## 経済産業省　クラウドサービスレベルのチェックリスト

| No. | 種別 | サービスレベル項目例 | 規程内容 | 対応/可否 | 内容 |
|---|---|---|---|---|---|
| | | | **アプリケーション運用** | | |
| 1 | 可用性 | サービス停止時間 | 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） | ○ | 提供時間：原則 24時間365日。定期アップデート・セキュリティにおいて必要とされる不定期メンテナンスを除く。<br>サポート：平日 10時～18時 |
| 2 | | 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） | ○ | システム保守やアップデート等に伴う計画メンテナンスを実施する場合は、サービス内お知らせ機能により、事前に利用者へ通知いたします。 |
| 3 | | 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） | ○ | サービス提供を終了する場合は、事前に利用者へ通知し、必要に応じて移行期間を設けます。 |
| 4 | | 突然のサービス提供停止時の対処 | プログラムや、システム環境の各種設定データの預託等の措置の有無 | | 現時点では、プログラムおよび設定情報等の第三者預託は実施しておりません。<br>なお、データは AWS上で冗長化・バックアップを実施し、保全体制を確保しております。 |
| 5 | | 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） | | 月間稼働率 99.9%以上を目標としてサービス提供を行っております（計画停止を除く）。<br>なお、本サービスはクラウド基盤上に構築されており、インフラの可用性は基盤サービスに依存します。 |
| 6 | | ディザスタリカバリ | 災害発生時のシステム復旧／サポート体制 | ○ | マルチAZ構成による冗長化および定期バックアップを実施しています。<br>大規模障害発生時にはバックアップから環境を再構築し復旧します。 |
| 7 | | 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 | ○ | 重大障害時には、影響範囲に応じてバックアップデータの活用等により、<br>サービスの早期復旧または代替対応を実施いたします。 |
| 8 | | 代替処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 | ○ | 必要に応じて、CSV等の一般的なデータ形式でデータを提供することが可能です。 |
| 9 | | 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 | ○ | 重大な脆弱性については情報配信され次第速やかに対応し、<br>それ以外の脆弱性対応は定期メンテナンス時に適用しています。 |
| 10 | 信頼性 | 平均復旧時間 (MTTR) | 障害発生から修理完了までの平均時間（修理時間の和 ÷故障回数） | ○ | 障害の重要度に応じた復旧目標時間を設定しており、<br>重大障害については原則 4時間以内の復旧を目標としております |
| 11 | | 目標復旧時間 (RTO) | 障害発生後のサービス提供の再開に関して設定された目標時間 | ○ | 目標復旧時間（RTO）は障害の重要度に応じて以下の通り目標値を設定しております。<br>・重大障害（サービス停止）：4時間以内のサービス再開を目標<br>・中程度障害（一部機能制限）：翌営業日以内のサービス復旧を目標<br>・軽微障害：通常対応内での対応<br>※上記は目標値であり、障害内容および影響範囲により変動する場合があります。 |
| 12 | | 目標復旧時点 (RPO) | 障害発生後のサービス提供再開に対応するバックアップ世代管理の目標時間 | ○ | データは定期的にバックアップを取得しており、<br>障害発生時には直近のバックアップ時点までの復旧を基本としています。 |
| 13 | | 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 | ○ | 重大なサービス停止を伴う障害は、現時点において発生しておりません。<br>軽微な事象については都度対応を行っております。 |
| 14 | | システム監査基準 | 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 | ○ | システムの稼働状況について監視を行い、異常を検知した場合には通知される仕組みを導入しております。 |
| 15 | | 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） | ○ | 障害を検知した場合、影響範囲を確認の上、速やかに利用者へ通知いたします。 |
| 16 | | 障害通知時間 | 異常検出後に指定された連絡先に通知するまでの時間 | ○ | 通知のタイミングは障害の内容および影響範囲に応じて適切に判断いたします。 |
