〇〇〇〇年〇月〇日作成

# クラウドサービスにおける情報セキュリティ対策に関するチェックリスト（記入済み例）

## 対象：Aサービス（X株式会社）

| 番号 | リスクの種類 | 事業者による説明（実施している対策の概要） | 利用者記入欄 | |
|---|---|---|---|---|
| | | | 判断 | 判断の根拠 |
| H01 | クラウドサービスにおける高集約化がもたらす悪影響 | 何らかの異常や大災害が生じた場合でも、サービスの全面停止を防ぐため、地理的に離れた3箇所以上の拠点でサービスを提供しています。いずれかの拠点が稼働していればサービスの継続が可能です。 | 〇 | 対策として適切と判断。 |
| H02 | クラウドサービスを構成する仮想システムで障害が発生することによる被害 | 機器の障害や操作ミスがサービスに影響を及ぼさないようにするため、自動監視システムを常時稼働し、異常の早期検知を図るとともに、仮想システムで異常が生じにくくなるような設計を行い、厳格なテストを通じてその効果を検証済みです。 | 〇 | 自社運用よりも障害可能性は低いと見込まれることから、適切と判断。 |
| H03 | クラウドサービス内の他利用者の活動による悪影響 | パブリッククラウドサービスの性質上、他のお客様の活動による影響を完全に排除することは困難です。他利用者の影響が気になるお客様にはプライベートクラウドサービスをお勧めしております。 | × | 他利用者の影響を受けることは避けたいが、コスト的にプライベートクラウドの利用は困難。 |
| H04 | クラウドサービスの提供に必要な資源の枯渇による被害 | 通常の利用ではお客様が必要とされる資源が不足する心配はございませんが、万一不足となった場合はサービス約款に基づく対応をさせていただいております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| H05 | クラウドサービスにおいて他利用者が自分のデータにアクセスすることによる被害 | お客様毎にデータは完全に隔離されています。この隔離が失われることのないよう、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施するとともに、不正アクセスの早期検知のための監視システムを常時稼働させております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| H06 | クラウドサービスの基盤インフラへの攻撃がもたらす被害 | Aサービスの基盤インフラは、お客様用の通信回線とは別の回線を通じて管理しており、外部からの攻撃を困難にしております。さらに、弊社の情報セキュリティポリシーのもとにシステムの脆弱性対策を実施しております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| M07 | クラウドサービス事業者内での内部不正による被害 | Aサービスの運用に係る操作はすべて記録されており、運用担当者はその記録を停止したり、改ざんすることができない仕組みとなっております。こうした仕組みと監視体制により、内部不正を行うことは困難です。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| M08 | クラウドサービスの管理用システムが不正利用されることによる被害 | Aサービスの基盤インフラは、お客様用の通信回線とは別の回線を通じて管理しており、外部からの攻撃を困難にしております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| M09 | クラウドサービスと利用者の間の通信回線上での攻撃による被害 | オプションのVPNサービスをご利用いただくことで、お客様との通信回線におけるデータの暗号化が可能となっております。 | 〇 | オプション利用により対策可能と判断。 |
| M10 | クラウドサービス上で消去したはずの情報の残留による被害 | お客様がAサービス上で削除されたデータに他のお客様がアクセスするおそれはございませんが、ディスク上の残留情報に基づく復元を困難とするための対策は実施しておりません。 | 〇 | 自社アプリケーションにて、アプリケーション終了時に使用した領域を上書きする処理を追加することでリスクを低減。 |
| M11 | クラウドサービスに対するサービス妨害攻撃による被害 | 明らかなサービス妨害の場合、その通信を遮断する機能を備えています。また、著しく過大なサービス要求は自動的に制限されるため、サービス妨害攻撃の影響は緩和されます。 | 〇 | 自社運用よりも障害可能性は低いと見込まれることから、適切と判断。 |
| L12 | クラウドサービスにおける特定の規格への依存による悪影響 | Aサービスは業界標準の技術をもとに提供されており、他のサービスからの移行や接続において支障となるおそれはございません。 | 〇 | 自社アプリケーションの動作環境として問題ないものと判断。 |
| L13 | クラウドサービスを利用することによるお客様におけるガバナンスへの影響 | お客様による個別のセキュリティ監査の実施、システム構成や運用手順の開示等のご依頼につきましては、お引き受けいたしかねます。 | ／ | クラウドサービスについては自社システムとは別のポリシーにて運用。 |
| L14 | クラウドサービスが利用している外部委託先での障害による被害 | お客様へのサービス提供に関する部分での外部委託は実施しておりません。 | ／ | 外部委託を必要とするサービスを利用せず。 |
| L15 | クラウドサービス利用者の経済的損失を狙ったサービス妨害攻撃による被害 | 経済的損失を狙った攻撃（いわゆるEDoS攻撃）については、通常の利用との区別が困難であるため、特別の対策を講じることができません。 | ／ | サービスの可用性以外の経済的損失の恐れはないため、リスクの対象外。 |
| L16 | クラウドサービスで用いる暗号鍵の不適切な扱いによる被害 | 使用する暗号鍵については、その漏洩や喪失を防ぐための対策を講じております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| L17 | クラウドサービスに対する不正な探査による被害 | お客様用の通信回線やインターネットからの探査を遮断するための機能を設けているほか、不審な活動の早期検知のための監視システムを常時稼働させております。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| L18 | クラウドサービスに対する証拠提出命令と電子的証拠開示による悪影響 | 当局からの要請があった場合、お客様のデータを含む記録装置等の提出や押収や行われる可能性があります。 | 〇 | やむを得ないものと判断。 |
| L19 | クラウドサービス提供国との司法権の違いがもたらす悪影響 | Aサービスは日本国内で提供しており、司法権の問題が発生することはございません。 | 〇 | 国内でのサービス提供事業者として適切と判断。 |
| L20 | クラウドサービス事業者が、所有者の許可なくデータを利用することによる被害 | 弊社ではお客様の許可なくお客様のデータを契約外の用途で利用することはございません。 | 〇 | これまでのX社の運用実績から障害可能性は低いと判断。 |
| L21 | クラウドサービス上でのライセンス管理に関するトラブル | 弊社が提供するアプリケーション以外のライセンス管理については、関知しておりません。 | ／ | 自社開発アプリケーションを稼働予定のため、ライセンス上のリスクはない。 |

判断欄凡例：〇＝適切、×＝不適切、／＝対象外