特定個人情報 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～

平成29年10月1日

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

（参考）　本書中に、『「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」』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、個人情報保護委員会から公表された「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成26年12月11日、平成28年1月1日一部改正）の関連記述を引用しています。

変更履歴:

平成 29 年 10 月

【変更】全般　一般財団法人マルチメディア振興センターを特定非営利活動法人 ASP・SaaS・IoT クラウド コンソーシアムに変更しました。

平成 29 年 9 月 7 日

全般　情報開示指針改定(総務省、平成 29 年 3 月 31 日公表)に伴う新規作成。

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。

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、記述内容は一般財団法人マルチメディア振興センター（以下、当財団とする。）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、当財団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.「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: 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及び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、執行役員も含みます。

（2）従業員

①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。

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。
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。
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】 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」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】 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、執行役員も含みます。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「a 組織体制の整備」に記載されている対策内容

「安全管理措置を講ずるための組織体制を整備する」

②専担の部署・会議体、特定個人情報の適正な取扱いを確保するための組織体制
(21: 選択開示項目/必須開示項目／一定の要件を考慮すべき項目)

【記述内容1】 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。

【記述内容2】 特定個人情報の適正な取扱いを確保するため責任者の有無（役職等）

【記述内容3】 特定個人情報の適正な取扱いを確保するための組織体制の状況（組織名等）

【記述内容4】 特定個人情報の適正な取扱いのための組織体制に関する情報提供の可否と、可能な場合の条件等

【説明】 特定個人情報の適正な取り扱いを確保するための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、役職を記述してください。
特定個人情報の適正な取り扱いを確保するための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。また、「有り」の場合は、組織名を記述してください。
特定個人情報の適正な取扱いを確保するための組織体制に関する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。
上記いずれかの記述内容が未記入の場合もしくは特定個人情報の適正な取扱いを確保するための責任者及び組織体制が無い場合は非認定となります。

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責任者の有無と、「有り」の場合は責任者名・役職名を記述してください。また、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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「a 組織体制の整備」に記載されている対策内容

「安全管理措置を講ずるための組織体制を整備する」

(2)法令等遵守

①法令・各種ガイドライン等の遵守(23:必須開示項目)

【記述内容】 関係法令・ガイドライン等を順守する旨の定めの有無と、「有り」の場合の記載箇所

【説明】 関係法令・ガイドライン等を順守する旨の定めの有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は記載箇所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)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「A 基本方針の策定」に記載されている対策内容

「特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である」

(3)個人情報

①個人情報の取扱い(24:必須開示項目)

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

【説明】 個人情報を収集する際の利用目的の明示について、「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。」

②特定個人情報の取扱い(25:必須開示項目/一定の要件を考慮すべき項目)

【記述内容1】 特定個人情報の取扱いについて定めた取扱規程の有無と、「有り」の場合は規程の名称

【記述内容2】 特定個人情報の取扱いについて定めた取扱規程の開示の可否と、可能な場合の条件等

【説明】 特定個人情報の取扱いについて定めた取扱規程の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は規程の名称を記述してください。

特定個人情報の取扱いについて定めた取扱規程の開示について、「可」または「非」で記述してください。また、可能な場合は条件等を記述してください。
特定個人情報の取扱いについて定めた取扱規程がない場合は非認定となります。
また、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。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「A 基本方針の策定」に記載されている対策内容

「特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である」

(4)守秘義務

①守秘義務契約(26: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】 守秘義務違反があつた場合のペナルティ条項の有無

【説明】 守秘義務について契約や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。
また、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」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は非認定となります。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－2－(1) 委託の取扱い」の「1 委託先の監督」の「B 必要かつ適切な監督針」に記載されている対策内容

「・・・委託先の選定については、委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。」

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「d 情報漏えい等事案に対応する体制の整備」に記載されている対策内容

「情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。・・・」

(5)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（27：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】 特定個人情報等の適正な取扱いに関する従業員教育の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。
従業員に対する特定個人情報等の適正な取扱いに関する取組みについて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は非認定となります。

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第４－２－⑴ 委託の取扱い」の「1 委託先の監督」の「B 必要かつ適切な監督針」に記載されている対策内容

「・・・委託先の選定については、委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「D 人的安全管理措置」の「a 事務取扱担当者の監督」に記載されている対策内容

「事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う」

②従業員に対する守秘義務等の状況（28：必須開示項目/一定のお要件を考慮すべき項目）

【記述内容1】 従業員に対する守秘義務対応の取組の有無

【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、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。
従業員に対する守秘義務対応の取組がない場合、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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の「必要かつ適切な監督」に記載されている対策内容

