報道資料

実はここにも 総務省
MIC Ministry of Internal Affairs and Communications

参考資料

平成１９年１１月２７日

「ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針」の公表について

総務省では、地方公共団体や中小企業など一般の利用者によるＡＳＰ(注1)・ＳａａＳ(注2)の評価・選択を支援するため、この度、「ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針（第１版）」（別紙）を取りまとめましたので、公表します。

本指針は、総務省で本年６月から開催中の「ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会」の検討経過を逐次踏まえつつ、総務省とＡＳＰＩＣ Ｊａｐａｎ(注3)との合同で設立した「ＡＳＰ・ＳａａＳ普及促進協議会」において策定したものです。

（注1）Application Service Provider の略。（注2）Software as a Service の略。
（注3）ASP Industry Consortium Japan：ASP を推進する特定非営利活動法人。

１　経緯・目的

ＡＳＰ・ＳａａＳの普及促進は、「経済財政改革の基本方針２００７」（平成１９年６月１９日閣議決定）にも掲げられた政策課題の１つとなっています。

ＡＳＰ・ＳａａＳの利用ニーズは高まっているが、「ＡＳＰ・ＳａａＳとはどのようなサービスなのか」、「どのような事業者が提供しているのか」、「評価・選択はどうすれば良いのか」といった評価・選択するための情報がない状況にあります。

そこで、「ＡＳＰ・ＳａａＳ普及促進協議会」において検討を進め、地方公共団体や中小企業など一般の利用者によるＡＳＰ・ＳａａＳの評価・選択を支援するため、「ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針」の策定に至ったものです。

この指針は、ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示を必須の項目と選択の項目に分け、情報開示項目を共通かつ豊富にするとともに、利用者によるＡＳＰ・ＳａａＳの比較、評価、選択等を容易にすることを目的としています。

２　今後の予定

必須項目を開示し、かつ特定の項目について一定以上の要件を充たしているＡＳＰ・ＳａａＳについては、その申請を受けて「認定」を行う仕組みを準備していきます（運用開始は平成２０年春を目途）。

「認定」の審査に当たっては、ＡＳＰ・ＳａａＳに関する有識者や知見を有する団体、「地域情報化アドバイザー」等で構成される審査委員会を設けることを想定しています。

また、総務省で開催中の「ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会」が近く取りまとめる予定の報告書（案）、パブリックコメント結果等を踏まえ、情報セキュリティ対策の詳細について、適宜、本指針の見直しを行っていきます。

【関連報道発表】
・ＡＳＰ・ＳａａＳ普及促進協議会の設立
（http://www.soumu.go.jp/s-news/2007/070427_14.html）
・ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会
（http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/asp_saas/index.html）
・経済財政改革の基本方針２００７
（http://www.keizai-shimon.go.jp/minutes/2007/0619/item1.pdf）

（お問い合せ先）
総務省情報通信政策局情報通信政策課
担当：中里課長補佐、西村
電話：03－5253－5735
FAX　：03－5253－5740

【別紙】　ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針（第１版）

事業者	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
開示情報の時点	開示情報の日付	開示情報の年月日		必須		
事業所・事業						
事業所等の概要	事業者名	事業者の正式名称（商号）		必須		
	設立年、事業年数	事業者の設立年、設立後の事業年数		必須		
	事業所	事業者の本店所在地、事業所数、主な事業所の所在地		必須		
事業の概要	主な事業の概要	事業者の主要な事業の概要		必須		
人材						
経営者	代表者	代表者名 代表者の写真・年齢・経歴（学歴、業務履歴、資格など）		代表者名は必須 他は選択		
	役員	役員数、役員氏名		選択		
従業員	従業員数	正社員の人数		選択		
財務状況						
財務データ	売上高	直近の決算期の事業者全体の売上高（単独ベース）		必須		
	経常利益	直近の決算期の事業者全体の経常利益額（単独ベース）		選択		
	資本金	直近の決算期の事業者全体の資本金（単独ベース）		必須		
	自己資本比率	直近の決算期の事業者全体の自己資本の比率（単独ベース）	○自己資本比率 ＝[自己資本]/[総資産]	選択		
	キャッシュフロー対有利子負債比率	直近の決算期の事業者全体のキャッシュフロー対有利子負債比率（単独ベース）	○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]	選択		
	インタレスト・カバレッジ・レシオ	直近の決算期の事業者全体のインタレスト・カバレッジ・レシオ（単独ベース）	○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]	選択		
財務信頼性	上場の有無	株式上場の有無、株式上場の場合は市場名		選択		
	財務監査・財務データの状況	会計監査人による会計監査、会計参与による監査、中小企業会計によるチェックリストに基づく財務データ、いずれでもない、の中から該当状況を選択		選択		
	決算公告	決算公告の実施の有無		選択		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

