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

別添2

前提1：＜定義＞
本指針における「ASP・SaaS」及び「特定個人情報取扱いサービス」の定義は、それぞれ以下のとおりとする。

「ASP・SaaS」とは、特定又は不特定のユーザー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のこととする。
（「ASP（Application Service Provider）」と「SaaS（Software as a Service）」を特に区別せず、「ASP・SaaS」と連ねて呼称する。）

「特定個人情報取扱いサービス」とは、「ASP・SaaS」のうち個人番号をその内容に含む特定個人情報を取り扱うサービスとする。

前提2：＜情報開示の対象＞
情報開示の対象（単位）は、「特定個人情報取扱いサービス」毎とする。

【情報開示項目】			【内容】	必須／選択
1	開示情報の時点	開示情報の日付	開示情報の年月日（西暦）	必須
事業所・事業				
2	事業所等の概要	事業者名	事業者の正式名称（商号）	必須
			法人番号	
3		設立年月日	事業者の設立年月日（西暦）	必須
4		事業所	事業者の本店所在地	必須
			事業者ホームページ	
5	事業の概要	主な事業の概要	事業者の主な事業の概要	必須
人材				
6	経営者	代表者	代表者氏名	必須
			代表者経歴（生年月日、学歴、業務履歴、資格等）	選択
7		役員	役員数	選択
8	従業員	従業員数	正社員数（単独ベース）	必須
財務状況				
9	財務データ	売上高	事業者の売上高（単独ベース）	必須
10		経常利益	事業者の経常利益額（単独ベース）	選択
11		資本金	事業者の資本金（単独ベース）	必須
12		自己資本比率	事業者の自己資本の比率（単独ベース）	選択
13		キャッシュフロー対有利子負債比率	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）	選択
14		インタレスト・カバレッジ・レシオ	事業者のインタレスト・カバレッジ・レシオ（単独ベース）	選択

（注）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

15	財務信頼性	上場の有無	株式上場の有無と、「有り」の場合は市場名	選択
16		財務監査・財務データの状況	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	選択
17		決算公告	決算公告の実施の有無	選択
	資本関係・所属団体			
18	資本関係	株主構成	大株主の名称（上位5株主程度）、及び各々の株式保有比率	選択
19	所属団体	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			
20	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役員の氏名	選択
21		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・会議体の有無と、「有り」の場合は社内の部署名・会議名	選択
		特定個人情報の適正な取扱いを確保するための組織体制	特定個人情報の適正な取扱いを確保するため責任者の状況（役職等）	必須
			特定個人情報の適正な取扱いを確保するための組織体制の状況（組織名等）	
			特定個人情報の適正な取扱いのための組織体制に関する情報提供の可否と、可能な場合の条件等	
22		情報セキュリティに関する組織体制の状況	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	必須
			情報セキュリティに関する組織体制の有無	
23	法令等遵守	法令・ガイドライン等の遵守	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	必須
24	個人情報	個人情報の取扱い	個人情報の取扱いに関する規程等の有無と、「有り」の場合は記載箇所	必須
25		特定個人情報の取扱い	特定個人情報の取扱いについて定めた取扱規程の有無と、「有り」の場合は規程の名称	必須
			特定個人情報の取扱いについて定めた取扱規程の開示の可否と、可能な場合の条件等	
26	守秘義務	守秘義務契約	守秘義務に係る契約又は条項の有無	必須
			守秘義務違反があった場合のペナルティ条項の有無	
27	従業員教育等	従業員に対するセキュリティ教育の実施状況	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	必須
			特定個人情報等の適正な取扱いに関する従業員教育の取組状況の開示の可否と、可能な場合の条件等	
28		従業員に対する守秘義務等の状況	従業員に対する守秘義務対応の取組状況	必須
			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	
29	委託	委託情報に関する開示	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	必須
30		委託先に対する管理状況	自社の個人情報保護指針に対する遵守規定の有無	必須
			委託先（再委託先）の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	
			委託先（再委託先）との守秘義務対応状況	

（注）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

31	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・マニュアル等の状況と文書名	必須
			(特定個人情報の適正な取扱いにも資する)情報セキュリティに関する規程等の内容に関する照会対応の可否と、可能な場合の条件等	
32		サービス提供に係るシステム等仕様・構成の文書の整備	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	必須
			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	
33		運用管理等に関する規程等の整備	運用管理等に係る規程等に関する情報提供の可否と、可能な場合の条件等	必須
34		変更管理等に関する規程等の整備	変更管理等に係る規程等に関する情報提供の可否と、可能な場合の条件等	選択
35		事業継続に関する規程の整備	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	必須
			BCP対応計画及び運用手順等の開示の可否と、可能な場合の条件等	
36		リスク管理に関する規程等の整備	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	必須
37		勧誘・販売・係争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と、「有り」の場合は文書名	必須
			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	
38		ASP・SaaSの苦情対応に関する規程等の整備	ASP・SaaSの苦情処理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合はそれらの文書名	必須
			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	
サービス基本特性				
39	サービス内容	サービス名称	本ASP・SaaSのサービス名称	必須
40		サービス開始時期	本ASP・SaaSのサービス開始年月日(西暦)	必須
			サービス開始から申請時までの間の大規模な改変等の有無と、「有り」の場合は改変年月日(西暦)	
41		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴	必須
			他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容	
42		サービス提供時間	サービスの提供時間帯	必須
43		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(契約内容に依存する場合はその旨記述)	必須
44		移行支援	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)	必須
45	サービスの変更・終了	サービス(事業)変更・終了時等の事前告知	利用者への告知時期(事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述)	必須
			告知方法	
46		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と、「有り」の場合はその概要	必須
47	契約の終了等	情報の返却・削除・廃棄	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、受託情報の返還方法・ファイル形式・費用等	必須
			情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等	
			削除又は廃棄したことの証明書等の提供	

