医療情報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、破線テキストボックスで記述した内容については、、「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　総務省公表）及び「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第1.1版」（平成22年12月　総務省公表）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、記述内容は特定非営利活動法人 ASP・SaaS・IoT クラウドコンソーシアム（以下、ASPIC 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、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、「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・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】 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、執行役員も含みます。

(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／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

【記述内容3】情報セキュリティに関する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】 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。

情報セキュリティに関する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情報セキュリティに関する責任者及び組織体制が無い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「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)法令等遵守

①法令・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・ガイドライン等を遵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・ガイドライン等を遵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。

(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の有無と、「有り」の場合は記載個所

【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、記載されている個所(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個人情報の取扱いに関する規程類(25:必須開示項目)

【記述内容1】サービス提供に係る個人情報取扱規程の有無

【記述内容2】サービス提供に係る個人情報取扱規程の開示の可否と、可能な場合の条件等

【記述内容3】医療関連ガイドラインに基づいて取り扱っていることの照会の可否(5000人基準等)

【説明】 サービス提供に係る個人情報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。
サービス提供に係る個人情報取扱規程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。
医療関連ガイドラインに基づいて取り扱っていることの照会の可否について、「可」または、「否」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）「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」（委託契約）に記載されている対策内容

「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。自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること。個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。」

（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」（個人情報の記録媒体の管理（保管・授受等）の方法）に記載されている対策内容

「個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱うこと」

（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「情報システムの改造と保守」（守秘義務）

「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」

（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「診療録等の外部保存委託先の事業者内における個人情報保護」「適切に委託先の監督」に記載されている対策内容

「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。自社で定める個人情報保護を記録した媒体の運用管理規程等が、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。個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること」

（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「診療開始前の説明」に記載されている対策内容

「外部保存実施に関する患者への説明」の①「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」

（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「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「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」

(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。

（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「保存した情報の取り扱いに対して監督」に記載されている対策内容

「守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと」

(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:必須項目／一定の要件を考慮すべき項目)

【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。
従業員に対するセキュリティ教育実施に関する取組みが無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）「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「情報および情報機器の持ち出しについて」に記載されている対策内容

「全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること」

②従業員に対する守秘義務等の状況(28:必須項目／一定の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。
従業員に対する守秘義務対応の取組が無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)「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「情報システムの改造と保守」(個人情報を含むデータを使用)に記載されている対策内容

「雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること」

(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「情報および情報機器の持ち出しについて」(盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと)に記載されている対策内容

「従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること」

(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「外部保存におけるASP・SaaS事業者への要求事項」守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること)に記載されている対策内容

「従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること」

(6)委託

①委託情報に関する開示(29: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「人的安全管理対策」（再委託）に記載されている対策内容

「外部組織に対して再委託等を行う場合には、事前に医療機関等の管理者に対して説明を行い、契約において体制を明確にすること」

② 委託先に対する管理状況（30：必須項目／一定の要件を考慮すべき項目））

【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。委託先（再委託先）と守秘義務契約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）「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」（個人情報の取扱いを委託する場合）に記載されている対策内容

「自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること」
「個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること」

(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:必須項目)

【記述内容1】システム仕様に係る情報提供の可否と、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。

③運用管理等に関する規程等の整備(33:必須項目)

【記述内容】運用管理等に関す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。

④変更管理等に関する規程等の整備（34：必須項目）

【記述内容】変更管理等に関す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。

⑤事業継続に関する規程の整備（35：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。
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」の場合は文書名

【記述内容2】 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。

（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）「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「情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと」に記載されている対策内容

「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」
「各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと」

（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「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること」
「運用しているアクセス管理に関する規程類が、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」

（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におけるASP・SaaS事業者への要求事項」の「理念（基本方針と管理目的の表明）」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」

（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におけるASP・SaaS事業者への要求事項」の.「運用管理規程等において次の内容を定めること」「契約書・マニュアル等の文書の管理」に記載されている対策内容

「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）「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「運用管理規程等において次の内容を定めること」「リスクに対する予防、発生時の対応の方法」に記載されている対策内容

