごとに 6 パターンに分類している。

（注 2）「機密性」への要求の高低に関する考え方は次のとおり。

以下の情報を扱う場合には、その件数に関わりなく、機密性への要求は「高」いものとする。

①個人情報：利用者及び利用者の顧客に関する、特定の個人を識別することができる情報。

②営業秘密情報：秘密として管理されている生産方法、販売方法、その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの。

（注 3）「完全性」への要求の高低に関する考え方は次のとおり。

ASP・SaaS 事業者が利用者のデータを管理するという特性上、そのデータに改ざん・削除等のインシデントが発生した場合、顧客の事業継続に多大な影響を与えるものと考えられる。また、ASP・SaaS 事業者が提供する情報においても、その情報に改ざん等のインシデントが発生した場合、その情報に依存している顧客にとって大きな損害が発生することが想定される。したがって、ASP・SaaS 事業者においては、そのサービス種別に関わらず、完全性への要求は「高」いものと考えられる。

（注 4）「可用性」への要求の高低に関する考え方は次のとおり。

①可用性への要求が「高」いサービス

a 運用時間中は原則として必ず稼働させておくことが求められるサービス

b サービスが停止することで、利用者に多大な経済的損失や人命危害が生じる恐れのあるサービス

②可用性への要求が「中」程度のサービス

a サービスが停止することで、利用者に部分的な経済的損失が生じる恐れのあるサービス

b サービスが停止することで、利用者の基幹業務に明確な影響を及ぼすサービス

③可用性への要求が「低」いサービス：　①②以外のサービス

図表2 パターンごとのサービス種別の分類例

| パターン | サービス種別 |
|---|---|
| 1 | 受発注、人事給与・勤怠管理・経理、ERP（財務会計等）、EC サポート（電子商取引のアウトソーシング）、ネットショッピング支援（仮想店舗貸しサービス）、コールセンター支援、金融業特化型サービス（地銀・信金共同アウトソーシング）、医療・介護・福祉業特化型サービス、電子入札、公共住民情報、決済サービス、不正アクセス監視 |
| 2 | 販売管理・売掛金管理、公共窓口業務、在庫管理、建設業特化型サービス、卸売・小売・飲食業特化型サービス、保険業特化型サービス（生命保険見積）、宿泊業特化型サービス、公共電子申請、公共個別部門業務、グループウェア、アドレス帳サービス、位置時間証明サービス |
| 3 | 購買支援、CRM（顧客管理）・営業支援、販売支援、契約、採用管理、資産管理、ネットショッピング（自らの売買支援）、金融業特化型サービス（信用情報提供）、保険業特化型サービス（自賠責保険見積）、アフィリエイト、メール配信 |
| 4 | ネットワーク監視 |
| 5 | EC サポート（産地直送等、物流・決済を一括で提供） |
| 6 | 広告、IT 資産管理、ニュースリリース業務、運輸業特化型サービス、電話会議・TV 会議・Web 会議、乗り換え、不動産物件検索、検索サービス（一般向け） |
| ※一律にパターンを設定することが困難なサービス | e ラーニング・LMS、文書管理、オンラインストレージ、ワークフロー、Web サイトのホスティング、ブログ・コミュニティコーディネート、コンテンツデリバリー・ストリーミングサービス、GIS（地図情報システム）/GIS 応用、映像監視、メディア・言語変換サービス、検索サービス（個別用途）、認証サービス、セキュリティサービス |

（注）ここでは、典型的な ASP・SaaS のサービスについて、その特性を考慮してパターンごとに分類した結果を示した。なお、ここでは全ての ASP・SaaS のサービスの特性を網羅しているものではない。したがって、自らが提供する ASP・SaaS のサービスが、ここで分類されているパターンにそぐわない場合、図表中に存在しない場合、「一律にパターンを設定することが困難なサービス」に該当する場合等は、該当するパターンを独自に判定し申請する必要がある。

図表3 ASP・SaaS が提供するサービスの稼働率

| パターン | 対策参照値 |
|---|---|
| 1 | 99.5%以上* |
| 2 | 99%以上* |
| 3 | 95%以上* |
| 4 | 99.5%以上* |
| 5 | 99%以上* |
| 6 | 95%以上* |