「・・・委託先の選定については、委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。」

(6)委託

①委託情報に関する開示(29:必須開示項目)

【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、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、「非」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。

未記入の場合は非認定となります。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－2－(1) 委託の取扱い」の「2 再委託」の「C 再委託先の監督」に記載されている対策内容

「・・・したがって、甲は乙に対する監督義務だけではなく、再委託先である丙、丁に対しても間接的に監督義務を負うこととなる。」

②委託先に対する管理状況(30: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)の個人情報保護等の状況の情報提供の可否と、可能な場合の条件等

【記述内容3】 委託先(再委託先)との守秘義務対応の有無

【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は非認定となります。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－2－(1) 委託の取扱い」の「2 再委託」の「C 再委託先の監督」に記載されている対策内容

「・・・したがって、甲は乙に対する監督義務だけではなく、再委託先である丙、丁に対しても間接的に監督義務を負うこととなる。」

(7) 文書類

①情報セキュリティに関する規程等の整備

(31 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・マニュアル等の有無と、「有り」の場合は文書名

【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】 (特定個人情報の適正な取扱いにも資する)情報セキュリティに関する規程等の内容に関する照会対応の可否と、可能な場合の条件等

【説明2】 (特定個人情報の適正な取扱いにも資する)情報セキュリティに関する規程等の内容に関する照会対応の可否について、「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。

(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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「A 基本方針の策定」に記載されている対策内容

「特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「D 人的安全管理措置」の「a 事務取扱担当者の監督」に記載されている対策内容

「事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う」

②サービス提供に係るシステム等仕様・構成の文書の整備（32:必須開示項目）

【記述内容1】システム仕様に係る情報提供の可否、可能な場合の条件等

【記述内容2】機器、ソフトウェア構成に係る情報提供の可否と、可能な場合の条件等

【説明】システム仕様に係る事前の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。

機器、ソフトウェア構成に係る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。

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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－2－(1) 委託の取扱い」の「1 委託先の監督」の「B 必要かつ適切な監督針」に記載されている対策内容

「・・・委託先の選定については、委託者は、委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認しなければならない。」

③運用管理等に関する規程等の整備（33:必須開示項目）

【記述内容】運用管理等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】　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。

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「b 取扱規程等に基づく運用」に記載されている対策内容

「取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「E 物理的安全管理措置」の「c 電子媒体等を持ち出す場合の漏えい等の防止」に記載されている対策内容

「特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「c 外部からの不正アクセス等の防止」に記載されている対策内容

「情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する」

④変更管理等に関する規程等の整備（34：選択開示項目）

【記述内容】変更管理等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】　変更管理等に関する規程等に関する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。

⑤事業継続に関する規程の整備（35：必須開示項目）

【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。

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。

⑥リスク管理に関する規程等の整備（36：必須開示項目）

【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。

⑦勧誘・販売・係争に関する規程等の整備（37: 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。

⑧ASP・SaaSの苦情対応に関する規程等の整備（38: 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、「有り」の場合はそれらの文書名

【記述内容2】 ASP・SaaS事業者の自己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】　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。
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。
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。
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　サービス基本特性

（1）サービス内容

①サービス名称（39: 必須開示項目）

【記述内容】 本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（40: 必須開示項目）

【記述内容1】 本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の大規模な改変等実施の有無と、「有り」の場合は改変年月日（西暦）

【説明】 サービス開始から申請時までの間に大規模改変等実施の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、大規模改変の実施時期について年月日（西暦）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は非認定となります。

③サービスの内容・範囲（41: 必須開示項目）

【記述内容1】 本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行っているサービス連携の有無と、「有り」の場合はその内容　＜前記述と合せて500字以内で記述＞

【説明】 本サービスの内容・特徴を記述してください。 他の事業が提供するサービスとの連携の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、内容について記述してください。
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サービス提供時間（42：必須開示項目）

【記述内容】 サービスの提供時間帯

【説明】 サービスの提供時間帯を記述してください。
未記入の場合は非認定となります。

⑤サービスのカスタマイズ範囲（43: 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】 顧客の要望に応じて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字以内でご記述してください。「特に決まっていない」、「個別相談に応じて決める」等の契約内容に依存する場合は、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。