「全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること」
「自社で定めるリスク等に対する予防措置及び事故等の発生時の対応等が、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」

（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.「システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと」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）「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「従業者に対する人的安全管理措置」.「医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること」「従業者の退職後の個人情報保護規程を定めること」に記載されている対策内容

「従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること」

（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「事務取扱委託業者の監督及び守秘義務契約」「病院事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと」①「受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること」に記載されている対策内容

「従業員に対する秘密保持又は守秘義務についての要求を明確にし、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）「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「方針の制定と公表」で「把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること」に記載されている対策内容

「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」
「組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること」
「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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「情報の破棄におけるASP・SaaS事業者への要求事項」「不要になった個人情報を含む媒体の破棄を定める規程の作成」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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」のシステム利用者を模して操作確認を行うための識別・認証」に記載されている対策内容

「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」

（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「情報システムの改造と保守におけるASP・SaaS事業者への要求事項」「そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること」に記載されている対策内容

「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」

（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」のアカウント管理体制を整えておくこと」に記載されている対策内容

「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」
「外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること」
「従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること」

（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
「医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること」に記載されている対策内容

「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」

（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
「リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること」に記載されている対策内容

「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」

（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
判断するための基準、手順、判断者、をあらかじめ決めておくこと」に記載されている対策内容

「組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること」

（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
「非常時の情報システムの運用」に記載されている対策内容

「自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）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」

（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
「関連組織の責任分界点、責任の所在を契約書等で明確にすること」に記載されている対策内容

「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」
「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
「一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること」 に記載されている対策内容

「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）「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
「同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること」に記載されている対策内容

「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）「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
「リモートログイン機能を制限すること」に記載されている対策内容

「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）「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
「見読性の確保におけるASP・SaaS事業者への要求事項」の(1)「情報の所在管理」に記載されている対策内容

「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」

（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
「記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと」に記載されている対策内容

「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）「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
「記録媒体が劣化する以前に情報を新たな記録媒体または記録機器に複写すること。記録する媒体及び機器毎に劣化が起こらずに正常に保存が行える期間を明確にし、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体または記録機器については、そのデータを新しい記録媒体または記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること」に記載されている対策内容

「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）「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
「医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
「受託事業者が民間事業者等に課せられたガイドライン等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
「保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
)「保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等において情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること」に記載されている対策内容

「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」

（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
)「診療録等の外部保存委託先の事業者内における個人情報保護」①「適切な委託先の監督を行なうこと」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること」

（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
「個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること」に記載されている対策内容

「重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること」
「受託した個人情報を参照可能な事務室等における入退室管理のルールが、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」

（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
「個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること」に記載されている対策内容

「サーバルームやラックの鍵管理を行うこと」

（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
「清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと」に記載されている対策内容

「利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと」
「重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること」

（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
「記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと」に記載されている対策内容

「情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、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、ネットワークの運用・管理に関する手順書を作成すること」
「重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること」

（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
「委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること」に記載されている対策内容

「外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること」

（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
「プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと」に記載されている対策内容

「外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること」

（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
「医療サービスを提供し続けるためのBCPの一環として“非常時” と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと」に記載されている対策内容

「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）「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
「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること」

（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
「情報システムへのアクセスにおける利用者の識別と認証を行うこと」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること」

（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
「本人の識別・認証にユーザIDとパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること」

（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
「入力者が端末から長時間、離席する際に正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること」に記載されている対策内容

「受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること」

（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
「そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること」
「保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること」

（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
「非常時の情報システムの運用」に記載されている対策内容

「自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）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」

（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
「システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある利用者以外による作成、追記、変更を防止すること」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること

（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
「電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合」の1.「利用者を正しく識別し、認証を行うこと」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること

（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
「業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること

（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
)「リモートログイン機能を制限すること」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること

（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
外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること」に記載されている対策内容

「ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること

（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
「運用管理規程等において次の内容を定めること」の(e)「機器を用いる場合は機器の管理」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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること」

（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
「電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること」に記載されている対策内容

「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」

（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
「機器・ソフトウェアの品質管理」の1.「システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること」に記載されている対策内容

「機器、ソフトウェア構成について、医療機関等と合意をとること」

「機器、ソフトウェア構成について文書化を行い、医療機関等の管理者に対して報告できる内容とすること」

（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
「医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること」に記載されている対策内容

「自社で講じるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること」

（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
「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「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」

（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
「運用管理規程等において次の内容を定めること」(f)「個人情報の記録媒体の管理（保管・授受等）の方法」 に記載されている対策内容

「自社で定める個人情報を記録した媒体の運用管理規程等が、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」

（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
システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある」に記載されている対策内容

「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」

（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
「組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること」、「運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること」、「情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること」に記載されている対策内容に記載されている対策内容

「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

（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
「医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと」に記載されている対策内容

「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」

（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
「個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること」に記載されている対策内容

「受託した個人情報を参照可能な事務室等における入退室管理のルールが、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」

（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
「医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること」に記載されている対策内容

「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」

（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
「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「ASP・SaaSサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること

（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
「アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること」に記載されている対策内容

「ASP・SaaSサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること」に記載されている対策内容

「従業員に対する秘密保持又は守秘義務についての要求を明確にし、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）「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
「メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。・・・」 に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「適切な委託先の監督を行なうこと 」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」

（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
「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「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」

（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
「方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること」に記載されている対策内容

「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
「情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること」に記載されている対策内容

「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること」に記載されている対策内容

「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
「運用管理規程において下記の内容を定めること」に記載されている対策内容

「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」
「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
「動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること」に記載されている対策内容

「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
3.4.3「ASP・SaaS事業者間のサービス移行における留意点」の表3-17「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「機器及び媒体を正式な手順に基づいて廃棄すること」

（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
「保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと」に記載されている対策内容

「受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと」
「許可されていない受託データの閲覧を禁止することにつき、その方法等を含め、医療機関等と合意すること」

（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
「外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること」に記載されている対策内容

「受託した医療情報は、匿名化されたものを含めて、医療機関との契約に基づくことなく、分析、解析等を実施しないこと」
「医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と合意すること」

（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」

（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
「置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること」に記載されている対策内容

「情報の持ち出しに関する自社において定めた運用管理規程が、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」

（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
「組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること」に記載されている対策内容

「情報の持ち出しに関する自社において定めた運用管理規程が、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」

（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
「運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること」に記載されている対策内容

「情報の持ち出しに関する自社において定めた運用管理規程が、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」

（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
「通信の相手先が正当であることを認識するための相互認証をおこなうこと」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「ネットワークに接続する場合は「外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること」に記載されている対策内容

「運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。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）「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
「持ち出した情報を、例えばファイル交換ソフト（Winny等）がインストールされた情報機器で取り扱わないこと。」に記載されている対策内容

「運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。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）「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
「個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること」に記載されている対策内容

「受託する個人情報を保守に用いる端末に保存しない旨、自社の運用管理規程等に定めること」

（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
「入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること」に記載されている対策内容

「受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること」

（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
「ネットワークに接続する場合は 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること」に記載されている対策内容
「受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、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」

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改変等実施の有無と、「有り」の場合は改変年月日(西暦)

【説明】 本ASP・SaaSのサービス開始年月日を西暦で記述してください。

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】 本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も非認定となります。
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、基本方針がある場合はその概略

【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)

【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。

(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
手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること」に記載されている対策内容

「自社において定めた情報の破棄手順が、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」

(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
事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること」に記載されている対策内容

「情報の破棄を実施した場合に、電磁記録媒体の消磁、物理的破壊等、情報の削除方法を含む実施内容を医療機関等に対して報告し、破棄記録等を提出すること」

（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
「運用管理規程において下記の内容を定めること」に記載されている対策内容