（注）*は、特に達成することが必要であると考えられる値

（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（40: 選択開示項目）

【記述内容1】 機器、ソフトウェア等のシステム障害によるサービス応答速度の低下等の検知方法
（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）

【記述内容2】 サービス応答速度等のサービスパフォーマンスの正常性の把握方法
（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）

（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サービスパフォーマンスの増強（41: 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

④認証取得・監査実施（42: 選択開示項目）

【記述内容】 プライバシーマーク、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の取得、18号監査（米ではSAS70）の監査報告書作成の有無、上記がある場合は認証名あるいは監査の名称

⑤個人情報の取扱い（43: 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。」

⑥脆弱性診断（44: 選択開示項目）

【記述内容1】 診断の対象（アプリケーション、OS、ハードウェア等）

【記述内容2】 診断の頻度、診断の結果から対策が必要となった部分に対する対応状況（対象ごとに）

（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ぜい弱性診断を行い、その結果に基づいて対策を行うこと。」

⑦バックアップ対策（45: 必須開示項目）

【記述内容1】 バックアップ実施インターバル

【記述内容2】 世代バックアップ（何世代前までかを記述）

【説明】 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。

（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。」

**⑧バックア**ップ管理（46: 選択開示項目）

【記述内容】 バックアップ確認のインターバル

（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「バックアップされた情報が正常に記録され、正しく読み出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。」

⑨受賞・表彰歴（47: 選択開示項目）

【記述内容】 ASP・SaaSに関連する各種アワード等の受賞歴

⑩SLA（サービスレベル・アグリーメント）（48: 必須開示項目）

【記述内容】 本審査基準に含まれる開示項目がSLAとして契約書に添付されるか否か

【説明】 ここでいうSLAとは、以下のいずれでも可とします。

- 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
- 「ASP・SaaSの安全・信頼性に係る情報開示認定制度」の審査対象項目（情報開示項目）の中で以下に示す項目に関する合意事項
- 「SaaS向けSLAガイドライン」（経済産業省）に示される項目に関する合意事項

未記入の場合は非認定となります。

「ASP・SaaS の安全・信頼性に係る情報開示認定制度」審査対象項目（情報開示項目）の中で SLA の対象となる項目：

＜サービス基本特性＞
サービス内容、サービスの変更・終了、サービス料金、サービス品質

＜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＞
セキュリティ

＜ネットワーク＞
回線、セキュリティ

＜ハウジング（サーバの設置場所）＞
施設建築物、非常用電源設備、消火設備、避雷対策設備、空調設備、セキュリティ

＜サービスサポート＞
サービス窓口（苦情受付）、サービス保証・継続、サービス通知・報告

（5）サービス利用量

①利用者数（49: 選択開示項目）

【記述内容】 申請したASP・SaaSのサービスの利用者ライセンス数、および該当企業数 （同時接続ユーザ数か、実ユーザ数かを明示のこと）

②代理店数（50: 選択開示項目）

【記述内容】 申請したASP・SaaSのサービスの取扱い代理店数

## 3．2 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

（1）内容

①サービスを実現する主要ソフトウェア（51: 必須開示項目）

【記述内容1】 サービスを実現する主要ソフトウェアの名称

【記述内容2】 主要ソフトウェアの概要

【説明】 未記入の場合は非認定となります。概要は200字以内で記述してください。

②主要ソフトウェアの提供事業者（52: 必須開示項目）

【記述内容】 主要ソフトウェアの提供事業者名

【説明】 未記入の場合は非認定となります。

（2）連携・拡張性

①他システム等との連携方法（53: 選択開示項目）

【記述内容1】 標準的なAPI等を他システム等連携のために使用している場合、そのAPI等の名称

【記述内容2】 標準的でないAPI等を他システム等連携のために使用している場合、そのAPI等の公表の可否

（3）セキュリティ

①死活監視（ソフトウェア、機器）（54: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容1】 死活監視の有無と「有」の場合は、死活監視対象（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）ごとの監視インターバル

【記述内容2】 障害時の利用者への通知時間

【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を検知した後、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。

死活監視を実施していることが認定の条件であり、実施していない場合は非認定となります。

・監視インターバルの記述は任意です。

・障害時の利用者への通知時間の記述は必須です。

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。

（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（ソフトウェア、機器）（55: 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（56: 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。」

④ウイルスチェック（57: 必須開示項目／一定の要件を考慮すべき項目）

【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と、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。

