ASP・SaaS（IoTクラウドサービス）の安全・信頼性に係る情報開示認定制度
～認定制度の概要～

令和6年9月30日 改定

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

目　次

改定内容履歴：

令和6年9月

【変更】認定機関の事務局名称を「クラウドサービス安全・信頼性認定制度事務局」から「クラウドサービス情報開示認定機関事務局」に変更しました。

令和４年４月

【変更】クラウドサービス情報開示認定機関を一般社団法人 ASP・SAAS・AI・IOT クラウド産業協会から一般社団法人日本クラウド産業協会に変更しました。

令和３年６月

４．（４）【削除】印鑑証明書の提出の記載を削除しました。

９．（１）【削除】印鑑証明書の提出の記載を削除しました。

令和２年４月

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

令和元年12月　【変更】４.認定に係る申請　（４）申請書類（５）送付方法
１１.認定の取り消し等　（３）認定の取り消し
１３.問合せ窓口　ホームページURL
https://www.aspicjapan.org/nintei/asp-iotに変更

令和元年9月：

別表１【追加】令和元年10月1日の消費税率の引き上げに伴う「審査手数料(新規申請費用)」、「更新審査手数料(2年ごとに更新する際の費用)」及び「認定証再発行手数料」の改定料金を追記しました。

１．認定制度の背景と経緯

世界最先端のブロードバンド環境が実現され、ICT（情報通信技術）は、経済成長に大きく寄与するとともに、人口減少社会下の我が国経済を新たな成長のトレンドに乗せる原動力として期待されている。そうした中、ネットワークを介してソフトウェアやハードウェアの機能を提供するクラウドサービスの活用によって、これまで ICT 投資や利用が困難であった中小企業が生産性を大幅に向上させる事例や、地方公共団体が行政事務や公共サービス提供を外部委託するための手段として活用する事例が急速に増加しつつある。

一方で、現在、クラウドサービス事業者によるサービス等に関する情報開示は必ずしも十分な状況とは言えず、ユーザとの間に情報の非対称性が存在しています。また、クラウドサービス事業者の安全・信頼性に対する不安を持つユーザも出てきています。このため、クラウドサービス事業者に対して情報開示を促進するとともに、クラウドサービスのうち安全・信頼性に係る情報を適切に開示しているものに関する認定制度の導入が求められていました。

このような中、総務省及び一般社団法人日本クラウド産業協会（以下「ASPIC」とします。）は、クラウドサービスの普及促進を推進してきました。

（1）「ASP・SaaS の安全・信頼性に係る情報開示認定制度」の創設

① ASP・SaaS 普及促進策に関する調査研究（平成 19 年 4 月 27 日）

総務省と ASPIC が共同で「ASP・SaaS の課題、安全・信頼性指針の策定及び情報開示認定制度を官民で検討すること等」の調査研究を行い、報告書をとりまとめました。

② ASP・SaaS 普及促進協議会の設立（平成 19 年 4 月 27 日）

前項の調査研究結果をとりまとめ具体的な施策を展開するため、総務省と ASPIC が合同で「ASP・SaaS 普及促進協議会」を設立しました。

③ 「ASP・SaaS における情報セキュリティ対策ガイドライン」の策定

（平成 20 年 1 月 30 日）

総務省では、「ASP・SaaS の情報セキュリティ対策に関する研究会」を開催し、その検討結果として「ASP・SaaS の情報セキュリティ対策に関する研究会報告書」及び「ASP・SaaS における情報セキュリティ対策ガイドライン」を公表しました。

④ 「ASP・SaaS 安全・信頼性に係る情報開示指針」の公表

（平成 19 年 11 月 27 日）

「ASP・SaaS 普及促進協議会」の傘下の「安全・信頼性委員会」の検討成果をもとに、総務省は「ASP・SaaS の安全・信頼性に係る情報開示指針」を公表しました。

⑤ 「ASP・SaaS の安全・信頼性に係る情報開示認定制度」の検討・立案

「ASP・SaaS 普及促進協議会」の傘下の「安全・信頼性委員会」で「ASP・SaaS の安全・信頼性に係る情報開示認定制度」の検討・立案を行いました。

以上のような背景を踏まえ、財団法人マルチメディア振興センター（以下、「FMMC」とします。）は ISO27001 をベースとした「ASP・SaaS の安全・信頼性に係る情報開示認定制度」（以下「認定制度」とします。）を平成 20 年 4 月に創設しました。