⑥移行支援（44:必須開示項目）

【記述内容】 申請サービスを利用する際における既存システムからの移行支援の有無（契約内容に依存する場合はその旨記述）

【説明】 当該サービスを利用する際に、既存システムからの移行作業の支援の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、内容について記述してください。契約内容に依存する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・終了時等の事前告知
（45: 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、利用者へ事前に通知する時期及び通知方法について記述してください。
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ヶ月未満となる場合には非認定となります。
また、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サービス（事業）変更・終了後の対応・代替措置（46: 必須開示項目）

【記述内容】 対応・代替措置の基本方針の有無と、「有り」のある場合はその概要

【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・終了した場合における、利用者へ対応・代替措置についての基本方針の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、概略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

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） 契約の終了等

① 情報の返却・削除・廃棄（47: 必須開示項目／一定の要件を考慮すべき項目）

【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】 情報の削除又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。
情報の削除又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。
削除又は廃棄したことの証明書の提供の可否について、「可」または「否」を記述してください。証明書の提供が「否」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も非認定となります。

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－3－⑶ 収集・保管制限」の「B 保管制限と廃棄」に記載されている対策内容

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「b 取扱規程等に基づく運用」に記載されている対策内容

「取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する。・・・」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「E 物理的安全管理措置」の「d 個人番号の削除、機器及び電子媒体等の廃棄」に記載されている対策内容

「個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する」

(4)サービス料金

①料金体系(48: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解約時違約金支払いの有無(49:必須開示項目)

【記述内容】 解約時違約金(利用者側)の有無と、「有り」の場合はその額

【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、その条件、違約金がある場合はその金額もしくは算定条件を記述してください。
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(50: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】 利用者側の都合により契約を解約する場合の利用者側から事前に解約を受け付ける期限の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、その期限(何日・何ヶ月前)を記述してください。
未記入の場合は非認定となります。

(5)サービス品質

①サービス稼働設定値(51: 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】 サービス稼働率の目標値についてはSLA等で設定している数値を記述ください。

申請したサービスについてのサービス提供時間、サービス稼働率については、次の式により算出し記述してください。

○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]－[事前通知のないサービス停止時間]) ／ [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。

- 新規申請時においては、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記述してください。
- 更新申請時においては、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記述してください。

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】 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。

- 新規申請時においては、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記述してください。
- 更新申請時においては、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.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（52: 選択開示項目）

【記述内容1】 システムリソース不足等による応答速度の低下の検知方法の有無と、「有り」の場合は、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】 ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（不可分散対策、ネットワークルーティング、圧縮等）の概要

【説明】 システムリソース不足等による応答速度の低下の検知方法の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、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について記述してください。
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、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）の概要について記述してください。

（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.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認証取得・監査実施（53: 必須開示項目【記述内容1】/選択開示項目【記述内容2】）

【記述内容1】 プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称

【説明1】 プライバシーマーク、ISMS、ITSMSの取得、18号監査（米ではSAS70や後継のSSAE16）の監査報告書作成の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、認証名あるいは監査の名称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。

【記述内容2】 監査状況に関する情報の開示の可否と、可能な場合の条件等

【説明】 情報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。

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「e 取扱状況の把握及び安全管理措置の見直し」に記載されている対策内容

「特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む」

④脆弱性診断（54: 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、診断の対象（アプリケーション、OS、ハードウェア等）と対策の概要

【説明1】 脆弱性診断の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と対策の概要について記述してください。

（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.2.1.4「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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「a アクセス制御」に記載されている対策内容

「情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う」

⑤バックアップ対策（55: 必須開示項目）

【記述内容1】 利用者データの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）

【記述内容3】 バックアップ対応の情報に関する開示の可否と、可能な場合の条件等

【説明】 利用者データのバックアップ間隔について記述してください。

また、バックアップを何世代前まで行っているか記述してください。
バックアップ対応の情報に関する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。
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

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（56：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】 DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要

【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。
DR対策の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、その概要について記述してください。
ここでいうDR対策とは、自然災害やセキュリティインシデント等により、被害を受けたシステムを復旧・修復するための対策（システム面の備えや体制）をいいます。
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（57: 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

【説明】 ASP・SaaSに関連する各種受賞暦について、受賞名と受賞年月を西暦で記述してください。

⑧SLA（サービスレベル・アグリーメント）（58: 必須開示項目）

【記述内容】 本サービス基準に係るSLAが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

(6)契約者数

①契約者数(59: 選択開示項目)

