別紙

クラウドサービスの利用に係る条件

サービス提供事業者の条件	
1	サービス提供事業者が情報セキュリティポリシーを利用者に明示している。
2	サービス提供事業者の情報セキュリティ管理状況に関する第三者による評価（ISMS認証取得証明書、外部監査報告書等）が行われていること。
サービス利用にあたっての条件	
1	サービスで取り扱う情報資産がサービス提供事業者により、目的外利用されないこと。
2	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サービス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	サービス提供事業者若しくは提案するサービスは、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	サービスは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・障害監視について監視が行われていること。
7	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、適宜対策が行われていること。
8	サービスは情報の盗聴・改ざん等から保護するため暗号化が行われていること。
9	不要なサービスを停止していること。 また、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遮断するとともに、マルウェア対策を実施していること。
10	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われていること。 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	サービスに保存されるデータが暗号化されていること。
12	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	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	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。 なお、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	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	サービスの稼働率や、サポート・問い合わせ窓口等に関する事項が示されていること。
17	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	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。