

【情報開示項目】			【記述内容】	必須／ 選択	申請内容	添付書類等
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	2023年4月1日	
－	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	ウエストユニティス株式会社	
法人番号			8120001075039			
3		設立年月日	事業者の設立年月日（西暦）	必須	1991年3月	
4		事業所	事業者の本店所在地	必須	〒530-0011 大阪府大阪市北区大深町1-1 LINKS UMEDA 8階 WeWork内	
	事業者ホームページ		<a href="https://www.westunitis.co.jp/">https://www.westunitis.co.jp/</a>			
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	・ウェアラブルコンピューティング、及びスマートグラスの開発・販売 （B2B向けソリューション提供に関し、ソフトウェア、ハードウェアを提供）	
－	人材					
6	経営者	代表者	代表者氏名	必須	鬼頭 和秀	
			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	9名	
－	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	－（非開示）	
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	95,000,000円（2021年9月期）	

12	財務信頼性	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	無し	
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	代表取締役社長 鬼頭 和秀	
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	有り 管理グループ・コンプライアンス・リスク管理委員会	
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	有り 代表取締役社長 鬼頭 和秀	
	情報セキュリティに関する組織体制の有無		有り			
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	有り <a href="https://www.westunitis.co.jp/agreement/">https://www.westunitis.co.jp/agreement/</a>	
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	必須	有り	
			守秘義務違反があった場合のペナルティ条項の有無		有り	

（注）必須/選択欄の「必須○」とは、一定の水準を考慮すべき項目

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	ISMSマニュアルに従って、社内教育計画を実施	
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	就業規則に守秘義務対応を定め、雇用契約書においても同遵守を記載し締結	
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	委託先無し	
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	必須	無し	
			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		無し	
			委託先(再委託先)との守秘義務対応状況		—	
			委託先(再委託先)の管理方法		—	
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、リスクアセスメント結果等の状況と文書名	必須○	規程あり: ISMS運用プロセスに則り、下記の文書を整備 ・ISMSマニュアル ・適用宣言書 ・情報取扱規程 ・施設入退管理基準 ・情報システム管理基準 ・セキュリティインシデント対応基準 ・緊急時対応規程 ・個人情報保護規程 ・特定個人情報取扱規程 ・リスクアセスメント評価基準	
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	必須	有り 緊急時対応規程	
			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		否	
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	有り コンプライアンス・リスク管理規程	
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	必須	有り 企業行動規範	
			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		有り 各取引契約の条項に記載	
33		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	無し	
			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		有り ・LinkerWorksご利用規約 ・LinkerWorksクラウドサービス仕様書	

-	サービス基本特性					
34	サービス内容	サービス名称	本ASP・SaaSのサービス名称	必須	LinkerWorks	
35		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	2021年7月1日	
			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）		無し	
36		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴(500文字以内)	必須	本サービスでは、当社製スマートグラス「InfoLinker3」等、LinkerWorksクライアントアプリ（以下、クライアントアプリ）がインストールされた端末と組み合わせて使用し、複数の人・現場とをつなぐことで、現場作業を支援するためのクラウドサービスです。  本サービスでは、主に下記の機能を提供します。  (A) 作業サポート機能 複数の作業者や監督者をビデオ通話でつなぎ、遠隔から作業を支援する機能を提供します。 (B) 作業ナビ機能 作業者が利用する端末に表示する作業指示コンテンツの作成と、作業指示に従って作業した履歴を確認する機能を提供します。  ※本サービスご提供機能の詳細については、当社ウェブサイト(https://www.westunitis.co.jp)にてご確認ください。	
			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		無し	
37		サービス提供時間	サービスの提供時間帯	必須	24時間365日 (LinkerWorksクラウドサービス仕様書に記載の「計画停止」を除く)	
38		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	個別相談による	
39		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	無し	
40		IoTクラウドサービス基本事項	IoTクラウド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	基本的な考え方: 全ての通信は暗号化され、データベースやストレージ暗号化を行うことで、利用者から入力されたデータの機密性を保護します。  InfoLinker3の利用における注意点: InfoLinker3には、カメラやマイクが搭載されており、さらに撮影した情報を本サービスへアップロードする機能が搭載されるため、InfoLinker3を装着している作業者が撮影を行う場合はカメラに映り込む人物や音声に関して、個人情報の取り扱いに注意が必要です。	
41	データ	利用	IoTクラウドサービスで収集したデータの利用の有無、内容同意の取得方法など	必須	有り データ利用の同意については、本サービスの契約締結を持って同意とします。	
42		権利関係	IoTクラウドサービスで収集したデータの権利(所有権、使用权、著作権、肖像権など)	選択	契約されたお客様のアカウント内にて、利用者が入力(テキストや撮影写真等)したデータは、契約されたお客様が全ての権利を有し、その他の当社システム機能が生成するデータ(アクセスログやAPIログ等)は当社が全ての権利を有します。	
43		サービス(事業)変更・終了	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○	サービス終了時に関しては、6ヶ月前での通知。 ただし、やむを得ない場合、速やかに通知するものとします。	