事業者	【開示項目】		【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
資本関係・取引関係							
	資本関係	株主構成	大株主名（上位5名程度）及び各々の株式保有比率		選択		
	取引関係	大口取引先	（可能であれば）大口取引先の名称		選択		
		主要取引金融機関	（可能であれば）主要取引金融機関の名称		選択		
		所属団体	所属している業界団体、経済団体等の名称		選択		
コンプライアンス							
	組織体制	コンプライアンス担当役員	コンプライアンス担当の役員名		選択		
		専担の部署／会議体	コンプライアンスを担当する社内の部署・会議体の有無、部署等がある場合には部署名・会議名		選択		
	文書類	情報セキュリティに関する規程等の整備	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 文書類がある場合は文書名、及び同文書の経営陣による承認の有無 （文書類の内容は開示しないが、認定の審査書類として提出が求められる）		必須	○	情報セキュリティ規程等の文書類が無い場合は非認定
		勧誘・販売に関する規程等の整備	勧誘・販売に関する基本方針・規程・マニュアル等の有無 文書類がある場合は文書名、及び同文書類の経営陣による承認の有無 （文書類の内容は開示しないが、認定の審査書類として提出が求められる）		選択		
		ASP・SaaSサービスの苦情対応に関する規程等の整備	ASP・SaaSサービスの苦情処理に関する基本方針・規程・マニュアル等の有無 文書類がある場合は文書名、及び同文書類の経営陣による承認の有無 （文書類の内容は開示しないが、認定の審査書類として提出が求められる）		必須		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

サービス	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
サービス基本特性						
サービス内容	サービス名称	申請したASP・SaaSサービスの名称		必須		
	サービス開始時期	申請したASP・SaaSサービスのサービス開始年月日 （サービス開始から申請時までの間に大きなリニューアル等が行われた場合は、その年月日も記述）		必須		
	サービスの基本タイプ	アプリケーションサービス、ネットワーク基盤サービス、ASP基盤サービス、その他サービス、の中から該当タイプを選択		必須		
	サービスの内容・範囲	申請したASP・SaaSサービスの内容・特徴 他の事業者との間でサービス連携を行っている場合はその内容		必須		
	サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲 （特に決まっていない、相談に応じて決める等の場合は、その旨を記述）		必須		
サービスの変更・終了	サービス（事業）変更・終了時の事前告知	利用者への通知時期、通知方法 （通知時期は1ヶ月前、3ヶ月、6ヶ月、12ヶ月等の単位で記述）		必須	○	利用者への通知時期が1ヶ月未満の場合は非認定
	サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無、基本方針がある場合はその概略 契約終了に伴うユーザへの対応策（代替サービスの紹介等）の有無、対応策がある場合はその概略 契約終了時の情報資産（ユーザデータ等）の返却責任の有無		必須		
	サービス（事業）変更・終了に係る問合せ先	問合せ先（通常の苦情等の問合せ窓口も含む）の有無、問合せ先がある場合は名称・受付時間		必須	○	問い合わせ先が無い場合は非認定
サービス料金	課金方法	従量部分、固定部分別の課金方法		必須		
	料金体系・金額	初期費用額、月額利用額、最低利用契約期間		必須		
	解約時ペナルティ	解約時違約金（ユーザ側）の有無、違約金がある場合はその額		必須		
	利用者からの解約事前受付期限	利用者からのサービス解約の申請時の受付期限の有無、ある場合はその期限（何日・何ヶ月前かを記述）		必須		
サービス品質	サービス稼働設定値	サービス提供時間・サービス稼働時間・稼働率の実態または最低限達成しようとしている目標値 サービス停止の事故歴	○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 ＝[実サービス稼動時間] ／[サービス提供時間]	必須	○	サービス稼働率が一定水準未満の場合は非認定 （「ASP・SaaSの情報セキュリティ対策に関する研究会」の検討結果を参考に、アプリケーションごとに必要な数値を別途設定する予定）
	サービスパフォーマンスの管理	機器障害やシステム遅延の早期検知方法 （検知の場所、検知のインターバル、画面の表示チェック等の検知方法） サービスのパフォーマンス把握方法 （検知の場所、検知のインターバル、画面の表示チェック等の把握方法）		選択		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