・ウイルスチェック対策が無い場合も非認定となります。

・パターンファイルの更新間隔の記述は任意です。

・他の方法によりウイルスチェックを実施している場合は「実施あり」と記述してください。

（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.2.2.1「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記録（ログ等）（58: 必須開示項目／一定の要件を考慮すべき項目）

【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）取得の有無と、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。

記録（ログ等）取得を実施していることが認定の条件であり、実施していない場合は非認定となります。

・保存期間の記述は任意です。

（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。」

⑥セキュリティパッチ管理（59: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容】 パッチの更新間隔（ベンダーリリースからパッチ更新開始までの時間）

【説明】 未記入の場合は非認定となります。

パッチ管理を実施していることが認定の条件であり、実施していない場合は非認定となります。

・パッチ更新開始までの時間の記述は任意です。

（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ぜい弱性に関する情報（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。」

## 3．3　ネットワーク

### (1)回線

①推奨回線(60: 必須開示項目)

【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

【記述内容2】 ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲

【説明】 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。

> (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.3.2.4「利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル(特に、通信容量とトラヒック変動が重要)及び管理上の要求事項を特定すること。」

②推奨帯域(61: 必須開示項目)

【記述内容】 推奨帯域の有無と、推奨帯域がある場合はそのデータ通信速度の範囲

【説明】 未記入の場合は非認定となります。

③推奨端末(62: 必須開示項目)

【記述内容1】 パソコン、携帯電話等の端末

【記述内容2】 OSの種類、利用するブラウザの種類

【説明】 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)セキュリティ

①ファイアウォール設置等(63: 必須開示項目／一定の要件を考慮すべき項目)

【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。
　また、ファイアウォール措置を実施していることの水準に満たない場合も非認定となります。

（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措置（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不正侵入検知（64: 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「不正な通過パケットを自動的に発見する措置（IDS の導入等）を講じること。」

③ネットワーク監視（65: 選択開示項目）

【記述内容】 事業者とエンドユーザ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

（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。」

④ID・パスワードの運用管理（66: 必須開示項目 / 一定の要件を考慮すべき項目）

【記述内容】 IDやパスワードの運用管理方法の規程の有無

【説明】 未記入の場合は非認定となります。
また、規程が存在していることの水準に満たない場合も非認定となります。

なお、運用管理方法の規程等を認定の審査書類として当センターにご提出いただきます。（認定審査に限ってのみ使用します。）

（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

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。」

⑤ユーザ認証（67: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容】 ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所や装置からの接続を認証する方法等

【説明】 未記入の場合は非認定となります。
また、ユーザ認証を実施していることの水準に満たない場合も非認定となります。

（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.3.1.2「情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。」
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管理者認証（68: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容】 サーバ運用側（サービス提供側）の管理者権限の登録・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。
また、手順が存在していることの水準に満たない場合も非認定となります。

なお、手順を示した規程等を認定の審査書類として当センターにご提出いただきます。(認定審査時のみ使用し、第三者への公開はいたしません)。

(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。」

⑦なりすまし対策(事業者サイド)(69: 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と、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.3.2.3「第三者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(70: 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を記述
(情報漏洩対策、データの暗号化等)

【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.3.2.2「外部ネットワークを利用した情報交換において、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。」

## 3．4　ハウジング（サーバ設置場所）

### （1）施設建築物

①建物形態（71: 必須開示項目）

【記述内容】 データセンター専用建物か否か

【説明】 未記入の場合は非認定となります。

②所在地（72: 必須開示項目）

【記述内容】 国名、日本の場合は地域ブロック名（例：関東、東北）

【説明】 未記入の場合は非認定となります。

③耐震・免震構造（73: 必須開示項目）

【記述内容1】 耐震数値

【記述内容2】 免震構造や制震構造の有無

【説明】 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。

> （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（74: 必須開示項目）

【記述内容】 無停電電源装置（UPS）の有無と、UPSがある場合は電力供給時間

【説明】 未記入の場合は非認定となります。

②給電ルート（75: 必須開示項目）

【記述内容】 別の変電所を経由した給電ルート（系統）で2ルート以上が確保されているか否か
（自家発電機、UPSを除く）

【説明】 未記入の場合は非認定となります。

③非常用電源（76: 必須開示項目）

【記述内容】 非常用電源（自家発電機）の有無と、非常用電源がある場合は連続稼働時間の数値

【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（77: 必須開示項目）

【記述内容】 自動消火設備の有無と、ある場合はガス系消火設備か否か

【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（78: 必須開示項目）

【記述内容】 火災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（79: 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（80: 必須開示項目）