(注)「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

48	サービス料金	料金体系	初期費用額	必須
			月額利用額	
			最低利用契約期間	
49		解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	必須
50		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）	必須
51	サービス品質	サービス稼働設定値	サービス稼働率の目標値	必須
			サービス稼働率の実績値	
			サービス停止の事故歴	
52		サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	選択
			ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要	
53		認証取得・監査実施	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	必須
			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	選択
54		脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	選択
55		バックアップ対策	利用者データのバックアップ実施インターバル	必須
			世代バックアップ（何世代前までかを記述）	
			バックアップ対応の情報に関する開示の可否、可能な場合の条件等	
56		サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	必須
			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	
57		受賞・表彰歴	ASP・SaaSに関連する各種アワード等の受賞歴	選択
58		SLA（サービスレベル・アグリーメント）	本サービスに係るSLAが契約書に添付されるか否か	必須
59	契約者数	契約者数	本ASP・SaaSサービスの契約企業数等	選択
アプリケーション等				
60	中核的ソフトウェア	情報の提供等	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	必須
			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	
61	連携	他のASP・SaaSとの連携状況に関する情報提供	他のASP・SaaSとの連携の有無と、「有り」の場合は情報提供の条件等	必須

（注）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

62	セキュリティ	死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	必須
63		時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	必須
			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	
64		ウイルス対策	ウイルス対策の有無	必須
			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	
65		ユーザ認証	利用者の職種単位への対応の有無	必須
			利用事務単位への対応の有無	
66		管理者権限の運用管理	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	必須
			管理者認証に関する情報開示の可否と、可能な場合の条件等	
67		ID・パスワードの運用管理	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状況	必須
			ID・PW認証以外の認証方法の採用の有無	
			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	
68		記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、その保存期間及び利用者への提供可否	必須
			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	
			ログの改ざん防止措置の有無	
69		セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	必須
70		暗号化対策	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	必須
71		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記述（情報漏えい対策等）	選択
	ネットワーク			
72	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	必須
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	
73		推奨帯域	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	必須
74		推奨端末	パソコン、携帯電話等の端末の種類、OS等	必須
			利用するブラウザの種類	

（注）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

75	セキュリティ	ファイアウォール	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	必須
76		不正侵入検知	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等の有無と、「有り」の場合は対応方法	必須
77		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
78		ユーザ認証	ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法等	必須
			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	
			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	
79		なりすまし対策（事業者サイド）	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	必須
			なりすまし対策への対応方法に関する情報提供の可否と、可能な場合の条件等	
80		暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	必須
81		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記述（情報漏洩対策等）	選択
ハウジング（サーバ設置場所）				
82	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
83		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
			特筆すべき立地上の優位性があれば記述（例：標高、地盤等）	選択
84		耐震・免震構造	耐震数値	必須
			免震構造や制震構造の有無	
85	非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間	必須
86		給電ルート	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）	必須
87		非常用電源	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	必須
88	消火設備	サーバルーム内消火設備	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	必須
89		火災感知・報知システム	火災検知システムの有無	必須
90	避雷対策設備	直撃雷対策	直撃雷対策の有無	必須
91		誘導雷対策	誘導雷対策の有無	必須
92	空調設備	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	必須

（注）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。

93	セキュリティ	入退室管理等	入退室記録の有無と、「有り」の場合はその保存期間	必須
			監視カメラの有無	
			個人認証システムの有無	
94		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	選択
			保管管理手順書の有無	
			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	必須
95		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記述（破壊侵入防止対策、防犯監視対策等）	選択
	サービスサポート			
96	サービス窓口（苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	必須
			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	
			特定個人情報の取扱いに関する苦情処理に係る受付の可否	
97		営業日・時間	営業曜日、営業時間（受付時間）	必須
98		サポート範囲・手段	サポート範囲	必須
			サポート手段（電話、電子メールの返信等）	
99	サービス通知・報告	メ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）	必須
			告知方法	
100		障害・災害発生時の通知	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	必須
			緊急事態発生時の通知の有無・方法	
101		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）「必須」は情報開示が必須である項目。「選択」は情報開示が任意である項目を指す。