No	確認事項	チェック項目
1	サービス事業者による情報資産の取扱い	外部サービスで取り扱う情報資産がサービス事業者により、目的外利用されないこと。
2	データセンターの物理的対策	外部サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（以下データセンターという）は、地震・水害・火災への対策が行われていること。
3	データセンターの所在	データセンターは、日本の法令が適応されること。また、管轄裁判所に関しては、日本国内の裁判所を合意管轄裁判所とできること。
4	セキュリティ管理水準	サービス提供事業者若しくはサービスは、情報セキュリティや個人情報保護に係る第三者認証等のレポートにより、その管理水準が適正と認められていること。
5	リソース容量・能力の確保	業務を実施するうえで必要となるリソースの容量・能力が確保されていること。
6	サービスの監視	サービスの提供に用いるアプリケーション、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の死活監視・障害監視を行っていること。
7	脆弱性の管理	サービスの提供に用いるアプリケーション、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的脆弱性に関する情報を収集し、適宜対策を行っていること。
8	通信の暗号化	情報の盗聴・改ざん等から保護するため通信の暗号化を行うこと。
9	不正アクセスの防止	不要なサービスを停止すること。 利用する通信プロトコル、ポートは必要最小限とし、利用していない通信プロトコル、 ポートはファイアウォール等にて自動的に遮断するとともに、マルウェア対策を実施すること。
10	アクセスログの管理	アクセス記録が保存されていること。なお、アクセス記録にはログイン成功だけでなくログイン失敗の記録も行うこと。また、これらの記録の正確性を確保するため、正確な時刻の設定が行われていること。
11	データの暗号化	サービスに保存されるデータは暗号化されていること。
12	データのバックアップ	データの消失対策として、定期的にバックアップがとられていること。また、復旧について、手順化されていること。
13	認証強化又はアクセス制限	ID・パスワードによる認証以外に、ワンタイムパスワードや生体認証等によるアカウント認証の強化、又は利用できるIPアドレスを制限する等のアクセス制限等が実施されていること。
14	データの消去	保存されるデータについてサービス利用終了時に適切に消去されること。 ※暗号化したデータの暗号鍵を無効化することでもデータ消去措置と見なせる。
15	仕様変更の通知	サービス仕様の変更やサービス終了等について、対応策が検討する期間を確保するため、サービス事業者から事前に通知がされること。
16	サービス稼働率とサポート	サービスの稼働率や、サポート・問い合わせ窓口等に関する記載があること。
17	セキュリティインシデント発生時の対応	利用者へ公開された情報セキュリティに関する統一的な窓口が設置されており、情報セキュリティインシデントが発生した際、利用者への報告、 収束に向けた対応等にかかる実施体制が確立していること。
18	免責事項等	サービス提供事業者の免責事項に関する記載があり、その記載内容は利用上問題ないこと。