クラウドサービスチェックリスト						
No.	種別	サービスレベル項目	規定内容	測定単位	対応可否	実施内容/備考
契約						
1	契約条項	利用規約	守秘義務は事業者側・ユーザ側の双方同等であること	○×	○	利用規約に記載
2			データ消失対策について規定されていること	○×	○	利用規約に記載
3			損害賠償について規定されていること（データ消失時、障害時）	○×	○	利用規約に記載
4			契約終了時のデータ返還、クラウド上のデータ完全消去が規定されていること	○×	○	利用規約に記載
5			サービス変更に関する規定がある（内容、方法、通知期間、通知方法等）こと	○×	○	利用規約に記載
6			契約は事業者側が一方的に解除できる条件になっていないこと	○×	○	利用規約に記載
7			契約をユーザ側が解除する場合にペナルティがない（利用料、拘束期間）こと	○×	○	利用規約に記載
8			サービス利用において免責条項定義	○×	○	利用規約に記載
アプリケーション運用						
9	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間366日（計画停止/定期保守を除く）	
10		計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	○×	○	3営業日前にはサービストップページのアナウンス項目内と公式Twitterアカウントにて通知
11		計画停止頻度	年間における計画停止の頻度	回	年2回	
12		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	○×	○	最低1ヶ月間の予告期間をもうけ、本ツールに関するお知らせもしくは当社公式ブログ等にて通知
13		サービス稼働率	サービスを利用できる確率（計画サービス時間－停止時間）÷計画サービス時間	稼働率	99.989% (直近1年の実績)	
14		ディザスタリカバリ	災害発生時のシステム復旧のサポート体制	○×	○	
15		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	○×	○	必要に応じて、自動バックアップから履歴の提供が可能
16		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	○×	○	JSONファイルエクスポート機能を提供しており、任意のタイミングでダウンロード可能
17		アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	○×	○	セキュリティ上重要なアップデートは即時対応、その他は定期的(最長でも3ヶ月に1回程度)にアップデートを実施
18			信頼性・可用性を確保する対策が講じられている（サーバやストレージやネットワークの多重化・冗長化、システムの自動バックアップ等）	○×	○	AWSのマルチアベイラビリティーゾーン構成、自動スケーリングを実施
19	信頼性	障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	回	2回	
20		システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視体制	○×	○	下記事項の管理を実施 ・AWS IAMユーザごとの各マネージドサービスごとの最終利用日時
21		障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）がある	○×	○	発生から1時間以内に公式Twitterアカウントにて通知
22		ログ管理	利用者に提供可能な各種ログ（アクセスログ、操作ログ、エラーログ等）の提供	○×	○	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供

クラウドサービスチェックリスト						
No.	種別	サービスレベル項目	規定内容	測定単位	対応可否	実施内容/備考
23		ログ管理	システムの操作ログの管理が行われていること	○×	○	システムの操作、データベースの操作全てログ管理実施
24			参照または提示可能な障害ログの期間	期間	2年間	
25	拡張性	外部接続性	既存システムや他のクラウドサービス等の外部システムとの接続仕様（API、開発言語等）がある	○×	○	API（プログラム機能を外部から利用するための手続き）を公開
サポート						
26	サポート	ヘルプデスク	ヘルプデスク窓口が設置されている	○×	○	
27		サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	24時間366日（メール）	
28		サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	営業時間(10:00-19:00)内（メール）（年末年始・土日・祝祭日を除く）	
29		FAQ	FAQが公開されている	○×	○	
データ管理						
30	データ管理	暗号化	暗号化が自動的に行われる、または、暗号化機能が提供されている	○×	○	Amazon Aurora のリソース暗号化を適用し、パスワードの暗号化/データベースの暗号化/通信の暗号化を実施
31		データバックアップ	データのバックアップが行われ、最低でも1日前の状態に復旧できるような対策が講じられている	○×	○	最長21日間、デイリーのデータベースのスナップショットを作成
32		バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法が確立されている	○×	○	データベースは日次バックアップを自動取得。アプリケーションコードやインフラ定義はバージョン管理を実施
33		データ消去の要件	サービス解約後の、データ消去の実施	○×	○	利用終了後、自動で削除
34			複数のサーバにデータを保存している場合、レコード単位でデータを消去したときには各サーバ上のデータ消去がされている	○×	○	データの作成・更新・削除は同期されている
35		同期	全てのサーバやネットワーク機器で時刻の同期がとられている	○×	○	
36			全ての情報処理システムのクロックで使用している時刻源がある	○×	○	Amazon Time Sync Serviceを使用
37		利用データ制限	クラウドサービスを利用するにあたって、利用企業にシステム資源（CPU、メモリ、ディスクなど）を割り当てる場合、割り当てられているシステム資源の限界値と超えた場合の対策	○×	○	添付ファイルの容量上限に到達した場合、過去の添付ファイルを削除することで対策が可能
38		バックアップ世代数	保証する世代数	世代数	20世代	
39		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件	○×	○	