【記述内容】 本ASP・SaaSのサービスの契約企業数等

【説明】 申請したASP・SaaSのサービスの契約企業数を記述してください。

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) 中核的ソフトウェア

①情報の提供等(60:必須開示項目)

【記述内容1】アプリケーション、データベースに関する個別照会の可否

【記述内容2】アプリケーション、データベースに関する技術情報提供の可否と、可能な場合の条件等

【説明】 個別照会の可否について、「可」または「否」を記述してください。
技術情報提供の可否について、「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。
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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－3－⑵ 個人番号の提供の求めの制限、特定個人情報の提供制限」の「2 特定個人情報の提供制限」の「A 「提供」の意義について」に記載されている対策内容

「「提供」とは、法的な人格を超える特定個人情報の移動を意味するものであり、同一法人の内部等の法的な人格を超えない特定個人情報の移動は「提供」ではなく「利用」に当たり、利用制限（番号法第9条、第28条、第29条第3項、第32条）に従うこととなる。・・・」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－6 個人情報保護法の主な規定」の「C データ内容の正確性の確保」に記載されている対策内容

「個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない」

（2）連携（61：必須開示項目）

①他のASP・SaaSとの連携状況に関する情報提供

【記述内容】 他のASP・SaaSとの連携の有無と、「有」の場合は情報提供の条件等

【説明】 他のASP・SaaSとの連携の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、その情報提供の条件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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」の
「第4－2－(1) 委託の取扱い」の「2 再委託」の「C 再委託先の監督」に記載されている対策内容

（3）セキュリティ

①死活監視（62: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容】 死活監視の有無と、「有」の場合は死活監視の対象（アプリケーション、プラットフォーム、サーバ・ストレージ等）

【説明】 死活監視の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、死活監視の対象（アプリケーション、プラットフォーム、サーバ・ストレージ等）と監視インターバル(何分ごとに監視を行っているかの数値（時間間隔）)を記述してください。
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。
未記入の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.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時刻同期（63: 必須開示項目）

【記述内容1】 時刻同期への対応の有無と、「有り」の場合は時刻同期方法

【記述内容2】 時刻同期への対応状況に関する情報提供の可否と、可能な場合の条件等

【説明】　時刻同期への対応の有無について「有り」又は「無し」で記述してください。
情報提供の可否について、「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。
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

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。」

③ウイルス対策（64: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容1】 ウイルス対策の有無

【記述内容2】 ウイルス措置への対応状況に関する情報開示の可否と、可能な場合の条件等

【説明】 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ウイルス対策の有無について、「有り」または、「無し」を記述してください。
情報提供の可否について、「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。
ウイルス対策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。
また、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。

（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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「c 外部からの不正アクセス等の防止」に記載されている対策内容

「情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「d 情報漏えい等の防止」に記載されている対策内容

「特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる」

④ユーザ認証(65:必須開示項目／一定の要件を考慮すべき項目)

【記述内容1】 利用者の職種単位への対応の有無

【記述内容2】利用事務単位への対応の有無

【説明】利用者の職種単位へ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。

利用事務単位へ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。

特定個人情報の取り扱いについて利用事務単位への対応が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も非認定となります。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「c 外部からの不正アクセス等の防止」に記載されている対策内容

「情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する」

⑤管理者権限の運用管理(66:必須開示項目／一定の要件を考慮すべき項目)

【記述内容1】 システム運用部門の管理者権限の登録・登録削除の手順の有無

【説明1】 正式な手順の有無について、「有り」または、「無し」を記述してください。

手順が存在していない場合は非認定となります。

未記入の場合も非認定となります。

【記述内容2】 管理者認証に関する情報開示の可否、可能な場合の条件等

【説明2】情報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。

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。」

⑥ID・パスワードの運用管理(67: 必須開示項目／一定の要件を考慮すべき項目)

【記述内容1】事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の有無

【説明1】利用者のIDやパスワードの運用管理方法の規程の有無について、「有り」または、「無し」を記述してください。規程が存在していない場合は非認定となります。
また、未記入の場合も非認定となります。

【記述内容2】ID・PW認証以外の認証方法の採用の有無

【説明2】ID・PW認証以外の認証方法の採用の有無について、「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。

【記述内容3】ID・PW認証採用の場合のポリシー等に関する情報開示の可否と、可能な場合の条件等

【説明3】情報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。
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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「b アクセス者の識別と認証」に記載されている対策内容

