資料9

クラウドサービス・データセンター及び機器・サービス管理に係る要件

ア．障害発生時にサービスを継続するため、一つの障害の影響が及ばないよう、冗長化を図ること。また、バックアップ系に切り替わった際でもデータの整合性が取れるよう、リアルタイムでのデータ複製等、必要な対応を行うこと。

イ．取り扱う情報資産がクラウドサービス事業者やデータセンター事業者により、目的外利用されないこと。

ウ．サーバ・ストレージ、情報セキュリティ対策機器等が設置されているデータセンターは地震・水害・火災への対策が行われていること。

エ．データセンターの外観は看板や標識がない匿名性を確保すること。

オ．データセンターの建物、サーバー室の扉はIDカードや生体認証による入退室管理が実施されていること。

カ．機器が格納されているラック/ケージは施錠されており、データセンター事業者により鍵の管理がされていること。

キ．データセンターは監視カメラ等により24時間365日侵入者の検知を行っており、異常を検知した場合は警備事業者等により即時対応が可能であること。

ク．データセンターは、日本の法令が適応され、日本国内のデータセンターで運営管理等の全てが行われること。訴訟を提起する場合、三重県庁の所在地がある地方裁判所を第一審の専属管轄裁判所とすること。

ケ．データセンターへ引き込むインターネット回線は、複数社のサービスを利用していること。また、バックボーン回線は、利用するクラウドサービス専用の回線として、インターネットハブの近隣に配置されること。

コ．クラウド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。なお、ISMAPに登録されたクラウドサービスを利用することが望ましい。また、ガバメントクラウドの利用も検討のうえサービスの選定を行うこと。

サ．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。

シ．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。

ス．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。

セ．サービスの提供に不要なプログラム、サービスを停止すること。

ソ．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こと。

タ．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。

チ．保存されるデータは暗号化されていること。

ツ．データの消失対策として、1日1回以上のバックアップがとられており、2世代以上のバックアップデータを常時保持すること。

テ．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。

ト．クラウドサービスやデータセンターの仕様の変更やサービス終了等について、対応策を検討する期間を確保するため、クラウドサービス事業者・データセンター事業者から事前に通知がされること。

ナ．クラウドサービス・データセンターのサポート・問い合わせ窓口等に関する記載があること。

ニ．クラウドサービス・データセンターにて情報セキュリティインシデントや障害が発生した際、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。

ヌ．クラウドサービス提供事業者・データセンター事業者の免責事項や利用規約は本業務の実施にあたり問題ないこと。