クラウドサービス情報開示認定機関（以下「認定機関」とします。）FMMC、クラウドサービス認定制度事務局

（以下「認定事務局」とします。）ASPIC として、クラウドサービス市場の発展に寄与してまいりました。

なお、平成 29 年 10 月に、認定機関は FMMC から ASPIC に移管され、ASPIC が認定制度を一元的に運営することになりました。

（2）クラウドサービス情報開示認定制度（IaaS・PaaS、データセンター）の創設

総務省と ASPIC が連携して設立した「データセンター促進協議会」にて平成 21 年より検討しました。

「データセンター促進協議会」は、「ASP・SaaS 普及促進協議会」と連携し、ISO27017 をベースとした「データセンター」、「IaaS・PaaS」の情報開示指針を策定し（平成 23 年 12 月総務省公表）、平成 24 年 9 月「IaaS・PaaS 情報開示認定制度」、「データセンター情報開示認定制度」を創設しました。

（3）認定制度高度化－「特定個人情報」、「医療情報」の創設－

「ASP・SaaS 普及促進協議会」は、認定制度高度化推進の検討を平成 28 年より行い、平成 29 年 3 月総務省より「特定個人情報を取扱うサービス」、「医療情報を取扱うサービス」に関する情報開示指針が公表されました。これをもとに認定機関 ASPIC は、平成 29 年 10 月「医療情報 ASP・SaaS 情報開示認定制度」、「特定個人情報 ASP・SaaS 情報開示認定制度」を創設しました。

（4）認定制度の拡充－「IoT」－

① IoT クラウドサービスリスクへの対応：ガイドライン

近年は IoT が急速に注目を集めるようになり、クラウドサービス事業者による IoT クラウドサービスの提供が増加してきました。

平成 29 年度、「ASP・SaaS 普及促進協議会」は、クラウドサービス事業者が IoT クラウドサービスに参入する際のリスクへの対応方針を検討しました。

この対応方針を盛り込む形で、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」の改訂が行われ総務省から公表されました。

（平成 30 年 7 月 31 日）（参考 1）。

② IoT クラウドサービスの情報開示指針

総務省は、ガイドラインの改訂をもとに、「IoT クラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」、「IoT クラウドサービスの安全・信頼性に係る情報開示指針（IaaS・PaaS 編）」を公表しました。（平成 30 年 10 月 26 日）（参考 2）

③ IoT クラウドサービスの情報開示認定制度

ASPIC は、この 2 つの情報開示指針をもとに、新たに「ASP・SaaS（IoT クラウドサービス）の安全・信頼性に係る情報開示認定制度」及び「「IaaS・PaaS（IoT クラウドサービス）の安全・信頼性に係る情報開示認定制度」の 2 制度を創設することとしました。（平成 30 年 12 月 1 日）

（参考１）「クラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）」の総務省公表資料

http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html

総務省
MIC Ministry of Internal Affairs and Communications

総務省トップ > 広報・報道 > 報道資料一覧 > 「クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）」の公表

報道資料

平成 30 年 7 月 31 日

「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」の公表

総務省は、今般、クラウド事業者が IoT サービスを提供する際のリスクへの対応方針を取りまとめたことから、「クラウドサービス提供における情報セキュリティ対策ガイドライン」（平成 26 年 4 月策定）を改定することとし、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」を策定しましたので、これを公表します。

あわせて、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」（案）に対する意見募集の結果を公表します。

1 概要

総務省では、平成 29 年 7 月より、特定非営利活動法人 ASP・SaaS・IoT クラウドコンソーシアムに委託し、「ASP・SaaS クラウド普及促進協議会」の下に設置された「クラウド事業者における IoT セキュリティ対策及び情報開示に関する検討会」（主査：佐々木良一　東京電機大学　教授）（構成員は別紙 1 のとおり）において、クラウド事業者が IoT サービスを提供する際のリスクへの対応方針について検討を行ってきました。

今般、検討結果を踏まえ、「クラウドサービス提供における情報セキュリティ対策ガイドライン」（平成 26 年 4 月策定）を改定することとし、あわせて、「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 月策定）を統合することとし、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」として取りまとめました。

また、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」（案）について、平成 30 年 6 月 7 日（木）から同年 7 月 6 日（金）までの間、意見募集を行った結果、6 件の意見が提出されました。提出された意見及びその意見に対する総務省の考え方を併せて公表することとします。