| 17 | | 障害監視間隔 | 障害インシデントを収集／集計する時間間隔 | ○ | システム監視により、異常を随時検知できる体制を構築しております。 |
| 18 | | サービス提供状況の報告 /間隔 | サービス提供状況を報告する方法／時間間隔 | △ | 定期的なレポート提供は実施しておりませんが、<br>サービス提供状況に関する情報は管理画面等にて随時ご確認いただけます。<br>また、障害発生時には速やかに利用者へ状況を通知いたします。 |
| 19 | | ログの取得 | 利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等） | ○ | 利用者の利用状況記録（ログ）および運用者の利用状況記録（ログ）を提供可能。 |
| 20 | 性能 | 応答時間 | 処理の応答時間 | ○ | 通常利用においては快適にご利用いただける応答性能を維持しておりますが、<br>データ量や利用環境等により変動する場合があります。 |
| 21 | | 遅延 | 処理の応答時間の遅延継続時間 | ○ | 応答遅延が発生した場合は原因調査および改善対応を行います。 |
| 22 | | バッチ処理時間 | バッチ処理（一括処理）の応答時間 | ○ | バッチ処理時間は処理内容およびデータ量、システム負荷状況に応じて変動します。 |
| 23 | 拡張性 | カスタマイズ性 | カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報 | ○ | 個別のカスタマイズには原則対応しておりませんが、サービス改善として機能追加を検討する場合がございます。 |
| 24 | | 外部接続性 | 既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（　API、開発言語等） | ○ | Slack連携により、特定の機能で通知を行うことができます。 |
| 25 | | 同時接続利用者数 | オンラインの利用者が同時に接続してサービスを利用可能なユーザ数 | ○ | 同時接続ユーザー数の上限は特に設定しておりません。 |
| 26 | | 提供リソースの上限 | ディスク容量の上限／ページビューの上限 | ○ | 利用可能なリソースはシステム構成および契約内容に応じて提供しております。 |
| | | | **サポート** | | |
| 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 | ○ | メール受付：24時間365日<br>電話窓口：平日 10時～18時（年末年始・夏季休暇を除く）<br>※メールによるお問い合わせを基本としております。<br>※営業時間外にいただいたお問い合わせは、翌営業日以降の対応となります。<br>※重大な障害が発生した場合は、必要に応じて営業時間外でも対応を行う場合があります。 |
| 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 | ○ | メール受付：24時間365日<br>電話窓口：平日 10時～18時<br>※年末年始・夏季休暇期間を除く |
| | | | **データ管理** | | |
| 29 | 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 | ○ | 毎日、全てのデータをバックアップしています。 |
| 30 | バックアップデータを取得するタイミング　(RPO) | | バックアップデータをとり、データを保証する時点 | ○ | 定期的にバックアップを取得しています。<br>障害発生時には直近のバックアップ時点までの復旧を基本としています。 |
| 31 | バックアップデータの保存期間 | | データをバックアップした媒体を保管する期限 | ○ | 障害用バックアップデータにつきましては、 1週間以上前のデータは保持していません。 |
| 32 | データ消去の要件 | | サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法 | ○ | 契約終了時にデータを廃棄します。引き渡しは行っていません。 |
| 33 | バックアップ世代数 | | 保証する世代数 | ○ | 7世代残しとなっています。 |
| 34 | 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、暗号化要件の有無 | ○ | SSL(HTTPS)通信で通信の暗号化を行っています。<br>データ出力時も暗号化を行い保護しています。 (HTTPS, 署名付きURL)。 |
| 35 | マルチテナントストレージにおけるキー管理要件 | | マルチテナントストレージのキー管理要件の有無、内容 | ○ | マルチテナント環境においては、テナント単位でデータを論理的に分離して管理しております。<br>また、クラウド基盤（AWS）のセキュリティ機能を利用し、アクセス制御および適切な鍵管理のもとでデータ保護を実施しております。 |

# Nsync_セキュリティチェックシート_2026.4

| | | | | |
|---|---|---|---|---|