「自社において定めた情報の破棄手順が、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」

（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
「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「情報の破棄の実施に際し、報告の内容・範囲・提出すべき資料等について、医療機関等と合意すること」

（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。

【記述内容4】 ネットワークに関する稼働設定値等に関する情報開示の可否と、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。
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
「医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。・・・」に記載されている対策内容

「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」

（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
「回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。」に記載されている対策内容

「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」

（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
「緊急に必要になるとまではいえない診療録等の見読性の確保」に記載されている対策内容

「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」

（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
「医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては 外部と個人情報を含む医療情報を交換する場合の安全管理を遵守していること」に記載されている対策内容

「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」

【記述内容5】 画面表示の応答速度に関する情報に係る情報提供の可否と、可能な場合の条件等

【説明】 画面表示の応答速度に関する情報に係る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
「見読性の確保におけるASP・SaaS事業者への要求事項」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や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あるいは計画の有無と、「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

【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

「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／一定の要件を考慮すべき項目）

【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】 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。
プライバシーマーク又は認証の取得もしくは監査を実施していない場合は非認定となります。未記入の場合は非認定となります。

【記述内容2】 保健医療福祉分野のプライバシーマークの取得の有無

【説明】 保健医療福祉分野のプライバシーマークの取得について「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】 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。
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
「運用管理規程等において次の内容を定めること」(h)「監査」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情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること」
「自社において実施するシステム監査等が、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」

④脆弱性診断（54: 選択開示項目）

【記述内容1】 脆弱性診断の有無、「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】 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

「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）「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
「回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。」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）「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
「記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと」に記載されている対策内容

「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」

③ 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（インターバル、世代情報以外含む）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。
何世代前までバックアップしているかについて記述してください。
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。」

（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
「確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと」に記載されている対策内容

「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」

（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
「一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること」に記載されている対策内容

「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」

（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
「同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること」に記載されている対策内容

「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」

（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
「ネットワーク上で「改ざん」されていないことを保証すること」に記載されている対策内容

「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、情報交換の実施基準・手順等を備えること」

（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
「システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること」に記載されている対策内容

「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」

（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
「各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと」に記載されている対策内容

「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」

（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
「見読性の確保におけるASP・SaaS事業者への要求事項」の【医療機関等に保存する場合】「バックアップサーバ」」に記載されている対策内容

「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」

（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
「ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止」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」

④ 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。
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。

⑤ 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歴について、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】 本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）「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
「同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること」に記載されている対策内容

「一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せられる機能を含めること」

（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
「システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること」に記載されている対策内容

「入出力するデータ項目の形式ついて、標準形式を採用する。標準形式によることができない場合には、妥当なデータ項目の形式について医療機関等と合意すること」

（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
「媒体・機器・ソフトウェアの整合性不備による復元不能の防止」の2.「マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること」に記載されている対策内容

「マスターテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備える。本機能を備えることが困難な場合には、妥当な提案を行い、医療機関等と合意すること」

（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

「見読性を保証するサービス仕様について、医療機関等と合意すること」

(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、「有り」の場合は技術情報提供の条件等

【説明】 アプリケーション・サービス・プロバイダ(ASP)との連携状況についての情報提供の可否、及び可能な場合の条件等について記述してください。なお、連携するASPがない場合は、「連携ASPはない。」と記述してください。
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
「緊急に必要になることが予測される診療録等の見読性の確保」に記載されている対策内容

「緊急時の医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)をASP・SaaSにおいて含めることについて、医療機関等の管理者と協議し、合意すること」

（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
「運用管理規程等において次の内容を定めること」「機器を用いる場合は機器の管理」「監査」」に記載されている対策内容

「連携ASP・SaaS事業者が提供するASP・SaaSサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること」

（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
「委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること」のに記載されている対策内容

「情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること」

（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）

【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

「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】　時刻同期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。

「有り」の場合はシステムの時刻同期方法について記述してください。

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。」

（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
「アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある」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）の時刻同期の方法を規定し、実施すること」