クラウドサービスチェックリスト						
No.	種別	サービスレベル項目	規定内容	測定単位	対応可否	実施内容/備考
40		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できている	○×	○	
41		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われている	○×	○	
42		入力データ形式の制限機能	入力データ形式の制限機能	○×	○	
43		環境	サービスの開発環境、試験環境、および運用環境は分離されている	○×	○	
セキュリティ						
44		情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されている	○×	○	
45		通信の暗号化レベル	端末からサーバまでの通信が暗号化されていて、システムとやりとりされる通信の暗号化強度対策がされている	○×	○	全ての通信でSSL/TLSを使用
46		情報取扱者の制限	・利用者のデータにアクセスできる利用者が限定されており、利用者組織にて規定しているアクセス制限と同様な制約が実現できている	○×	○	利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る
47		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されている	○×	○	
48		ウイルス対策	ウイルス、マルウェア感染への対策が講じられている	○×	○	開発マシンはウイルス対策ソフトのインストール、サーバーへはデプロイでのみファイル等のアップロードがされるように対応
49		ウイルススキャン	ウイルススキャンの頻度	頻度	自動で対応	AWS GuardDutyを用いて検知しており、自動で定義が更新
50		防御対策	障害や攻撃に対する監視、検知、解析、防御対策が行われている	○×	○	AWS WAFを用いた攻撃への対策を実行
51		不正アクセス	不正アクセスを防止するための技術が実装されている	○×	○	下記事項を実施 ・セキュリティグループを用いて必要最低限の通信のみを許可 ・ロードバランサーを除いた全てのサーバはNATゲートウェイを配備したプライベートサブネット内に設置し、パブリックインターネットに直接接続不可 ・AWS GuardDutyを用いてVPC内での不正な通信を検出 ・AWS WAFを用いてDoS対策を実施
52		不正利用	システムユーティリティを利用する場合に不正操作がなされないように管理されている	○×	○	バックアップ等はAWS上で操作が可能で、AWS IAMを用いて操作可能な権限を管理

クラウドサービスチェックリスト						
No.	種別	サービスレベル項目	規定内容	測定単位	対応可否	実施内容/備考
53	セキュリティ	二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管しており、廃棄の際にはデータの完全な抹消を実施し、また検証し、USBポートを無効化しデータの吸い出しの制限等の対策を講じている	○×	○	
54		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握している	○×	○	AWSのデータセンター管理に基づく
55		施設管理	十分な物理的および環境的セキュリティを備えたオフィスや施設においてサービスが提供されている	○×	○	下記事項の管理を実施 ・入退館（室）管理 ・オフィス、部屋及び施設に対する、物理的セキュリティ設計 ・自然災害、悪意のある攻撃又は事故に対する、物理的保護の設計 ・セキュリティを保つべき領域での作業手順の定義 ・荷物の受渡場所などの立寄り場所、およびび認可されていない者が施設に立ち入ることもある場所の管理
56		アクセス管理	システムへのアクセス権限や管理者特権の管理が行われている	○×	○	限られたメンバーのみアクセス権付与を実施し、権限付与のログも管理
57			利用企業のシステム管理者は、利用者IDごとに利用可能な機能及びアクセス権限を割り当てることができる	○×	○	
58			利用企業のシステム管理者が、利用企業の利用者ID及びアクセス権の確認方法がある	○×	○	設定画面からチームメンバーの権限確認可能
59			クラウドベンダーの管理者やオペレータなどのアカウントについて、不要時の速やかな削除および定期的な棚卸をおこなっている	○×	○	
60			接続元のグローバルIPアドレスを指定することで、指定した以外のグローバルIPアドレスからの利用制限ができる	○×	○	
61			モバイル端末（タブレット、スマホ、携帯電話など）の置き忘れや、放置したまま離席するなどによって、許可された本人以外の利用者がクラウドサービスを利用する事を防止するための機能	○×	○	短期間に一定回数以上ログイン失敗の際にアカウントロックを実施
62		認証	クラウドベンダーのシステム管理者による管理者権限での接続は、二要素での認証となっている	○×	○	ID/Passwordによる認証 2段階認証
63			利用企業によるクラウドサービスへの接続を特定IPアドレスや証明書保有端末に制限できる	○×	○	特定IPアドレス帯
64			利用企業によるクラウドサービスへの認証方法を二要素での認証とすること	○×	○	ID/Passwordによる認証 2段階認証

クラウドサービスチェックリスト						
No.	種別	サービスレベル項目	規定内容	測定単位	対応可否	実施内容/備考
65		セキュリティプロセス	全てのシステム開発ライフサイクルを通して、セキュリティに配慮したプロセスの確立	○×	○	下記を継続的に実施 ・アプリケーションの自動テスト、自動デプロイ ・ソースコードを保管するリポジトリのアクセス制限 ・プロビジョニングツールを用いたサーバ構成のコード化、構築の自動化、自動テスト ・インフラ定義のコード化、構築の自動化 ・開発、検証データの適正化