サービス	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
サービス品質	サービスパフォーマンスの増強	ネットワーク・機器等の増強判断基準あるいは計画の有無、判断基準や計画がある場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要		選択		
	認証取得、監査実施	プライバシーマーク、ISMS、ITSMSの取得、18号監査（米ではSAS70）の監査報告書作成の有無、上記がある場合は認証名あるいは監査の名称		選択		
	個人情報の取扱い	個人情報を収集する際の利用目的の明示		必須		
	脆弱性診断結果	診断の対象（アプリケーション、OS、ハードウェア等） 診断の頻度、診断の結果、対策が必要な部分に対する対応状況（対象ごとに）		選択		
	バックアップ対策	バックアップ実施インターバル 世代バックアップ（何世代前までかを記述）		必須		
	バックアップ管理	バックアップ確認のインターバル		必須		
	受賞・表彰歴	ASP・SaaSサービスに関連する各種アワード等の受賞歴		選択		
	SLA （サービスレベル・アグリーメント）	本指針に関連するSLAが契約書に添付されるか否か		必須		
サービス利用量	利用者数	申請したASP・SaaSサービスの利用者ライセンス数 （同時接続ユーザ数か、実ユーザ数かも明示）		選択		
	代理店数	申請したASP・SaaSサービスの取扱い代理店数		選択		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

サービス	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
アプリケーション、基盤、ストレージ等						
内容	中核的ソフトウェア	中核的アプリケーションの名称と概要		必須		
	中核的ソフトウェアの提供事業者	中核的アプリケーションの提供事業者名		必須		
連携・拡張性	他システム等との連携方法	連携が可能な標準的なAPIの使用状況、標準的なものを使用している場合はそのAPI名、標準的なものを使用していない場合はAPIの公表の可否		選択		
セキュリティ	死活監視（ソフトウェア、機器）	死活監視の有無、死活監視を行っている場合は監視の対象（アプリケーション、基盤、ストレージ等）、及び死活監視の対象ごとの監視インターバル、監視時間、通知時間	○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） ○監視時間 ＝[実監視時間]/[サービス提供時間] ○通知時間： 死活監視結果を指定された管理者に通知するまでの時間	必須	○	死活監視が無い場合は非認定
	障害監視（ソフトウェア、機器）	障害監視の有無		必須		
	時刻同期	システムの時刻同期方法		必須		
	ウイルス対策	ウイルス対策の有無、対策がある場合はパターンファイルの更新間隔（ベンダーリリースからの時間）		必須	○	ウイルス対策が欠けている場合は非認定
	管理者認証	管理者権限の登録・登録削除の正式な手順の有無 （内容は開示しないが、手順を示した規程等は認定の審査書類として提出が求められる）		必須	○	手順が無い場合は非認定
	記録（ログ等）	利用者の利用状況、例外処理及びセキュリティ事象の記録（ログ等）取得の有無、記録（ログ等）がある場合にはその保存期間		必須	○	記録（ログ等）取得が無い場合は非認定
	ID・パスワードの運用管理	IDやパスワードの運用管理方法の規程の有無 （内容は開示しないが、運用管理方法を示した規程等は認定の審査書類として提出が求められる）		必須	○	規程が無い場合は非認定
	セキュリティパッチ管理	パッチの更新間隔（ベンダーリリースからパッチ試験開始までの時間）		必須	○	管理が無い場合は非認定
ネットワーク						
回線	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類 ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲		必須		
	推奨帯域	推奨帯域の有無、推奨帯域がある場合はそのレベル		必須		
	推奨端末	パソコン、携帯電話等の端末の種類、利用するブラウザの種類		必須		
セキュリティ	ファイアウオール	ファイアウオールの有無		必須	○	ファイアウオールが無い場合は非認定
	ネットワーク不正侵入検知（不正パケット、サーバへの不正侵入）	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		必須		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