2　ガイドライン

「クラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）」は、別紙2PDFのとおりです。

3　提出された意見

提出された意見及びその意見に対する総務省の考え方は、別紙3PDFのとおりです。

4　資料の入手方法

別紙 1～別紙 3 の資料については、総務省ホームページ（http://www.soumu.go.jp）の「報道資料」欄に、本日（31 日（火））14 時を目途に掲載するほか、総務省サイバーセキュリティ統括官室（総務省９階）において閲覧に供するとともに配布します。また、別紙２及び別紙３については電子政府の総合窓口[e－Gov]（http://www.e-gov.go.jp）の「パブリックコメント」欄にも掲載します。

【関係報道資料等】

・「クラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）」（案）に対する意見募集

http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000149.html

連絡先

【連絡先】

サイバーセキュリティ統括官室

電話　：03-5253-5749（直通）

FAX　：03-5253-5752

メール　：cloud-security-gl_atmark_ml.soumu.go.jp

※迷惑メール防止のため、@を「_atmark_」と表示しています。メールをお送りになる際には、「_atmark_」を@に直してください。

（参考２）IoT クラウドサービスの安全・信頼性に係る情報開示指針追加の総務省公表資料

http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000216.html

総務省
MIC Ministry of Internal Affairs and Communications

報道資料

平成 30 年 10 月 26 日

「クラウドサービスの安全・信頼性に係る情報開示指針」における「IoT クラウドサービスの安全・信頼性に係る情報開示指針」の追加

総務省では、クラウドサービスの安全・信頼性を向上させるため、利用者によるクラウドサービスの比較・評価・選択等に資する情報の開示項目を示した 5 つの情報開示指針からなる「クラウドサービスの安全・信頼性に係る情報開示指針」を公表しています。

今般、クラウド事業者による IoT サービスの提供の増加等を踏まえ、クラウド事業者が IoT サービスに参入しようとする際のリスクへの対応方針を新たに盛り込む形で「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」の改訂がなされました。それに伴い、新たに「IoT クラウドサービスの安全・信頼性に係る情報開示指針」を策定しましたので、公表します。

1. 経緯

総務省では、IaaS、PaaS 及び ASP・SaaS（※1）等のクラウドサービスの普及に伴い、利用者によるクラウドサービスの比較・評価・選択等に資する情報に対するニーズに対応するため、ASPIC（※2）と合同で設立した「ASP・SaaS・クラウド普及促進協議会」（以下「協議会」という。）における検討を踏まえて、サービスに関する情報開示を推進するとともに、利用者によるサービスの比較・評価・選択等を容易にすることを目的として、「クラウドサービスの安全・信頼性に係る情報開示指針」と総称する以下の各情報開示指針を順次策定し、公表してきました。

【クラウドサービスの安全・信頼性に係る情報開示指針（平成 29 年 3 月改訂）】
・ASP・SaaS の安全・信頼性に係る情報開示指針（第 2 版）
・ASP・SaaS（特定個人情報取扱いサービス）の安全・信頼性に係る情報開示指針
・ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針
・IaaS・Paas の安全・信頼性に係る情報開示指針（第 2 版）
・データセンターの安全・信頼性に係る情報開示指針（第 3 版）

これらの各情報開示指針の策定・改定以降も、クラウドサービス市場は成長を続けて、社会に広く普及しており、提供されるサービスの利便性や質の向上が図られています。特に、近年は IoT が急速に注目を集めるようになり、ビジネス環境は急変し、本格的な IoT サービスの時代が到来しようとしているなかで、クラウド事業者による新たなサービスの開発・提供も広がりをみせています。こうした動向を踏まえ、新たに IoT クラウドサービス(※3)の安全・信頼性に係る情報開示項目を定めました。

※1: IaaS(Infrastructure as a Service)とは、サーバ、ハードディスク、ストレージ等の ASP・SaaS・PaaS に必要なハード基盤機能とデータセンターの複合機能をネットワーク経由で提供するサービスを指す。また、PaaS(Platform as a Service)とは、狭義にはシステム基盤機能、ネットワーク基盤機能、開発・実行基盤機能をネットワーク経由で提供するサービスを指し、広義にはデータセンター及び IaaS を包含するサービスをいう。なお、IaaS 及び PaaS を総称して、ホスティングサービスという場合もある。ASP(Application Service Provider)・SaaS(Software as a Service)とは、特定及び不特定ユーザが必要とするシステム機能を、ネットワークを通じて提供するサービス、あるいは、そうしたサービスを提供するビジネスモデルのことである。

