Ⅰ.基本情報

◆基本項目

1	サービスに関する準拠法。	日本法	
2	サービスのデータ保護に関する準拠法。	個人情報保護法	
3	サービスに登録されるデータの帰属先。	サービス利用者	
4	情報セキュリティおよび個人情報保護について方針を定め、これらの方針を組織の内外へ周知しているか。	○	
5	情報セキュリティまたは個人情報保護について第三者認証を取得しているか。	○	・プライバシーマーク：2020年8月19日更新 ・ISMS（ISO/IEC 27001）：2020年2月24日更新
6	サービス提供者およびクラウドサービスが満たすべき関連法令や規制、契約上の要求事項を整理し、これらを満たすための取組を継続的に実施しているか。	○	
7	セキュリティ対策が正しく実装され意図した通り運用されているか、関連法令や規制、契約上の要求事項を満たしているかを社外監査など評価部門により定期的に評価しているか。	○	社外監査を行なっております。

Ⅱ.個人情報保護に関する項目

◆個人情報保護・データ利用について

8	個人情報保護方針をサービス利用者に開示しているか。	○	
9	個人情報保護に関連する法令および規制が適用される場合は、その要求に従って対応できるか。	○	
10	サービスでは個人情報を取得しているか。	○	
11	サービス契約者の個人情報を自社利用しているか。	○	匿名化しマーケティング等を目的として利用しております。
12	サービス契約者の個人情報を第三者に提供しているか。	×	
13	サービス契約者の預託データを自社利用しているか。	○	
14	サービス契約者の預託データを第三者提供しているか。	×	
15	外部サービスの利用や外部委託等により預託データが他国に移転されることはあるか。	×	

◆免責について

16	サービスレベルについて定めているものはあるか。	○	SLAを定めております。 参照： https://www.kingtime.jp/wp-content/uploads/2017/11/KOTSLA07.pdf
17	サービス利用における免責など、条件を定めているか。	○	KING OF TIME 第12条で定めております。 参照：https://www.kingtime.jp/kot_contract/

Ⅲ.セキュリティ全般

◆情報セキュリティについて

18	情報セキュリティ管理の責任者を定め、職務範囲や権限、責任について定めているか。	○	
19	情報セキュリティ体制について、通常時だけでなく有事を想定した役割や責任を定めているか。	○	
20	情報セキュリティ管理に関する関係部署や業務、機能を明らかにしているか。	○	
21	自社で対応する箇所、外部に委託する箇所を適切に切り分け、役割と責任を明確にしているか。	○	
22	承認されていない、意図しない変更や不正利用のリスクを低減するため、組織の役割と責任に応じて情報資産へのアクセスや閲覧、修正等の権限を分離しているか。	○	
23	情報セキュリティおよび重要情報の取扱いに関する意識向上のため、定期的に適切な教育や訓練を実施し、理解が足りないと思われる箇所は継続的に教育を実施している。	○	

◆従業員に対するセキュリティ対策

24	従業員に対しセキュリティインシデントを想定した教育や訓練を実施しているか。	○	
25	従業員と秘密保持に関する契約を締結をしているか。	○	
26	従業員および契約相手との契約が終了または変更となった場合、アクセス権の変更や削除、貸与資産の返却等を実施しているか。	○	

◆情報資産管理について

27	情報資産の管理プロセスおよび重要度の基準を定め、管理プロセスに従い情報資産の洗い出しと評価を行い、資産一覧を作成しているか。	○	
28	情報資産の消去またはサーバや媒体等のコンポーネントを廃棄する場合は書き込まれたデータを復旧できない状態にしているか。	○	記憶媒体については物理破壊しております。
29	契約や規約等により、サービス利用終了時のデータの取り扱いが明確になっているか。	○	解約時に即座に論理消去を行っております。ただし、バックアップデータからは削除しておらず暗号化にて対応しております。
30	サービス利用終了時に、サービス利用者からの預託データ、またはサービス利用者が作成したデータを返還および削除できるか。	○	返還は行なっておりませんが、削除を行なっております。

◆アクセス制限について

31	外部記憶媒体の保管や移動、廃棄、取扱者範囲等の管理手順を定め、その手続きにもとづき媒体を利用しているか。	×	外部記憶媒体に保管は行なっておりません。
32	クラウドサービスの開発および保守、運用で利用するソフトウェア、ハードウェア、ネットワーク上で取り扱われるデータについて、アクセス制御方針を定めて実施しているか。	○	
33	従業員やシステム管理者は、サービス利用者からの預託データへのアクセスを原則として禁止されているか。 業務上必要な場合で預託データにアクセスする場合は、事前に承認を得たものに限定すると共に、アクセス者の操作ログをモニタリングしているか。	○	お客様環境へのログインは許可をいただいた上で実施しております。