（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
「診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。」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】 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）「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
常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと」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」

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。電子カルテ等資格を要する機能については、対応がない場合は非認定となります。

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。
アクセス対象資産への設定単位の可否について、「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。

(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
「業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること」に記載されている対策内容

「提供する電子カルテシステム等に関するサービスにおいて、医療機関等の職務権限等に応じたアクセス制御が可能であることを含め、仕様内容について、医療機関等と合意すること」

(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
複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある」に記載されている対策内容

「医療機関等の利用者の職種等に応じたアクセス制御の設定に関しては、医療機関等の管理者と協議の上、実際に設定する作業に関する役割も含めて合意すること」

(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
「メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。」に記載されている対策内容

「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。」

(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「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「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、運用管理規程を作成すること。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)「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「患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。・・・」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること」 に記載されている対策内容

「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、運用管理規程を作成すること。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。

（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
.「患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。・・・」 に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「利用者を正しく識別し、認証を行うこと」 に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。・・・」に記載されている対策内容

「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、運用管理規程を作成すること。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」

【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認証の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

「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）「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
「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。・・・」 に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「利用者を正しく識別し、認証を行うこと」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等において情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること」に記載されている対策内容

「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、運用管理規程を作成すること。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 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、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管理者の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。

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)取得及びログの改ざん防止措置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項目が未記入の場合も非認定となります。

(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
「アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。・・・ 」に記載されている対策内容

「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」

(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
「アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録(会計記録、データベース記録、取引ログ、監査ログ、運用手順等)については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」
「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」

（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
「保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと」に記載されている対策内容

「ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること」
「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」

（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
「リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること」に記載されている対策内容

「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」

（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
「ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項」に記載されている対策内容

「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」

（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
「代行操作が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行操作の都度記録されること」に記載されている対策内容

「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（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

「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。」

⑦ 暗号化対策（70:必須開示項目）

【記述内容】暗号化措置（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)」の
「委託先の監督」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」

（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
「講ずべき安全管理措置の内容」の「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
「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

【記述内容3】利用者が無線LANを利用する場合の仕様等の情報の提供の可否と、可能な場合の条件等

【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。
仕様等の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。
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

「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。」

(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
「無線LANを利用する場合 システム管理者は以下の事項に留意すること。・・・」に記載されている対策内容

「医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策について、事業者の役割、範囲等について合意すること」

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、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ファイアウォール設置等(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も非認定となります。
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。また、「有り」の場合は、対応方法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

「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

「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

「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。」
「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）「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「情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。・・・」に記載されている対策内容

「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、運用管理規程を作成すること。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】 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、専用ソフトによるアクセス監視、 他事業者による関連サービスの利用、 認証局が発行する証明書による確認、ID・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

「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）「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
「情報システムへのアクセスにおける利用者の識別と認証を行うこと」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。・・・」に記載されている対策内容

「ASP・SaaSを利用するネットワークで用いられる医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、医療機関等から事業者までの確認を行うこと（但し事業者が保守業務を再委託している場合には、事業者と再委託先との接続では本項の対応を適用せず、別途なりすましを防止する策を講じること」

⑥暗号化対策（80： 必須開示項目）

【記述内容】 暗号化処置（ネットワーク）への対応の有無と、「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)」の
「委託先の監督」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」

（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
「利用者を正しく識別し、認証を行うこと」に記載されている対策内容

「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、運用管理規程を作成すること。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）「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
「医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること」に記載されている対策内容

「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
「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
「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

「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）「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
「データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。・・・」に記載されている対策内容

「厚生労働省ガイドラインに基づいて医療機関等が採用する通信方式認証手段が妥当なものであることを確認することにつき、事業者の役割と範囲を、医療機関等と合意すること」

3．4 保守・運用

(1) 運用

① 運用端末の物理セキュリティの状況(82: 必須開示項目)

【記述内容1】 入退出管理の有無

【記述内容2】その他実施している対策

【説明】 入退出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。
その他実施している対策について、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
「リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること」に記載されている対策内容