※2:特定非営利活動法人 ASP・SaaS・IoT クラウドコンソーシアム

※3:「IoT クラウドサービス」とは、IoT 機器(センサーやアクチュエータ)を使ったクラウドサービスのことをいう。

2. 公表資料

・IoT クラウドサービスの安全・信頼性に係る情報開示指針(ASP・SaaS 編)

・IoT クラウドサービスの安全・信頼性に係る情報開示指針(IaaS・PaaS 編)

・(参考)クラウドサービスの安全・信頼性に係る情報開示指針

※資料の入手方法

公表資料については、総務省ホームページ(http://www.soumu.go.jp)の「報道資料」欄に、本日(14 時頃を予定)に掲載するほか、総務省情報流通振興課(総務省 11 階)において閲覧に供するとともに配布します。

【関係報道資料等】

・「クラウドサービス提供における情報セキュリティ対策ガイドライン(第 2 版)」の公表

http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00001.html

連絡先

総務省情報流通行政局情報流通振興課

連絡先:ryutsu_shinko_atmark_ml.soumu.go.jp

TEL:03-5253-5748

FAX:03-5253-5752

(注)迷惑メール防止のため、メールアドレスの一部を変えています。「_atmark_」を「@」に置き換えてください

認定制度の基本的な考え方は、以下のとおりです。

（1）ASP・SaaS（IoT クラウドサービス）のユーザの視点に立った制度である。

- ASP・SaaS（IoT クラウドサービス）についての高度な専門知識を持たないユーザでも、審査基準や審査内容が理解できます。
- ユーザによる ASP・SaaS（IoT クラウドサービス）及び事業者の評価・選択等が容易になります。

（2）発展期にある ASP・SaaS（IoT クラウドサービス）市場の拡大を促進する制度である。

- ユーザによる ASP・SaaS（IoT クラウドサービス）及び事業者への信頼性が高まります。
- ASP・SaaS（IoT クラウドサービス）を提供しようとする中小企業等の市場への参入促進につながります。

（3）事業者から適切に情報開示されていることを認定する制度である。

- 安全・信頼性に係る実施水準や状態に関する情報が、ASP・SaaS（IoT クラウドサービス）を提供する事業者から適切に開示されていることを認定する制度であり、安全・信頼性に係る実施水準や状態を認定するものではありません。

（4）ASP・SaaS（IoT クラウドサービス）を認定対象とする制度である。

- 安全・信頼性に係る情報開示が適切に行われている ASP・SaaS（IoT クラウドサービス）を対象として認定する制度であり、事業者の経営状況等を認定するものではありません。

3．認定制度の意義

ユーザ、事業者、社会の 3 つの視点からみた本認定制度の意義は、以下のとおりです。

（1）ASP・SaaS（IoT クラウドサービス）を利用するユーザにとっての意義

ASP・SaaS（IoT クラウドサービス）に係る情報開示が豊富になるとともに、情報開示項目が共通化されることで、サービス及び事業者の比較・評価・選択が容易になります。

（2）ASP・SaaS（IoT クラウドサービス）を提供する事業者にとっての意義

認定によって提供するサービスの認知度が高まり、ユーザ獲得の機会が広がります。

（3）社会全体としての意義

認定制度の実施により、ASP・SaaS（IoT クラウドサービス）が産業、生活、社会システム等の経済社会活動の多くの分野に普及・定着し、安全・信頼性の高い効果的・効率的な社会情報基盤の形成が進みます。

4．認定に係る申請

（1）申請対象

申請対象はASP・SaaS（IoT **クラウドサービス**）であり、既に提供を開始しているものに限ります。

（2）申請資格

申請できるのは、特定又は不特定ユーザが必要とする情報通信システム機能を、ネットワークを通じてサービス提供するASP・SaaS（IoTクラウドサービス）事業者です。

ア．申請者が自らユーザと契約するのであれば、データセンター、コールセンター等へ業務の一部を委託する場合であっても申請することができます。

イ．外国法人については、日本語で情報開示が行われている場合に申請することができます。

ウ.ユーザと契約する販売代理店あるいは仲介代理店等については､ASP･SaaSのサービス提供元の事業者が、販売代理店あるいは仲介代理店等の名称、本店の所在地、本店の連絡先等の情報を記載することにより申請することができます。

エ．他事業者のASP・SaaS（IoTクラウドサービス）をOEM販売する事業者や、サービス提供元の事業者とは異なる独自のサービスサポートを行う販売・仲介代理店等については、当該サービスの申請を独自に行うことができます。