34	クラウドサービス内のコンポーネントやデータへのアクセスを、各コンポーネント単位で業務上必要な従業員にのみ限定しているか。	○	
35	特権アカウントを用いた情報資産に対するネットワークアクセスを記録し、適切な利用かどうかをモニタリングしているか。	○	
36	クラウドサービスにおいて、不要または一定期間使用していないアカウント（異動や退職、役割変更を含む）を無効化もしくは削除しているか。	○	
37	共有アカウントの利用は原則禁止の上、例外的に利用が承認された場合でも、管理簿や利用ログ等で適切な利用か確認しているか（確認方法を備考欄に記載する事）。	○	
38	発行済のIDを他の人に重複して払出できない仕様にしているか。	○	
39	接続元IPアドレスによる接続経路を制限しているか。	○	お客様側の設定でIPアドレスの接続元を制限することが可能でございます。
40	多要素認証やシングルサインオン、2段階認証等の適切な認証機構を用いているか。	×	
41	指定回数続けて認証に失敗したアカウントはロックまたは一定期間認証を不可としているか。	○	
42	認証情報の送受信には通信を暗号化しているか。	○	
43	ログイン後一定時間以内に操作が無かった場合には、セッションを切り再度ログインを要求しているか。	○	有効期限は30分で設定されております。
44	パスワードに関して英字を大文字と小文字で区別し、文字数と数字、特殊文字を組み合わせ、最低限の文字数を課す事でパスワードに必要な複雑さを確保しているか。	○	
45	入力したパスワードは画面上へ表示されないようにしているか。	○	
46	暗号化されたパスワードのみを保存および伝送しているか。	○	
47	パスワードの最短、最長有効期間を設定しているか。	○	
48	同じパスワードを世代にわたって再利用するのを禁止しているか。	○	
49	クラウドサービスのサーバやコンポーネントにおいて、パスワードを初期設定の状態では利用していないか。	○	
50	利用者自らによるパスワード変更を可能としているか。	○	
51	クラウドサービスの開発および保守、運用において、特権アカウントの割当および利用する際は、承認を必須とし必要最小限に制限しているか。	○	
52	クラウドサービスおよびアプリケーションの管理者権限や特権的ユーティリティのアクセス制限は実施しているか。	○	
53	プログラムソースおよび仕様書等へアクセスできる人を限定しているか。	○	
54	クラウドサービスに対する変更に関して、リリースやローンチをできる人を限定するためアクセスを制御しているか。	○	
◆データ、通信の暗号化について			
55	情報資産を保護するため、重要度や用途に応じて暗号化方針を定めているか。	○	
56	暗号化するためのキーやパスワードは、必要なときに限られたシステム管理者のみアクセスできるよう制御しているか。	○	
57	サービスに格納されたデータは、データベースまたはファイルを直接アクセスされた際に、データ内容が認識できないよう暗号化またはマスク処理されているか。	○	
58	データベースへのアクセス制御およびアクセスログのモニタリングを実施しているか。	○	
59	バックアップデータは、データ内容が認識できないよう暗号化されているか。	○	
60	バックアップデータへのアクセス制御およびアクセスログのモニタリングを実施しているか。	○	
61	SSL通信を行う場合は、脆弱性がある通信プロトコルでの通信を禁止しているか。	×	打刻専用機の一部で、TLS1.0、1.1を利用しておりますが、今後禁止にしていく予定にしております。
62	Webサイトへアクセス時の通信を暗号化しているか。	○	
63	有効期限が切れていない、信頼できる認証局が発行したSSLサーバ証明書を利用しているか。	○	グローバルサイン社製 SSLサーバー証明書を利用しております。
◆物理及び環境のセキュリティについて			
64	情報および情報処理施設のある領域を保護するために、境界内に設置している資産の重要度にもとづいて、それぞれ物理的セキュリティ境界の位置や強度を定めているか。	○	
65	セキュリティ区画への入館および入室は承認にもとづき許可され、ICカード認証や生体認証等の認証により入退室を制御しているか。	○	
66	入退室ログを定期的に確認し、不正アクセスがないか確認しているか。	○	
67	特に重要な場所には監視カメラを設置したり、立会人を同行させる等の対策を講じているか。	○	
68	国内リージョンおよびデータセンターを利用しているか。	○	
69	国外リージョンおよびデータセンターを利用しているか。	○	
◆サービス運用に関するセキュリティについて			
70	クラウドサービスの機能やコンポーネントの構成、仕様、サービス提供の条件、利用方法等を定め文書化しているか。	○	
71	クラウドサービスに対する変更をレビューし、不正な変更の有無を確認するためにシステム構成やネットワーク構成図、変更状況を可視化しているか。	○	
72	クラウドサービスの機能や運用それぞれについて定期的な点検を行い、不備事象を是正しているか。	○	
73	クラウドサービスに対する変更について、影響をあきらかにし文章化・可視化しているか。	○	
74	クラウドサービスに対する変更について、承認された変更をのみ提供しているか。	○	
75	クラウドサービスに対する変更について、判明した欠陥とその対処について定められた方法で報告しているか。	○	