「サービス提供に必要なシステムの保守をリモートメンテナンスで行う場合の医療機関等の管理者に対する報告、承認等について、医療機関等と合意すること」

(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
「リモートログイン機能を制限すること」に記載されている対策内容

「ASP・SaaS提供に必要なシステムの保守をリモートメンテナンスで行う場合の、医療機関等への報告対象とするシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容等について、医療機関等と合意すること」

② 寄託情報の可搬媒体に関する管理(83: 必須開示項目)

【記述内容1】 管理規程等の有無

【記述内容2】 管理方法等に関する情報提供の可否

【説明】 管理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。
管理方法等に関する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。
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
「持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。・・・」に記載されている対策内容

「受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、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) 保守

① 保守端末の物理セキュリティの状況（84: 必須開示項目）

【記述内容1】 入退出管理の有無

【記述内容2】その他実施している対策

【説明】入退出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。
その他実施している対策について、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
「個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。・・・・」に記載されている対策内容

「委託業務に基づき受託する個人情報の内容を参照する必要が生じる場合には、データアクセスが可能な端末が設置されている部屋に対する入退出の施錠管理及び入退出管理を行うこと」

② テスト環境と本番環境の分離に関する状況（85: 必須開示項目）

【記述内容1】 テスト環境と本番環境の分離の原則に関して、例外措置の有無

【記述内容2】例外措置に関する概要

【説明】テスト環境と本番環境の分離の原則に関する例外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。
例外措置に関する概要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
「動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること」に記載されている対策内容

「受託した情報の処理に必要な、システムの動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること」
「システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること」

3．5 ハウジング（サーバ設置場所）

（1）施設建築物

①建物形態（86: 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（87: 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（88: 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

「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（89: 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（90: 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、異なる変電所を経由した2系統以上の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（91: 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

「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（92: 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

「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（93: 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。

（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 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。」

未記入の場合は非認定となります。

（4）避雷対策設備

①直撃雷対策（94: 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

「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（95: 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

「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（96: 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

「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（97: 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

「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。」
「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（98: 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

「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）「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
「窃視防止の対策を実施すること」に記載されている対策内容

「利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと」
「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」
「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」

（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
「記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと」に記載されている対策内容

「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」

（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
「保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと」に記載されている対策内容

「利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと」

③ その他セキュリティ対策（99: 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

「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。」
「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。」

3．6　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(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】 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。

(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
「運用管理規程等において次の内容を定めること」b.「医療機関等の体制」に記載されている対策内容

「医療機関等の体制に対応する事業者の体制を明らかにすることを、医療機関等と合意すること」

(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
「保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと」に記載されている対策内容

「保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等について合意すること」

②営業日・時間(101: 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サポート対応(102: 必須開示項目)

【記述内容1】 連携するASP・SaaSに関する苦情対応の可否

【記述内容2】 エンドユーザーからの苦情対応への可否

【説明】連携ASP・SaaSに関する苦情対応の可否について、「可」または「否」を記述してください。

エンドユーザーからの苦情対応への可否について、「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も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
「運用管理規程等において次の内容を定めること」(i)「苦情・質問の受け付け窓口」に記載されている対策内容

「ASP・SaaSサービスの提供に支障が生じた場合には、その原因が連携ASP・SaaS事業者に起因するものであったとしても、利用者と直接契約を結ぶASP・SaaS事業者が、その責任において一元的にユーザサポートを実施すること」
「医療機関等の管理者側からの問合せ窓口を設けること。また受付の時間帯等について、医療機関等と合意すること」

④ サポート範囲・手段（103: 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
（104: 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

【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。

（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
「保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること」に記載されている対策内容

「サービス提供に必要な保守業務を行うに際して、医療機関等の管理者に対して書面等により作業の事前及び事後に通知を行うこと、及び事前の了解を必要とする作業等について医療機関等と合意すること」

②障害・災害発生時の通知（105: 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通知の有無・方法

【説明2】 緊急時発生時の通知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
「正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること」に記載されている対策内容

「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）「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定期報告（106: 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。」