オ．「ASP・SaaS（IoTクラウドサービス）の安全・信頼性に係る情報開示認定制度運用規程」第17条（認定の取消し）によって認定を取り消したサービスは、当該取消しの日から１年以上経過している場合に申請することができます。

（3）申請単位

申請および認定は、原則として独立して提供されるサービス単位とします。ただし、複数のアプリケーション・サービスや基盤（プラットフォーム）サービスを統合して提供している場合、および同一サービスであっても、複数の安全性、信頼性等のサービスレベルを設定して提供している場合は、以下のとおりとします。

なお、サービスの提供形態については事業者により様々なケースが想定されるため、疑問の点があれば窓口までお問合せください。

ア．複数のサービスを統合して提供している場合

（ア）複数のアプリケーション・サービスや基盤サービスを統合して提供している場合、以下の条件をすべて充たしているときは、統合したものを一つの申請単位とすることができます。

① 統合するサービスの業務内容に関連性があり、かつ、別表２の「ASP･SaaS区分」（本資料の最終ページを参照下さい）の同一区分内にあること。

② 各サービスの開示すべき情報（申請書Bの「申請内容」）の内容が同じであり、それぞれのサービス毎に分けて記述する必要がないこと。

③ 統合するサービスとしての利用契約があること。

（イ）これ以外の場合は、統合したものではなく、それぞれを一つのサービスとします。ただし、各サービスの開示情報の内容（申請書Bの「申請内容」）が同じであり、かつ統合するサービスとしての利用契約があるときは、サービス単位を個別に審査します。

※（ア）の②、③の条件は充たすが、①については該当しない場合等を言う。

イ．同一サービスにおいて異なるサービスレベルで提供している場合

同一サービスであっても、複数の安全性、信頼性等のサービスレベルを設定して提供しており、各サービスレベルの開示情報の内容（申請書Bの「申請内容」）が異なる場合は、それぞれを申請単位とします。

（4）申請書類

申請サービスごとに、日本語で記述された以下の書類を提出していただきます。

また、この他に申請書Aと申請書Bの電子ファイルを格納したCD-R、提出書類及び資料内訳書等が必要です。

※申請書類の詳細、申請書類の綴じ込み方法等については、本認定制度のサイト（https://www.aspicjapan.org/nintei /asp-iot/）の関連ページをご参照下さい。

ア．申請書A、申請書B

新規申請時や更新申請時には、申請書A（フェースシート）、申請書B（情報開示内容の詳細）を提出していただきます。

申請書Bでは「申請内容」欄と「添付書類等」欄のそれぞれについて、以下に留意した記述が必要です。

- 「申請内容」欄では、必須開示項目は全て記述してください。選択開示項目の記述は任意となっていますが、認定制度の趣旨を勘案し、出来る限り記述するようにしてください。
- 「添付書類等」欄では、必ず「申請内容」欄の記述を疎明する（裏付ける）資料名称とその中の記載箇所（ページ、章節等）を記述してください。

イ．申請書Aに関わる添付書類

申請者（企業等）の実在を証明する登記事項証明書もしくはその他の申請者の実在を証明する公的書類、の提出が必要です。

なお、「代表者氏名」欄に記載された方に代表権がない場合、添付資料として申請事業者に所属し、事業責任者であることを疎明できる資料の提出が必要です。

（注1）申請者（企業等）の実在を証明する資料の具体例

- 法人の場合： 商業・法人登記簿謄本
- 個人事業主の場合： 旅券、運転免許証、住民基本台帳カードその他官公署が発行した免許証、許可証又は資格証明書等（本人の写真が貼付されたものに限る。）のうちいずれか1つの写し
- 外国語で記載されている場合には原本及び訳文

（注2）商業・法人登記簿謄本については、原本の提出を必要とするが、複数サービスを申請する場合の2サービス目以降は、写し（コピー）も可とする

ウ．申請書Bに関わる添付書類

（ア）申請書Bの各項目の申請内容については、必須開示項目／選択開示項目にかかわらず、その実施水準や内容に係る開示情報を疎明するための資料の提出が必要です。ただし、申請内容が「実施なし」、「開示なし」等の場合は、疎明は不要とします。

（イ）データセンター等に外部委託している場合、外部委託先に関わる申請書Bの記述に対し、外部委託先による公表資料もしくは外部委託先の事業担当責任者の署名のある資料を提出してください。

（ウ）疎明する資料としてウェブページを用いる場合は、URL 及び日付を付したハードコピーの添付が必要です。添付資料が大量ページとなる場合、表紙、目次、および疎明に必要なページを含む抜粋資料も可とします。