| 36 | **データ漏えい・破壊時の補償／保険** | データ漏えい・破壊時の補償／保険の有無 | | データ漏えい・破壊に関する補償は行っておりません。<br>ただし、データ保護の観点から、アクセス制御、バックアップ、冗長化等の対策を講じ、<br>情報セキュリティの確保に努めております。 |
| 37 | **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こと | ○ | 契約終了時には、当社環境上のデータを適切に削除いたします。<br>なお、利用者からのご要望に応じたデータのエクスポート対応については、内容に応じて別途費用にて対応いたします。<br>データ削除にあたっては、外部への漏えいが発生しないよう管理された手順に基づき実施いたします。 |
| 38 | **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こと | ○ | データの整合性に配慮した管理を行っており、必要に応じて確認作業を実施しています。 |
| 39 | **入力データ形式の制限機能** | 入力データ形式の制限機能の有無 | ○ | 入力データについては、不正な値や想定外の形式を受け付けないよう、クライアント側およびサーバー側の双方で入力形式の制限機能を実装しています。 |
| | | **セキュリティ** | | |
| 40 | **公的認証取得の要件** | JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること | ○ | 情報処理管理に関する公的認証として、ISMS認証を取得しています。 |
| 41 | **アプリケーションに関する第三者評価** | 第三者によるウェブアプリケーション脆弱性評価実施 | ○ | クラウド環境に対して脆弱性管理サービスを用いた継続的な脆弱性評価・監視を実施し、検出事項に応じて必要な是正対応を行っています。 |
| 42 | **情報取扱い制限** | データをバックアップした媒体を保管する期限 | ○ | データは適切な管理体制のもとクラウド環境にて保管・運用しており、<br>アクセス制御および監視体制を整備しています。 |
| 43 | **通信の暗号化レベル** | システムとやりとりされる通信の暗号化強度 | ○ | システム間および利用者との通信については、適切な暗号化強度を有する標準的な暗号化プロトコルを用いて保護しています。これにより、通信データの盗聴、改ざんおよびなりすましの防止を図っています。 |
| 44 | **会計監査報告書における情報セキュリティ関連事項の確認** | 会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の 18号監査報告書」 | | 当該監査報告書（SAS70 Type2／18号監査報告書）は保有しておりませんが、<br>当社の運用体制、アクセス管理、データ保護、バックアップ等に関する資料を提示し、<br>個別にご説明・確認対応を行っております。 |
| 45 | **マルチテナント下でのセキュリティ対策** | 異なる利用企業間の情報隔離、障害等の影響の局所化 | ○ | アプリケーションおよびデータ管理上の制御により論理的に分離して管理しております。 |
| 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いること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こと | ○ | 利用者データへのアクセスは、業務上必要な範囲に限って許可する運用としており、権限管理によりアクセス可能な利用者を限定しています。また、利用者組織におけるアクセス制限の考え方に沿った制約を設けるよう配慮しています。 |
| 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るか | ○ | アクセス履歴はアクセスログとして保管しており、各利用者には一意の　IDを付与しています。また、当該 IDに紐づく形でユーザー単位の監査ログを保存しているため、識別情報を用いた検索が可能です。 |
| 48 | **ウイルススキャン** | ウイルススキャンの頻度 | ○ | クラウド環境において脅威検知および監視を行い、<br>不正アクセスやマルウェア等のリスクに対する対策を実施しています。 |
| 49 | **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いること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、 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こと | ○ | バックアップを含む保存データは、保管時に暗号化された状態で管理しています。なお、当該データはクラウド環境上で管理しており、外部記憶媒体その他の二次記憶メディアに保存・保管する運用は行っていません。 |
| 50 | **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か | ○ | 日本の法令・規制を踏まえ、データを保存・処理し、利用・アクセス管理・削除等の必要な制約条件を把握したうえで運用しています。 |