76	サービスの大きな変更や終了について、サービス利用者に対する事前告知ルールを定め、実施しているか。	○	
77	サービスを提供する時間帯を定め、サービス利用者へ告知しているか。	○	ログイン画面通知やメール通知等で行なっております。
78	クラウドサービスにおいて、サービス提供に関わる障害やパフォーマンス低下等が発生した場合について速報や追加情報の通知ルールを定め、実施しているか。	○	ログイン画面通知やメール通知等で行なっております。
79	サービス提供に関わる、クラウドサービスの緊急もしくは不定期な保守が必要な場合についてサービス利用者への事前通知ルールを定めているか。	○	ログイン画面通知やメール通知等で行なっております。
80	預託データの取り扱いについて、規約や契約書、個人情報保護方針等に明記しサービス契約者へ開示しているか。	○	
81	システム要件の充足もしくはサービス妨害攻撃によるリソース不足解消のための管理しているか。	○	
82	リソースの管理には現状だけでなく将来の必要量を考慮しているか。	○	
83	本番環境の変更による不具合を防ぐために、本番環境と同等の開発環境で予めテストを実施し不具合を解消しているか。	○	
84	サービスの提供に関わるクラウドサービスおよび構成するコンポーネント、端末に対してマルウェア対策ソフトを導入し、定期的にパターンファイルを更新しているか。	○	
85	クラウドサービスの時刻は各コンポーネントで統一された時刻（タイムゾーン）を管理し、NTPの仕組み等によりクラウドサービスの時刻を同期させているか。	○	
86	ソフトウェアの導入および変更作業はデバイス認証やMACアドレス認証、接続元IPアドレス制限等により制限され、許可された端末から行っているか。	○	
◆バックアップについて			
87	クラウドサービスが予め定められた目標時間やポイントに復旧できるようクラウドサービスおよびデータをバックアップしているか。	○	
88	クラウドサービスがバックアップから復旧する際は、適切に復旧できるかリストアテストを行っているか。	○	
89	クラウドサービスのバックアップが取得されていることを確認しているか。	○	前日AM4:00までのデータをバックアップしております。
90	クラウドサービスのバックアップデータをクラウドサービスが設置してある場所とは物理的に離れた場所（別リージョン）で保管しているか。	○	
◆ログの取得について			
91	システム障害や例外処理や誤操作によるエラー、セキュリティインシデントを記録したイベントやアクセスログを取得している。	○	
92	サービス利用者およびシステム管理者のログインおよびログアウトのログを取得しているか。	○	
93	サービス利用者およびシステム管理者の操作ログを取得しているか。	○	
94	関連法令や規制を満たす事ができるよう、データやログ等の保管期間と管理要件を定め、ルールに従い実施しているか。	○	保管期間は5年分となります。
95	セキュリティインシデント発生から即時に事象を解析するため、クラウドサービスのログを効率的に分析する仕組みを導入しているか。	○	
96	取得したログとバックアップデータが不正アクセスおよび改ざんされないよう、アクセス制御や暗号化等により保護しているか。	○	
◆脆弱性について			
97	クラウドサービスについて、脆弱性診断を実施しているか。	○	ポートスキャン等の簡易診断、ネットワーク等への詳細診断、ペネトレーションテストを毎週行なっております。
98	クラウドサービスのインフラやネットワーク、運用等を変更する場合は、機能や非機能、セキュリティ脆弱性診断を行ない、変更後に影響や不具合がないか確認しているか。	○	
99	クラウドサービスの変更前に脆弱性診断を行い、その結果にもとづいて対策を講じているか。	○	サービス開始前、修正/変更後の公開前及び1年に1回以上の頻度で専門検査機関による脆弱性診断（Webアプリケーション、ネットワーク、スマートフォンアプリケーション等）を実施しております。
100	クラウドサービスについて、OSやMW、ソフトウェア等の脆弱性およびEOSLに関する情報を定期的に収集し、適宜パッチによる更新やソフトウェアのアップデートを行っているか。	○	
101	脆弱性を管理するためのリスクレベルやリスクレベルに応じた対処時期等の方針を定め、その方針に従って脆弱性に対処しているか。	○	
◆セキュリティインシデントについて			
102	セキュリティインシデントやシステム障害への対処手順を確立しているか。	○	
103	セキュリティインシデントやシステム障害を検知するためにクラウドサービスおよびネットワークに対するパフォーマンス監視を行なっているか。	○	
104	セキュリティインシデントやシステム障害を検知するために、クラウドサービスの死活や障害監視、外形監視（運用監視）を行なっているか。	○	
105	セキュリティインシデントやシステム障害を検知するために、内部および外部からの不正アクセスや不正利用を監視しているか。	○	
106	セキュリティインシデントやシステム障害を検知するために、不正なパケットに関する監視しているか。	○	
107	セキュリティインシデントやシステム障害を検知するために、不正なネットワークアクセスやリモートアクセスの監視しているか。	○	
108	セキュリティインシデントやシステム障害に対して迅速かつ効果的に対応をするために責任および役割を明確にしているか。	○	
109	地震や火災等の災害または大規模なシステム障害に備えてリカバリ計画や緊急時対応計画を策定しているか。	○	
◆ネットワークのセキュリティ			