（5）送付方法

申請者は、郵便書留により申請書類の送付を行うことができます。

※ 申請方法の詳細については、本認定制度のサイト（https://www.aspicjapan.org/nintei /asp-iot/）の関連ページをご参照下さい。

（6）申請受付

申請は、随時受け付けます。

（7）審査手数料

申請時には、別表１（本資料の最終ページを参照下さい。）に定める審査手数料をお支払いください。なお、この審査手数料は、認定・非認定にかかわらず、返還いたしません。

審査手数料は、認定機関から形式審査が完了した旨を通知しますので、その後１週間以内を目途に指定の銀行口座にお振込み下さい。振込みが確認でき次第、書類審査を開始します。

なお、事業者名称およびサービス名称等の変更により、認定証に変更を生じた場合は、認定証の再発行手数料をお支払いいただきます。

５．審査対象項目と審査基準

（1）審査対象項目

認定の審査対象項目は、「IoT クラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）（総務省；平成 30 年 10 月 26 日公表）で示されている情報開示項目に基づきます。

なお、審査対象としている情報開示項目は、以下のような構成となっています。

ア．事業者の安全・信頼性に関する情報開示項目

- 開示情報の時点
- 事業所・事業
- 人材
- 財務状況
- 資本関係・所属団体
- コンプライアンス

イ．サービスの安全・信頼性に関する情報開示項目

- サービス基本特性
- アプリケーション等
- ネットワーク
- 提供端末
- 推奨端末
- ハウジング（サーバ設置場所）
- サービスサポート）

（2）審査基準

審査対象となる情報開示項目は、「必須開示項目」（必ず情報開示していただく項目）と「選択開示項目」（情報の開示は任意である項目）に分かれており、以下の基準により審査します。

なお、「選択開示項目」については、これらの開示の有無により認定もしくは非認定とするものではありま

せん。

ア.「必須開示項目」の全てについて適切な情報開示を行っており、かつ「必須開示項目」の中で特にユーザにとって重要な「一定の要件を考慮すべき項目」（下表を参照）の全てについて一定の要件を満たす場合（対策・措置等を行っている場合、最低水準数値以上の場合）は認定する。

イ．ア項の基準に適合しない場合は非認定とする。

表　一定の要件を考慮すべき項目の内容

【対策・措置などを行っていない場合に非認定とする項目】		
	コンプライアンス	情報セキュリティに関する規程等の整備
	アプリケーション等	死活監視
		ウィルス対策
		管理者権限の運用管理
		ＩＤ・パスワードの運用管理
		記録（ログ等）
		セキュリティパッチ管理
	ネットワーク	ファイアウォール
		ユーザ認証
		IoT 機器認証
	サービスサポート	連絡先
		メンテナンス等の一時的サービス停止時の事前告知
		障害・災害発生時の通知
【最低水準数値以下の場合に非認定とする項目】		
	サービス基本特性	サービス（事業）変更・終了時等の事前告知

６．認定に係る審査手順

受理した申請書類をもとに、次により審査を行い、結果を通知します。

（1）形式審査

申請者より提出された申請書類（申請書A、申請書B、申請内容を疎明する関係資料、申請者の実在を証明する公的書類等）が指定どおり提出されているかを審査します。

（2）書類審査

申請書類をもとに、「審査対象項目と審査基準」で示した審査基準に基づき書類審査を行います。

なお、申請内容に明らかに誤解に基づく記述、記入漏れ、不鮮明な記述がある場合は照会することがあります。

（3）調査

審査上必要があるときは、申請者に対し、その営業所、事務所その他事業場における調査の受け入れを求めることがあります。

（4）認定審査委員会

認定にあたっては、認定機関内に設置する学識経験者及び民間有識者等により構成される認定審査委員会を開催し、あらかじめ意見を聴くことがあります。

（5）審査結果の通知

審査終了後、認定又は非認定の結果を通知します。
なお、非認定の場合には、改善等が求められる情報開示項目等について説明を付すこととします。

7．認定サービスの公表

認定したサービスについて、以下の情報を公表します。

（1）認定サービスの基本内容

認定番号、サービス名称、事業者名称、認定年月日を認定サービス一覧表の形で公表します。

（2）認定サービスの開示内容

申請書Bの“申請内容”欄については、申請者が記述した内容を公表します。
ただし、申請者からその一部につき公表を留保したい旨の申し出があった場合、認定機関において正当な理由であると判断したときは、必要な期間、公表を留保することがあります。