サービス	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
セキュリティ	ネットワーク監視	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		選択		
	ウイルスチェック	メール、ダウンロードファイル、サーバ上のファイルアクセスに対する対処の有無、対処がある場合はパターンファイルの更新間隔（ベンダーリリースからの時間）		必須	○	ウイルスチェック対策が無い場合は非認定
	ユーザ認証	認証基盤を通じた個人認証（Web、サーバ）/IDパスワードによるユーザの認証の有無、認証がある場合は認証の方法		必須	○	ユーザ認証が無い場合は非認定
	なりすまし対策（事業者サイド）	第三者による自社を装ったなりすましに関する対策の実施の有無、対策がある場合は認証の方法		必須	○	なりすまし対策が欠けている場合は非認定
	その他セキュリティ対策	情報漏洩対策、データの暗号化等の対策について自由に記述		選択		
ハウジング（サーバ設置場所）						
施設建築物	建物形態	データセンター専用建物か否か		必須		
	所在地	国名、（日本の場合は）地域ブロック名（例：関東、東北）		必須		
	耐震・免震構造	耐震数値 免震構造、制震構造の有無		必須		
非常用電源設備	無停電電源	無停電電源装置（UPS）の有無、UPSがある場合は電力供給時間		必須		
	給電ルート	別の変電所給電ルートで2ヵ所以上が確保されているか否か（自家発電機、UPSを除く）		必須		
	非常用電源	非常用電源（自家発電機）の有無、非常用電源がある場合は連続稼働時間の数値		必須		
消火設備	サーバルーム内消火設備	自動消火設備の有無、ある場合はガス系消火設備か否か		必須		
	火災感知・報知システム	火災検知システムの有無		必須		
避雷対策設備	直撃雷対策	直撃雷対策の有無		必須		
	誘導雷対策	誘導雷対策の有無、対策がある場合は最大対応電圧の数値		必須		
空調設備	十分な空調設備	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		選択		
セキュリティ	入退館管理等	入退室記録の有無、入退室記録がある場合はその保存期間		必須		
		監視カメラの有無、カメラがある場合は監視カメラ稼働時間、監視カメラの監視範囲		必須		
		個人認証システムの有無		必須		
	媒体の保管	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 保管管理手順書の有無		選択		
	その他セキュリティ対策	その他特筆すべきセキュリティ対策を自由に記述 （破壊侵入防止対策、防犯監視対策等）		選択		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。

サービス	【開示項目】	【記述内容】（注1）	【定義等】	必須（注2）／選択	一定の要件を考慮すべき項目（注3）	
サービスサポート						
サービス窓口（苦情受付）	連絡先	電話/FAX、Web、電子メール等の連絡先		必須	○	窓口（連絡先）が無い場合は非認定
	営業日・時間	営業曜日、営業時間（受付時間）		必須		
		メンテナンス実施時間		必須		
	サポート対応	サービスサポートの稼働率	○サービスサポートの稼働率 ＝[窓口が実際稼働した時間] /[サービスサポートの対象時間]	選択		
		放棄率	○放棄率： 着信電話に出られなかった確率（オペレータービジー）	選択		
		応答時間遵守率	○応答時間遵守率： オペレーターが決められた時間内に応答したコール数の全コール数に対する割合	選択		
		基準時間完了率	○基準時間完了率： サービス窓口やサービス種別ごとに定められた基準時間内に完了した件数の全要求件数に対する比率	選択		
	サポート範囲・手段	サポート範囲 サポート手段（電話、電子メールの返信等）		必須		
サービス保証・継続	サービスダウンしない仕組み	サービスが停止しない仕組み（冗長化、負荷分散等）		必須		
	事故発生時の責任と補償範囲	ASP・SaaS事業者の事故責任の範囲と補償範囲のポリシー		必須		
サービス通知・報告	メインテナンス等の一時的サービス停止時の事前告知	利用者への通知時期、通知方法 （通知時期は1ヵ月前、3ヵ月、6ヵ月、12ヵ月、その他等の単位で記述）		必須	○	事前告知が無い場合は非認定
	障害・災害発生時の通知	障害発生時通知の有無		必須	○	障害発生時通知を行っていない場合は非認定
	定期報告	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）		必須		

（注1）「必須」の開示項目で有無の記述を求めている場合は、「ある」、「なし」を記述。（注2）「必須」の開示項目は、1つでも開示されていない項目があれば「非認定」となることを想定。
（注3）「必須」の開示項目の中で特に重要な項目について「○」を付してあり、すべての項目について一定の要件を満たせば「認定」となることを想定。