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）

前提1：＜定義＞
本指針における「IaaS・PaaS」および「IoTクラウドサービス」の定義は以下のとおりとする。

「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に必要なハードウェア資源等を提供するサービスを指し、広義にはデータセンターを包含するサービスのことをいう。また、「PaaS（Platform as a Service）」とは、狭義にはシステム資源、開発・実行資源、ネットワーク資源を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のことをいう。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。
「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を使ったクラウドサービス（本編ではIaaS・PaaS）のことをいう。

前提2：＜情報開示の対象＞
情報開示の対象（単位）は、「IaaS・PaaS」毎とする。

【情報開示項目】			【記述内容】	必須/選択（注）
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
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

（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。

	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
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 情報セキュリティに関する組織体制の有無	必須
23	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
24	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 守秘義務違反があった場合のペナルティ条項の有無	必須
25	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
26		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
27	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
28		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 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	必須
29	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
30		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 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	必須
31		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
32		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 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	必須
33		IaaS・PaaSの苦情対応に関する規程等の整備	IaaS・PaaSの苦情処理に関する基本方針・規程・マニュアル等文書類の有無と、「有り」の場合は文書名 IaaS・PaaS事業者の事故責任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	必須
	センターサービス			
34		サービス名称	本IaaS・PaaSのサービス名称	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。

35	サービス内容	サービス開始時期	本IaaS・PaaS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）	
36		サービスの基本タイプ	システム基盤サービス、IoT関連サービス、開発・実行基盤サービス、アプリ基盤サービス、ハード基盤サービス、ネットワーク基盤サービスの中から該当タイプを選択（複数選択可）	必須
37		サービスのカスタマイズ範囲	サービスのカスタマイズの範囲（契約に依存する場合は、その旨を記述）	必須
38		提供回線・帯域	専用線（VPNを含む）、インターネット等の回線の種類、提供帯域の種類、帯域保証がある場合にはその内容	選択
			提供回線が別契約（有償）回線か、基本料金に含まれているかの区別	
39		IoTサービス基本事項	IoTサービスに対する基本的な考え方。安全性（セーフティ）、連携内容、資産の管理方法、セキュリティ・バイデザイン、調達管理など	必須
40	サービス構成（システム基盤サービス）	提供OS	仮想化ソフト（ハイパーバイザ）提供の有無、単一OSとして動くOS（Windows、Unix、Linux等）及びバージョンを記述	必須
41		サーバ管理	サーバOS初期化、OSに関するパッチアップデート等のサービス内容	必須
42		ASP・SaaS支援サービス	検索、認証、決済・課金、セキュリティ、位置情報、タイムスタンプ、メディア、言語変換等のサービス内容	必須
43		管理者接続用ネットワーク提供サービス	リモートデスクトップ、SSH等の接続手段の内容	必須
44		バックアップ・リストアサービス	バックアップサービス、障害時のリストアサービス等の内容	必須
45		その他サービス	各種申請代行、決済代行、業務代行、コンサルティング等の内容	必須
46	サービス構成（IoT関連サービス）	IoT支援サービス	IoTシステムの構築を支援するサービスの内容（データ集約、プロトコル変換、アクセスコントロールなど）	必須
47		IoT側ネットワークサービス	推奨（提供）するIoT側ネットワークの回線、帯域など	必須
48	サービス構成（開発・実行基盤サービス）	ソフトウエア開発環境支援サービス	Java、Servlet、Perl、PHP、Ruby、C/C++、その他のオープンソースの開発環境の提供等	必須
49	サービス構成（アプリ基盤サービス）	ドメイン等管理サービス	IPアドレス管理、ドメイン取得・管理、DNSサーバ等のサービス内容	必須
50		メールサービス	Webメール、メーリングリスト等のサービス内容	必須
51		Webサービス	Webサーバ、FTPサーバ、Webアカウント、アクセス制御、アクセスログ解析、アクセスログ取得、ブログ、掲示板などのサービス内容	必須
52		その他サービス	API、DBサーバ等のサービス内容	必須
53	サービス構成（ハード基盤サービス）	サーバ提供サービス	共用サーバ、専用サーバ等のサービス内容	必須
54		ストレージ提供サービス	ストレージ提供サービスの内容	必須
55		レンタル機器サービス	レンタル機器類の障害時対応サービス、定期運用サービス、運用・保守支援サービスの有無と、「有り」の場合はその内容	必須
56		統合リソース提供サービス	仮想リソース群（仮想マシン、サーバ、ストレージ、ネットワーク等）を統合して提供するサービスの内容	必須
57		その他サービス	上記に該当しないその他サービスの内容	必須
58	サービス構成（ネットワーク基盤サービス）	ロードバランサーサービス	ロードバランサーサービスの内容	必須
59		ネットワーク機器提供サービス	ルーター、スイッチ等のネットワーク機器提供サービスの内容	必須
60		その他サービス	上記に該当しないその他サービスの内容	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。