43	サービスの変更・終了	了時等の事前告知	告知方法	必須	当社ウェブサイトおよび、購入申込書にて登録された設定・運用担当者宛への電子メール送信	
44		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	無し	
45	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	お客様のデータは、サービス契約中に全てお客様にてデータのエクスポート機能を利用し、バックアップを行なって頂きます。	
			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		契約終了時の全ての利用者データの破棄は当社にて実施します。	
			削除又は廃棄したことの証明書等の提供		当社指定の書式にて提供可能	
46	サービス料金	料金体系	初期費用額	必須	要お問い合わせ	
			月額利用額		要お問い合わせ	
			最低利用契約期間		要お問い合わせ	
47		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	無し	
48		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	有り 期限：解約日3ヶ月前	
49		サービス稼働設定値	サービス稼働率の目標値	必須	99.5%	
			サービス稼働率の実績値		100%（2021年7月1日～2023年3月1日）	
			サービス停止の事故歴		無し	
50		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		—	
51		IoT性能対策	大量のIoT機器からの大容量のデータが送られる場合等の性能対策の内容（委託先による対策を含む）	必須	データ容量が最大となる1ファイルのデータサイズは最大で700MBまでに制限されます。 また、アップロードされるファイルを受信するサーバは、負荷に応じてオートスケーリングすることにより、性能を自動で拡張して適宜対応します。	

52	サービス品質	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	情報セキュリティマネジメントシステム（ISMS（ISO/IEC 27001））：2021年9月取得済	
53		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	有り 下記の診断をクラウド上のシステムに対して、第三者の診断サービス会社により実施しています。 ・アプリケーション診断 ・ネットワーク診断 ・ペネトレーションテスト	
54		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	1回/日	
			世代バックアップ（何世代前までかを記述）		7世代	
55		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	マルチAZ構成によるサーバの冗長化と、ロードバランサ及びオートスケーリングによる負荷分散の実施	
			DR（ディザスタリカバリー）対策の有無と、「有り」の場合はその概要		有り サービスを構成する全てのインフラとデータをIaaS事業者のAWS（Amazon Web Service）内のクラウド上に構築・保存することで、DR対策が整ったデータセンター内にて管理。	
56		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	MCPC award 2021 サービス＆ソリューション部門：奨励賞	
57		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	「LinkerWorksクラウドサービス仕様書」に記載	
58	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、プラットフォーム、サーバ・ストレージ等					
59	連携	他のサービス・事業との連携状況に関する情報提供	他のサービスや事業との連携の有無と、「有り」の場合は情報提供の条件等	必須	無し	
60		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○	有り （主要機能に関するサーバを監視対象）	
61		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	有り 同期方法：NTP	
62		ウイルス対策	ウイルス対策の有無	必須○	有り ソースコード・ライブラリ管理レベルでの脆弱性検出。 運用時のWAF機能による検出と遮断、及びコンテナサービスを利用した不正プログラム実行の抑止	
63		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○	有り	