【記述内容】 誘導雷対策の有無、対策がある場合は最大対応電圧の数値

【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（81: 選択開示項目）

【記述内容】 空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容

（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（82: 必須開示項目）

【記述内容1】 入退室記録の有無と、入退室記録がある場合はその保存期間

【記述内容2】 監視カメラの有無と、カメラがある場合は監視カメラ稼働時間、監視カメラの監視範囲、映像の保存期間

【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１つでも記入が無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.4.4.1「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（83: 必須開示項目）

【記述内容】 紙、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の有無と、保管管理手順書の有無

【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.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（84: 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を自由に記述
（破壊侵入防止対策、防犯監視対策等）

【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。」

## 3．5　サービスサポート

### (1)サービス窓口(苦情受付)

①連絡先(85: 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】 代理店がサポート窓口となる場合、その名称、本店所在地、本店連絡先

【説明】 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。
また、窓口(連絡先)を設置していることの水準に満たない場合も非認定となります。

②営業日・時間(86: 必須開示項目)

【記述内容】 営業曜日、営業時間(受付時間)、及びメンテナンス実施時間

【説明】 未記入の場合は非認定となります。
コールセンターのように情報システムに基づいて窓口対応している場合は、情報システムのメンテナンスが発生するので記述していただまきす。そうでない場合(単に担当者が窓口対応する場合等)は、メンテナンスは発生しないと想定されますので、その旨を記述してください。

③サポート対応(87: 選択開示項目)

【記述内容1】 サービスサポートの稼働率の実績値(単位%)

【説明1】 サービスサポートの稼働率は、下式を用いてください。
サービスサポートの稼働率＝[窓口が実際稼働した時間]
／[サービスサポートの対象時間]

【記述内容2】 サービスサポートの放棄率の実績値(単位%)

【説明2】 放棄率については以下の数値を用いてください。
放棄率 ＝ [着信電話に出られなかった割合(オペレータービジー)]

【記述内容3】 サービスサポートの応答時間遵守率の実績値(単位%)

【説明3】 応答時間遵守率については下式を用いてください。
応答時間遵守率(%)＝([オペレーターが決められた時間内に応答したコール数]／[全コール数])×100

【記述内容4】 サービスサポートの基準時間完了率の実績値(単位%)

【説明4】 基準時間完了率については以下の数値を用いてください。
基準時間完了率(%)＝([サービス窓口やサービス種別ごとに定められた基準

時間内に完了した件数]／[全要求件数]）×100

【上記4つの記述内容に共通した説明】

・サービス窓口やサービス種別ごとに定められた基準時間についても併せてご記入ください。

・なお、実績値を記入することと、計測期間は直近1年とすることを原則とします。ただし、新規申請時に、サービス開始から1年に満たない場合は、開始から申請日までの期間の数値を記入してください。

④サポート範囲・手段（88: 必須開示項目）

【記述内容1】 サポート範囲

【記述内容2】 サポート手段（電話、電子メールの返信等）

【説明】 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)サービス保証・継続

①サービスダウンしない仕組み（89: 必須開示項目）

【記述内容】 サービスが停止しない仕組み（冗長化、負荷分散等）

【説明】 未記入の場合は非認定となります。

②事故発生時の責任と補償範囲（90: 必須開示項目）

【記述内容】 ASP・SaaS事業者の事故責任の範囲と補償範囲が記述された文書等の有無、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

（91: 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ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）

【記述内容2】 通知方法

【記述内容3】 記述よりも短い通知時期での緊急メンテナンスの有無

【説明】 上記3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。

また、事前告知を実施していることの水準に満たない場合も非認定となります。

②障害・災害発生時の通知（92: 必須開示項目／一定の要件を考慮すべき項目）

【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。

また、障害発生時通知を実施していることの水準に満たない場合も非認定となります。

なお、サービスのユーザに影響の無い障害に限り、通知を行わないことによって非認定にはなりません。

③定期報告（93: 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】 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。」