61	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	
62		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	
63		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	選択
64		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
65		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）	
66		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
			他データセンターへのデータのバックアップの有無と、「有り」の場合は当該データセンターの場所（国内の場合は地域ブロック名、国外の場合は設置国）	
			他データセンターへのシステム（データを含む）のバックアップの有無と、「有り」の場合は当該データセンターの場所（国内の場合は地域ブロック名、国外の場合は設置国）	
67		受賞・表彰歴	IaaS・PaaSに関連する各種アワード等の受賞歴	選択
68		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
端末サービス				
69	IoT機器（センサー、アクチュエータ）	推奨（提供）機器	推奨（提供）する機器の種類、製品名など	必須
			主な機能	
			セキュリティレベル、認証取得状況など	
70		接続条件	接続数、設置場所などの制約	必須
71		使用条件	目的外使用の禁止など	必須
72		推奨（提供）ソフトウェア	推奨（提供）する組み込みソフト	必須
73		推奨（提供）物理的セキュリティ	推奨（提供）する盗難防止策など	必須
74		推奨（提供）保守・管理	推奨（提供）する保守体制、管理手法など	必須
75		推奨（提供）セキュリティ対策	推奨（提供）するIoT機器のセキュリティ対策（初期パスワードの変更、OS等の最新化、エッジコンピュータ、ゲートウェイの導入など）	必須
76	GW／エッジコンピュータなど	推奨（提供）機器	推奨（提供）する機器の種類、製品名など	必須
			主な機能	
			セキュリティレベル、認証取得状況など	
77		接続条件	接続数、設置場所などの制約	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。

78		使用条件	目的外使用の禁止など	必須
79		推奨（提供）物理的セキュリティ	推奨（提供）する盗難防止策など	必須
80		推奨（提供）保守・管理	推奨（提供）する保守体制、管理手法など	必須
	サービス共通事項			
81	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
82		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
83	契約の終了等	情報の返却・削除・廃棄	契約終了時の情報資産（利用者データ等）の返却責任の有無と、「有り」の場合は受託情報の返却方法・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の可否	
84	サービス料金・解約	料金体系	初期費用額	必須
			月額利用額	
			最低利用契約期間	
85		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
86		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と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	必須
87	契約者数	契約者数	本IaaS・PaaSサービスの契約企業数等	選択
88	データ管理	データの所在	本IaaS・PaaSサービス提供時における顧客データの保存先・所在先（国名）	必須
89		使用データセンター	本IaaS・PaaSサービス提供時における使用データセンターの数	必須
	システム運用（システム基盤運用、セキュリティ等）			
90	システム基盤運用	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
91		障害監視（機器等）	障害監視の有無	必須
92		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
93	セキュリティ（基盤、ストレージ等）	ウイルス対策	ウイルス対策の有無と、 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
94		管理者認証	システム運用部門の管理者権限の登録・登録削除の手順の状況	必須
95		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
96		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）取得の有無と、「有り」の場合はその保存期間	必須
97		セキュリティパッチ管理	セキュリティパッチの情報取得方法、評価方法、判断基準、更新手順、通常時の更新間隔、緊急時の対処方法等を定めた規程の有無	必須
98		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
99		ネットワーク不正侵入検知	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

（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。

100	セキュリティ（ネットワーク）	ネットワーク監視	事業者と契約利用者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
101		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と、「有り」の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
102		ユーザ認証	利用者に対する認証手段と方法（認証基盤を通じた個人認証、又はID、パスワード等）による利用者の認証の有無と、「有り」の場合は認証の方法	必須
103		IoT機器認証	IoT機器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
104		記録（ログ等）	システム運用に関するログ取得の有無と、「有り」の場合はその保存期間	必須
105		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と、「有り」の場合は認証の方法	必須
106		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）使用データセンターごとに記載				
107	施設建築物	データセンター識別名	当該データセンターの正式識別名又は簡易略称名＜※＞ ※簡易略称名とは、「A、B、C ・・・」、「1、2、3 ・・・」など	必須
108		データセンター事業開始年	本データセンターの事業開始年（西暦）	必須
109		建物形態	データセンター専用建物か否か	必須
110		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
111		耐震・免震構造	耐震数値	必須
			免震構造や制震構造の有無	
112	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
113		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
114		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
115	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
116		火災感知・報知システム	火災検知システムの有無	必須
117	避雷対策設備	直撃雷対策	直撃雷対策の有無	必須
118		誘導雷対策	誘導雷対策の有無	必須
119	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
120	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	
121		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	

（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。

122		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				
123	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
124		営業日・時間	営業曜日、営業時間（受付時間）	必須
			営業時間外の対応の可否	
125		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）	
126	サービス通知・報告・インシデント対応	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	
127		障害・災害発生時の通知	障害発生時通知の状況と通知方法及び利用者への通知時間	必須
128		セキュリティ・インシデント対応	セキュリティに関するインシデントが発生した場合の対応（通知、被害の拡大防止、暫定対処、本格対処など）	必須
129		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。