（注）必須/選択欄の「必須○」とは、一定の水準を考慮すべき項目



64	セキュリティ	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○	サービス契約時に提供する、アカウント管理者用の1ユーザーのみ当社からお客様に付与し、管理者パスワードは、お客様自身で変更していただきます。  上記以外のユーザーID登録は、ユーザー登録権限を持つ利用者にて登録・管理していただくため、ID/PWの運用管理はお客様にて実施していただきます。	
65		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○	ログ取得:有り 保存期間:1年 利用者への提供:なし ただし、別途利用者向けのセキュリティ管理機能として、アクセス履歴の参照機能を提供(過去6か月分)	
			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	必須	ログ取得:有り 保存期間:1年	
			ログの改ざん防止措置の有無	必須	クラウド環境での操作に対して、ユーザー権限によるアクセス制限にて管理	
66		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○	IaaS事業者側でのセキュリティパッチに対応するコンテナサービスを利用	
67	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	有り ストレージ:暗号化設定されたIaaS提供ストレージサービスの利用 データベース:暗号化設定の有効化		
68	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					
69	センター側ネットワーク	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	IaaS環境としてAWS(Amazon Web Service)を利用しています。 データセンター内はプライベートなネットワークを構築	
70		帯域	データ通信速度の範囲、帯域保証の有無	必須	IaaS環境としてAWS(Amazon Web Service)を利用しています。 非公開	
71	PC側ネットワーク	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	インターネット回線	
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲		接続回線による影響で発生した問題について、責任は負いません	
72		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	有り 10Mbps以上 利用できる帯域に応じて、ビデオ通話の品質と同時通話数に影響を受けます。	
73	IoT側ネットワーク	推奨(提供)回線	インターネット、IoT専用回線等の回線の種類	必須	インターネット回線	
			IoT機器接続回線について、ASP・SaaS事業者が負う責任範囲		接続回線による影響で発生した問題について、当社は責任を負いません	

74		推奨（提供）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	有り 1～5Mbps 利用できる帯域に応じて、ビデオ通話の品質に影響を受けます。	
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○	有り	
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	有り IaaS事業者管理のコンテナサービス利用及び、WAF機能により検知	
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○	Web：ID/PW方式、シングルサインオン（SSO）方式 InfoLinker3：ログインQRコードスキャン方式	
79		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○	全てのサーバ/デバイス間通信用のAPIはアクセストークンによる認証を実施	
80		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	有り パスワード入力に連続7回失敗した場合、当該IDからのログインができないようにロックします。ロックされたIDは管理者権限ユーザーからのみ解除可能とし、時間経過によるロック解除機能は設けません。 シングルサインオン方式に変更することによる、認証プロバイダー側での強固な不正ログイン対策の適用。	
81		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	有り TLS暗号化のみ（SSL暗号化は脆弱性が存在するため対応しません）	
82		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	LinkerWorksクラウドサービス仕様書に記載	
—	提供端末		端末が複数ある場合は、端末ごとに記述する			
83		機器	機器の種類、製品名など	必須	InfoLinker3（LTE搭載スマートグラス）	
			主な機能		作業サポート：ビデオ通話による遠隔作業支援 作業ナビ：作業指示情報による作業のナビゲーション 作業レコーダ：カメラによる写真・動画撮影（端末内にのみ保存し、サーバ通信はしない） 作業ファイル：端末内に保存された、静止画・動画・書類ファイルのビューワー	
			セキュリティレベル、認証取得状況など		TELEC JATE VCCI CE RoHS PSE CCC BSMI UN38.3	