- 「必須開示項目」及び「選択開示項目」は、申請者が記述した内容をそのまま公表します。
- 添付資料に関わる内容については一切公表しません。
- 公表を留保する期間は、申請者の申し出に基づいて判断します。また、期間を更新する必要がある場合についても同じとします。

8．認定証・認定マークの発行・使用

認定したASP・SaaS（IoTクラウドサービス）のサービスに対して、認定証及び認定マーク（図1、図2参照）を発行します。

- 認定証及び認定マークの有効期間は、認定日より2年間とします。
- 認定サービスを提供する事業者は、認定期間中、認定マークをウェブページ、広告媒体、取引書類等に表示することができます。有効期間経過後は、速やかに使用を中止しなければなりません。
- 認定マークの使用に関しては、「ASP・SaaS（IoTクラウドサービス）の安全・信頼性に係る情報開示認定制度運用規程」第10条（認定マークの使用）に従っていただきます。

図１　認定証

（注）認定番号、サービスの名称、事業者の名称、認定期間、発行日は、サンプル例示となっています。

図２　認定マーク

（注）認定マークはロゴと認定番号から構成されます。なお、認定番号の IoT は識別子、上４桁は認定サービス通番、下４桁は認定年月（西暦）を表します。

９．認定の更新及び変更の届出

（１）認定の更新

認定の更新を求める場合は、認定の有効期間満了日の 60 日前から 30 日前までに手続を行い、更新審査を受ける必要があります。

・上記の期間内に更新の申請をしたときは、認定の効力は、有効期間後も更新を決定するまでの間、継続します。

・更新申請の際には、更新申請書及び添付資料を提出していただきます。また、「ASP・SaaS（IoT クラウドサービス）の安全・信頼性に係る情報開示認定制度運用規程」第 10 条（認定マークの使用）に照らして、適切にマークを使用したことについて自己申告（様式は任意）していただきます。

・更新の際の審査は、新規申請時点から変更のあった項目を対象とします。
なお、変更のあった項目については、新規申請時の記述内容と変更後の内容を併記し、それらを朱書きしてください。

・「事業者名称」「事業者の代表者氏名」および「事業者の住所」が変更になった場合、事業者の「商業・法人登記簿謄本」の再提出をしてください。

・　申請書Ｂの記載内容に変更がある場合は、当該箇所の変更を証明できる疎明資料を添付してください。

・更新手続き後、認定の有効期間内に変更内容を疎明する資料の補正あるいは変更処理ができないときは、更新できない場合があります。

・　申請諸Ｂの記載内容には変更がないものの、当初に添付した疎明資料に変更があった場合、期間限定資料や改版がなされた資料がある場合は、最新版の疎明資料を提出してください。

（２）変更の届出

認定期間内に以下に該当する変更事由が発生したときは、指定する様式により、遅滞なく届出を行ってください。

・　申請書の記述内容の変更

・　登記事項証明書その他の申請者の実在を証明する公的書類の記載内容の変更

・　その他認定機関が指定する書類の記述内容の変更

（３）サービス終了の届出

認定期間内に当該認定サービスの提供を終了したときは、指定する様式により、遅滞なく届出を行ってください。また、その際には、認定証も同時に返納していただきます。

１０．申請書類の返却

提出された申請書類は認定の有効期間内においては、認定事務局内で保管し、次の場合に返却します。

（１）返却する場合

・　非認定となったとき

・　更新せず、認定の有効期間が終了したとき

・ 運用規定第 17 条に基づき、認定が取り消されたとき

（2）返却する申請書類

次の資料を除く申請書類一式を申請担当者に返却します。

・ 申請書Ａ
・ 認定サービスとして公開された申請情報

（3）更新時の返却資料

更新時においては、変更内容と提出された疎明資料を照合し、不要となった旧資料を返却します。

１１．認定の取消し等

（1）事業者の通知・報告

認定期間内に障害によるサービスの停止、個人情報又は企業情報の漏洩その他認定サービスの安全・信頼性を損なう恐れのある緊急事態が発生又は発覚したときは、認定機関に速やかにその旨を通知し、経過を報告していただきます。

・ 「障害によるサービスの停止」は、大規模な性能劣化または何らかの障害により、事業者がサービス停止と判断したものを指します。
・ メンテナンスの事前告知の通知時期が、申請書の「メンテナンス等の一時的サービス停止時の事前告知」で開示した時期よりも短い場合には、「認定サービスの安全・信頼性を損なう恐れのある緊急事態」に該当すると考えられ、通知・報告が求められます。