「特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「d 情報漏えい等の防止」に記載されている対策内容

「特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる」

⑦記録（ログ等）（68必須開示項目／一定の要件を考慮すべき項目）

【記述内容1】 利用者の利用状況の記録(ログ等)取得の有無と、「有り」の場合はその保存期間及び利用者への提供可否

【記述内容2】 システム運用に関するログの取得の有無と、「有り」の場合は保存期間

【記述内容3】 ログの改ざん防止措置の有無

【説明】 利用者の利用状況の記録(ログ等)取得の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、保存期間、及び利用者への提供可否についても記述してください。

システム運用部門のアクセスログの取得の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、保存期間についても記述してください。

アクセスログへの改ざん防止措置の有無について、「有り」または、「無し」を記述してください。

利用者の利用状況の記録(ログ等)取得を実施していることおよびアクセスログへの改ざん防止措置の設定が認定の条件であり、ない場合は非認定となります。

また、上記いずれかの記述項目が未記入の場合も非認定となります。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「b 取扱規程等に基づく運用」に記載されている対策内容

「取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する」

⑧セキュリティパッチ管理(69: 必須開示項目／一定の要件を考慮すべき項目)

【記述内容】 パッチ管理の状況とパッチ更新間隔等、パッチ適用方針

【説明】 セキュリティパッチ管理の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、パッチ更新間隔等のパッチ適用方針について記述してください。

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。

また、未記入の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.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。」

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「c 外部からの不正アクセス等の防止」に記載されている対策内容

「情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「d 情報漏えい等の防止」に記載されている対策内容

「特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる」

⑨暗号化対策（70：必須開示項目）

【記述内容】暗号化処置（データベース）への対応の有無と、「有り」の場合はその概要

【説明】データベースに対する暗号化処置の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、その概要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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「b アクセス者の識別と認証」に記載されている対策内容

「特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する」

⑩その他セキュリティ（71：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（情報漏洩対策等）

【説明】情報漏洩対策等、その他の特筆すべきセキュリティ対策について記述してください。

3．3 ネットワーク

(1)回線

①推奨回線(72: 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】 サービスを提供するに当たり推奨する回線の種類について記述してください。
回線に障害が発生した場合、事業者が負う責任範囲について記述してください。

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

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（73: 必須開示項目）

【記述内容】 推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲

【説明】 推奨帯域の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、データ通信速度の範囲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。

③推奨端末（74: 必須開示項目）

【記述内容1】 パソコン、携帯電話等の端末種類、OS等

【記述内容2】 利用するブラウザの種類

【説明】 推奨端末(パソコン、携帯電話、タブレット等)、OS等について記述してください。
利用するブラウザの種類とそのバージョンについて記述してください。
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）セキュリティ

①ファイアウォール（75: 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】 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について、「有り」または、「無し」を記述してください。
ファイアウォール措置を実施していない場合は非認定となります。
また、未記入の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（76: 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と、「有り」の場合は対応方法

【説明】 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、その対応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（77: 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
【説明】 事業者とエンドユーザとの間のネットワークにおいて障害を検知した場合の通報時間につい記述してください。

（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.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ユーザ認証（78: 必須開示項目／一定の要件を考慮すべき項目）

【記述内容1】 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1】 利用者のなりすましを防ぐために実施している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について記述してください。
利用者認証を実施していない場合は非認定となります。
未記入の場合も非認定となります。

【記述内容2】 ID・PW以外の認証方法の採用の有無と、「有り」の場合は具体的な内容

【説明2】 ID・PW以外の認証方法の採用の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、具体的な内容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。

【記述内容3】 ユーザ認証に係る技術情報の提供の可否と、可能な場合の条件等

【説明3】 技術情報の提供の可否について、「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。

未記入の場合は非認定となります。

「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「b アクセス者の識別と認（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
証」に記載されている対策内容

「特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する」

（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。」

⑤なりすまし対策（事業者サイド）（79: 必須開示項目）

【記述内容1】 第三者によるなりすましサイトに関する対策の実施の有無と、「有り」の場合は認証の方法

【記述内容2】 なりすまし対策への対応方法に関する情報提供の可否と、可能な場合の条件等

【説明】 事業者のなりすましを防ぐために実施している対策の実施の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、対策方法について記述してください。 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。
情報提供の可否可否について、「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。
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

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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「c 外部からの不正アクセス等の防止」に記載されている対策内容

「情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「d 情報漏えい等事案に対応する体制の整備」に記載されている対策内容