（注）必須/選択欄の「必須○」とは、一定の水準を考慮すべき項目



84	IoT機器（センサー、アクチュエータ）	接続条件	接続数、設置場所などの制約	必須	利用場所： ・日本国内  使用可能動作環境 ・温度：-20℃～50℃ ・湿度：30%～90%	
85		使用条件	目的外使用の禁止など	必須	InfoLinker3およびLinkerWorksの購入時に締結された契約書または利用規約に記載の禁止行為。	
86		ソフトウェア	組み込みソフト	必須	LinkerWorksクライアントアプリケーション（当社製）	
87		物理的セキュリティ	盗難防止策など	必須	無し	
88		保守・管理	保守体制、管理手法など	必須	保守・管理において、下記のサービスを提供します。 ・購入1年以内：無償修理 または 交換（故意の破損等除く） ・購入1年以降：有償にて修理 ・当社カスタマサポートによるヘルプデスクの設置	
89		セキュリティ対策	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	・QRコードによるログイン認証 ・ログインQRコードの発行からの有効期間設定 ・Webサービスからの操作による発行済みログインQRコードの無効化	
90		機器	機器の種類、製品名など	必須	該当なし	
			主な機能		該当なし	
			セキュリティレベル、認証取得状況など		該当なし	
91	GW／エッジコンピュータなど	接続条件	接続数、設置場所などの制約	必須	該当なし	
92		使用条件	目的外使用の禁止など	必須	該当なし	
93		物理的セキュリティ	盗難防止策など	必須	該当なし	
94		保守・管理	保守体制、管理手法など	必須	該当なし	
-	推奨端末					
95		PC等	パソコン、スマホ、タブレット、シンクライアント等の端末の種類、OS等	必須	パソコン：Windows 10以降、Macintosh OS X以降 iPad：Safari（最新バージョン）	

95	端末	(操作端末)	利用するブラウザの種類	必須	Google Chrome推奨(最新バージョン) Microsoft Edge (Chromium版)(最新バージョン)	
96		IoT機器(センサー、アクチュエータ)	機器の種類、製品名など	必須	該当なし	
			主な機能		該当なし	
			セキュリティレベル、認証取得状況など		該当なし	
97		GW／エッジコンピュータなど	機器の種類、製品名など	必須	該当なし	
			主な機能		該当なし	
			セキュリティレベル、認証取得状況など		該当なし	
-	ハウジング(サーバ設置場所)		データセンターを複数使用している場合は、データセンターごとに記述する			
98	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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 データセンター専用建物です。	
99		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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 東京リージョンをマルチAZ設定にて利用しています。	
			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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
100		耐震・免震構造	耐震数値	必須	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
			免震構造や制震構造の有無		IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
101	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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
102		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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
103		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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
104	消防設備	サーバールーム内消火設備	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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	

(注) 必須/選択欄の「必須○」とは、一定の水準を考慮すべき項目

105		火災感知・報知システム	火災検知システムの有無	必須	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
106	避雷対策設備	直撃雷対策	直撃雷対策の有無	必須	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
107		誘導雷対策	誘導雷対策の有無	必須	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
108	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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
109	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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
			監視カメラの有無		IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
			個人認証システムの有無		IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
110		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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
			保管管理手順書の有無		IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
11		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	IaaS環境としてAWS (Amazon Web Service)を利用しています。 https://aws.amazon.com/jp/compliance/data-center/data-centers/	
-	サービスサポート					
112	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○	電子メール customer_support@westunitis.co.jp	
			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	必須	無し	
113		営業日・時間	営業曜日、営業時間(受付時間)	必須	当社営業日 10:00 ～ 17:00	
114		サポート範囲・手段	サポート範囲	必須	本サービスに関するお問い合わせ、及び障害に対して対応します。 サポートデスクにて提供する資料やお問い合わせについては、すべて日本語での提供とします。	
			サポート手段(電話、電子メールの返信等)		電子メール	

（注）必須/選択欄の「必須○」とは、一定の水準を考慮すべき項目

115	サービス通知・報告・インシデント対応	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か月前、3か月前、6か月前、12か月前等の単位で記述）	必須○	「LinkerWorksクラウドサービス仕様書」に記載、下記の通りとなります。 [計画] 機能追加・バグフィックス・機能改善（サービス停止あり）：2週間前 [計画] 機能追加・バグフィックス・機能改善（サービス停止なし）：1週間前 [計画] メジャーバージョンアップ・業務に影響のあるUI変更：2週間前 [計画] 既存機能の廃止：1ヶ月前 [緊急] サービス継続に必要な緊急メンテナンス：即日都度 [緊急] メンテナンス後に問題が発生した切り戻し：即日都度	
			告知方法	必須	サポートウェブサイト及び購入申込書にて登録された設定・運用担当者宛への電子メール送信	
116		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○	通知：有り 通知方法：サポートウェブサイト、及び契約時に登録頂く運用・設定担当者（最大3名）宛電子メール 通知時間：時間規定なし（ベストエフォート）	
117		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	有り （ISMS運用マニュアルに従って対応を行います）	
118		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	無し	