（2）事業者への調査及び改善要請

認定機関が、認定制度の適正な運営のために必要があると判断したときは、認定サービスを提供する事業者に対して、説明及び資料の提出、調査の受入れ等を求めることがあります。
また、認定サービスを提供する事業者に対して改善その他必要な措置を要請することがあります。その場合、認定機関のウェブページ等にその旨を公表することがあります。

（3）認定の取消し

認定サービスを提供する事業者が、次のいずれかに該当する場合には、その認定を取り消すことがあります。

① 審査基準に適合しなくなったと認められるとき
② 不正の手段により認定を受けたことが明らかになったとき
③ 認定サービス以外のサービスに認定マークを使用したとき
④ 認定サービスと認定サービス以外のサービスとを明確に区分せずに認定マークを使用したとき
⑤ 電磁的方法により認定マークを使用する場合に、認定機関が指定する URL（https://www.aspicjapan.org/nintei /asp-iot/）にリンクを設置しなかったとき
⑥ 認定マークの使用に際して、色を変更したり、一部のみを掲載したとき
⑦ 申請の記載内容に変更があったにもかかわらず、正当な理由なく届出をしなかったとき
⑧ 正当な理由なく、緊急事態の通知・報告を遵守しなかったとき
⑨ 正当な理由なく、認定機関の求める調査に応じない場合又は当該調査に虚偽の説明又は資料の提出をした

とき

⑩ 正当な理由なく、改善の要請に従わないとき

⑪ 不法行為及び法令違反行為を行ったとき

⑫ 認定サービスに係る事業譲渡、又は認定サービスを提供する事業者の合併、分割もしくは相続があった場合において、サービスの認定時の提供体制に変動が生じ、サービスの維持継続に疑義が生じたとき

１２．守秘義務及び免責

（1）守秘義務

認定機関、認定審査委員会を構成する有識者及び認定事務の委託を受けた者（以下「認定機関等」という。）は、認定制度に関連して知り得た事業者に係る非公知の情報（以下「秘密情報」という。）を、当該事業者の事前の承諾なく第三者に開示せず、認定制度の運営に必要な目的以外に使用しないものとします。

ここで、秘密情報には、以下に掲げる情報を含まないものとします。

① 事業者から知得する以前に自己が所有していたもの

② 事業者から知得した後に、自己の責によらず公知公用となったもの

③ 正当な権限を有する第三者から、合法的な手段により秘密保持の義務を伴わずに知得したもの

④ 認定機関等が独自に創作したもの

なお、認定機関等は、上述のような守秘義務を負いますが、法律に基づく強制処分又は裁判所の命令が執行された場合は、当該処分又は命令に定められた範囲において秘密保持の義務を負わないものとします。

（2）免責

認定機関等は、認定制度の運営に関して直接又は間接に生じた事業者又は第三者の損害について、その内容、態様の如何にかかわらず一切の責任を負わないものとします。ただし、認定機関等の故意又は重過失による場合はこの限りではありません。

また、認定サービスに関し、事業者と第三者との間で紛争を生じた場合は、当事者が自己の費用と責任において解決するものとし、認定機関等は一切の責任を負わないものとします。

１３．問合せ窓口

問合せ窓口は、次のとおりです。

- 名　称：　クラウドサービス情報開示認定機関事務局
- 受付時間：　9：30～17：00（土日、祝祭日を除く）
- メールアドレス：　aspic_atmark_cloud-nintei.org
  （スパムメール防止のため、@を「_atmark_」と表示しています。
  メールをお送りになる際には、「_atmark_」を@に直してください。）
- ホームページ：　https://www.aspicjapan.org/nintei /asp-iot/
- 電　話：　03-6662-6854
- ファックス：　03-6662-6347
- 住　所：　東京都品川区西五反田 7-3-1　たつみビル 2F（〒141-0031）

（別表１）

① 審査手数料 ＜新規申請費用＞ 1サービスにつき 209,000円 （消費税込み）

（内訳）審査手数料（税別）190,000円+消費税（10%）19,000円

② 更新審査手数料 ＜2年ごとに更新する際の費用＞

1サービスにつき 104,500円 （消費税込み）

（内訳）更新審査手数料（税別）95,000円+消費税（10%）9,500円

③ 認定証再発行手数料 1サービスにつき 10,450円 （消費税込み）

（内訳）更新審査手数料（税別）9,500円+消費税（10%）950円