	110	クラウドサービスへリモートアクセスする場合は、システム管理者による事前の承認を必要とした上でアクセスを許可しているか。	○	
	111	外部および内部からの不正アクセスを防止するためにファイアウォールを設置しているか。	○	
	112	不正アクセス防止装置についてパターンファイルおよび定義の更新を定期的に実施しているか。	○	
	113	WAFを導入し、Webアプリケーションの脆弱性を悪用した攻撃等から保護しているか。 ※ WAF …Web Application Firewall	○	
	114	WAFのパターンファイルおよび定義の更新を定期的に実施しているか。 ※ WAF … Web Application Firewall	○	
	115	DDoS等サービスの維持運用を妨害する攻撃へ対策しているか。 ※ DDoS … Distributed Denial of Service attack	○	
	116	サービス維持運用妨害からの保護についてパターンファイル及び定義の更新を定期的に実施しているか。	○	
	117	不正アクセスを検知した場合はシステム管理者やサービス利用者へ迅速に通知できるような対応フローを規定しているか。	○	
	118	サービス利用企業において、クラウドサービスへのアクセスする場合、接続元IPアドレスによる接続経路の制限ができるか。	○	
	119	クラウドサービスの開発および保守、運用において利用する管理画面へのアクセスする場合、接続元IPアドレスによる接続経路の制限ができるか。	○	
	120	クラウドサービスでは、各サーバの用途に応じた論理的分離により境界を保護しているか。	○	
	121	DBサーバがWebサーバと分離された構成になっており、WebサーバとDBサーバ間の通信経路が必要最低限になるようアクセスを制御しているか。	○	
	122	DBサーバは外部から直接アクセスできないようにアクセスを制御しているか。	○	
	123	クラウドサービスにおける情報授受において、情報の機密性や完全性を担保するため、情報授受の伝送経路において暗号化やチェックデジットを活用しているか。	○	
	◆クラウドサービスのシステムの取得・開発・保守について			
	124	クラウドサービスの開発および保守、運用において、セキュリティ対策の要求事項を明確にしているか。	○	
	125	クラウドサービスの開発および保守、運用の各工程でセキュリティや品質を考慮するため、機能要件や非機能要件、セキュリティ要件を洗い出してレビューを実施しているか。	○	
	126	クラウドサービスの開発および保守、運用の各工程でセキュリティや品質を考慮するため、セキュアコーディングやセキュリティテストのレビューを実施しているか。	○	
	127	クラウドサービスの開発および保守、運用の各工程でセキュリティや品質を考慮するため、各工程における承認プロセスや、データ修正プロセスの整備を行なっているか。	○	
	128	クラウドサービスの開発および保守、運用において、データ漏洩を防止するため、開発環境と本番環境の分離しているか。	○	
	129	クラウドサービスの開発および保守、運用において、データ漏洩を防止するため、本番環境のデータについて、複製および本番環境以外での利用禁止（テスト利用等）しているか。	○	
	130	クラウドサービスの開発および保守、運用する端末へインストールするソフトウェアについて、禁止したソフトウェアが利用されないよう制限やモニタリングをしているか。	○	
	131	アプリケーションを変更する場合は、変更後の影響や不具合がないか事前にテストを行ない確認しているか。	○	
	◆外部委託先管理について			
	132	外部委託先が預託データを用いることがあるか。	○	サポート業務や不具合調査業務等、必要に応じて用いております。
	133	外部委託先に対して自社と同等基準の情報セキュリティを要求、合意しているか。	○	
	134	外部委託先を定期的に評価しているか。	○	年1回行なっております。