「情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する」

⑥暗号化対策（80： 必須開示項目）

【記述内容】 暗号化措置（ネットワーク）の有無と、「有り」の場合はその概要

【説明】 ネットワークに対する暗号化処置の有無について、「有り」または、「無し」を記述してください。また、「有り」の場合は、その概要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）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「b アクセス者の識別と認証」に記載されている対策内容

「特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する」

⑦その他セキュリティ対策（81: 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 （情報漏洩対策等）

【説明】 可能な範囲で記述してください。

（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.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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「C 組織的安全管理措置」の「c 取扱状況を確認する手段の整備」に記載されている対策内容

「特定個人情報ファイルの取扱状況を確認するための手段を整備する」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「F 技術的安全管理措置」の「b アクセス者の識別と認証」に記載されている対策内容

「特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する」

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（82: 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】 データセンター専用建物か否か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。

②所在地（83: 必須開示項目（記述内容1）／選択開示項目（記述内容2）

【記述内容1】 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】 特筆すべき立地上の優位性があれば記述（例：標高、地盤等）

【説明】 サーバ設置場所について国名を記述してください。設置場所が日本の場合には、地域ブロック名（例：関東、東北）も記述してください。
特筆すべき立地上の優位性があれば記述してください。
記述内容1について未記入の場合は非認定となります。

③耐震・免震構造（84: 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】 サーバが設置されている建物の耐震数値について記述してください。

サーバが設置されている建物の免震構造や制震構造の有無について、「有り」または、「無し」を記述してください。
上記いずれかの項目について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（85: 必須開示項目）

【記述内容】 無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間

【説明】 無停電電源装置（UPS）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、電力供給時間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。

②給電ルート（86: 必須開示項目）

【記述内容】 異なる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】 自家発電機やUPSを除き、2系統以上の異なる変電所を経由した給電ルートが確保されているか否か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。

③非常用電源（87: 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」の場合は連続稼働時間の数値

【説明】 非常用電源（自家発電機）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、連続稼働時間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.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（88: 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か否か

【説明】 自動消火設備の有無について「有り」または、「無し」を記述してください。また、「有り」の場合は、ガス系消火設備か否かについても記述してください。
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.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(89: 必須開示項目)

【記述内容】 火災検知システムの有無

【説明】 火災検知システムの有無について「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

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(90: 必須開示項目)

【記述内容】 直撃雷対策の有無

【説明】 直撃雷対策の有無について「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

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(91: 必須開示項目)

【記述内容】 誘導雷対策の有無

【説明】 誘導雷対策の有無について「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

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空調設備（92: 必須開示項目）

【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

【説明】 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.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（93: 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

【記述内容3】 個人認証システムの有無

【説明】 入退室記録の有無について「有り」または、「無し」を記述してください。また、「有り」の場合は、保存期間についても記述してください。
監視カメラの有無について「有り」または、「無し」を記述してください。
個人認証システムの有無「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

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（94: 選択開示項目【記述内容1】【記述内容2】/必須開示項目【記述内容3】）

【記述内容1】 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

【記述内容2】保管管理手順書の有無

【説明1/2】 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について「有り」または、「無し」を記述してください。
保管管理手順書の有無について「有り」または、「無し」を記述してください。

【記述内容3】 ラック・媒体管理の方法に関する情報提供の可否と、可能な場合の条件等

【説明3】情報提供の可否について、「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。

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。」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「E 物理的安全管理措置」の「a 特定個人情報等を取り扱う区域の管理」に記載されている対策内容

「特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる」

（参考）「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「E 物理的安全管理措置」の「b 機器及び電子媒体等の盗難等の防止」に記載されている対策内容

「管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる」

③その他セキュリティ対策（95: 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（破壊侵入防止対策、防犯監視対策等）

【説明】 可能な範囲で記述してください。

（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.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・問合せ)

①連絡先(96: 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】 特定個人情報の取扱いに関する苦情処理に係る受付の可否

【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)を設置しているない場合は非認定となります。
特定個人情報の取扱いに関する苦情処理に係る可否について、「可」または「否」を記述してください。
また、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。

(参考)「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(別添)」の
「2 講ずべき安全管理措置の内容」の「A 基本方針の策定」」に記載されている対策内容

「特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である」

②営業日・時間(97: 必須開示項目)

【記述内容】 営業曜日、営業時間(受付時間)

【説明】 営業曜日、営業時間(受付時間)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。

③サポート範囲・手段(98: 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】 サポート範囲とその手段について記述してください。
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)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

（99: 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】 告知方法

【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。
また、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（100: 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。

③定期報告（101: 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

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。」