Ver1.0.0

クラウドサービスセキュリティチェックシート

本チェックシートは、アールシーソリューション株式会社が運用する「BCP-PREP」、「防災クラウド」について、経済産業省が発行した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013年版）」を踏まえ、当社の利用環境や運用実態に合わせて項目の追記・見直し、および解釈の調整を加えて独自に作成したものです。
（参照元：https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）
本チェックシートは運用や改善のために予告なく変更することがあります。

【評価欄（記号）の定義】

○（適合）：要件を満たし、運用・管理を実施している

△（一部適合）：一部対応中、または代替対策を講じている

×（不適合）：未実施

ー（対象外）：自社運用範囲外（クラウド基盤側依存）または該当なし ※「△」「対象外」を選択した場合は、補足・実施内容欄に理由・代替策を明記しています。

項番	確認項目	評価要件	評価	補足・実施内容
0.	情報セキュリティ基本方針			
0-1	基本方針の策定と承認	経営陣によって承認された情報セキュリティ基本方針（ポリシー）を策定・文書化し、組織の方向性を明確にしていること。	○	当社では、代表取締役の承認のもと「情報セキュリティ基本方針」を策定・文書化しております。本方針に基づき、組織全体におけるセキュリティ管理体制および情報資産の保護に関する基本ルールを明確に定め、役員および全従業員へ周知徹底を図っております。
0-2	公開および周知徹底	策定した基本方針を全従業員へ周知徹底するとともに、クラウドサービス利用者（顧客）に対してWebサイト等で明示・開示していること。	○	入社時研修等を通じて全従業員へ周知徹底を図っております。また、顧客・外部利用者に向けては、当社コーポレートサイト（https://www.rcsc.co.jp/security）上に「情報セキュリティ基本方針」を常時公開・明示しております。
0-3	定期的なレビュー	基本方針は定期的、またはサービス提供環境や社会情勢における重大な変更が生じた際に、適宜見直し（レビュー）を行っていること。	○	年1回の定例見直しを実施しているほか、サービス提供環境の大幅な変更や法改正、セキュリティを取り巻く社会情勢の変化に応じて、随時基本方針のレビューおよび改定を行っております。
1	組織的・人的セキュリティ			
1-1	推進体制・第三者認証	情報セキュリティ責任者（CISO等）を設置し、ISMS（ISO/IEC 27001）やPマーク等の第三者認証に基づき運用を行っていること。	○	情報セキュリティ責任者（CISO）を設置し、全社的な推進・管理体制を整備しております。また、ISMS（ISO/IEC 27001）認証を取得・維持しており、同規格の基準に基づいた運用・リスクアセスメント・定期監査を継続的に実施しております。 取得認証規格　ISO/IEC 27001:2022 / JIS Q 27001:2023 認証登録番号　IS185 登録日　2019年10月24日 認証機関　一般財団法人 ベターリビング　システム審査登録センター
1-2	雇用時の管理	従業員・開発者との機密保持契約（NDA）締結、セキュリティ上の責任・義務の説明を行っていること。	○	雇用時および契約時にセキュリティ上の責任・義務に関する説明を実施しております。また、当社内で業務を行い秘密情報を取り扱うすべての者（役員、正社員、業務委託・開発パートナー等）に対し、入社・契約時に「個人情報保護および機密保持に関する誓約書」の提出を義務付けております。
1-3	教育・訓練	全従業員に対し、定期的な情報セキュリティ教育や標的型メール訓練を実施していること。	○	全従業員を対象にした「ISMS理解度確認テスト」を定期的に実施しております。
1-4	違反時の対応	セキュリティ規定違反が発生した場合の処罰基準および手続を定義していること。	○	社内規定違反および情報セキュリティ規定違反が発生した場合の懲戒・処罰基準については、「就業規則（懲戒規定）」において明確に定めております。また、違反発覚時の報告・対応手続については、インシデント対応手順に基づき厳格に対処する体制を整えています。
2	物理的・環境的セキュリティ			
2-1	入退室管理	サーバー室・データセンター等への入退室をICカードや生体認証等で厳格に制限・ログ記録していること。	―	当社提供サービスはすべてパブリッククラウド上に構築されており、自社での物理サーバーの所有・運用はありません。基盤となるクラウド事業者のデータセンターにおいては、多層防御構造、生体認証、監視カメラ、24時間365日のガードマン常駐およびログ記録等の厳格な物理アクセス制御が実施されていることを、SOC 2等の監査レポートにて確認しております。
2-2	環境障害保護（耐災害性）	火災・落雷・水害等の自然災害や過電圧・停電に対し、防火・耐震構造および自家発電装置/UPS等の防護措置を備えていること。	―	当社提供サービスはすべてパブリッククラウド上で運用しているため、物理的なデータセンター設備の自社所有・管理はございません。利用中のクラウド事業者におけるデータセンターでは、N+1以上の自家発電装置・UPSによる電源冗長化、耐震構造、自動消火設備等の環境障害保護措置が備わっており、これらはクラウド事業者の「SOC 2 Type 2 報告書」および「ISO/IEC 27001」等の第三者監査レポートにより確認・担保しております。
2-3	クラウド基盤の安全評価	AWS/GCP等のパブリッククラウドを利用している場合、基盤側の物理・環境セキュリティ（SOC 2報告書やISO/IEC 27017等）を確認・評価していること。	○	利用するパブリッククラウド基盤（AWS等）のセキュリティレベルについて、発行されるSOC 2報告書やISO/IEC 27017等の第三者認証取得状況を定期的に確認・評価し、物理・環境面の安全性を確認しております。
3	アクセス制御・ID管理			
3-1	API認証・認可	情報配信APIへのアクセスに対し、APIキー、OAuth2.0、HMAC署名等による適切な認証およびアクセス制御を適用していること。	○	当社が提供する情報配信APIへのアクセスに対しては、契約企業（顧客）ごとに固有のAPIキーを発行し、リクエスト時の適切な認証および認可制御を実施しております。また、通信経路はすべてTLS（HTTPS）により暗号化されており、不正な第三者による盗聴やAPIキーの漏洩を防止しております。
3-2	最小権限の原則（IAM）	システムおよびデータへのアクセス権限は業務上必要な最小限とし、定期的な見直しを実施していること。	○	システムおよびデータへのアクセス権限は、業務上必要最小限の範囲（最小権限の原則）に限定して付与しております。権限の付与にあたっては原則として都度期限付きで発行しているほか、定期的なアクセス権限の棚卸（見直し）を実施し、異動や退職、契約終了等に伴う不要な権限の速やかな削除・見直しを徹底しております。
3-3	特権ID管理・MFA	管理者権限（root, IAM管理者等）の利用者を限定し、多要素認証（MFA）の義務付けや操作ログの記録を行っていること。	○	管理者権限の利用者は必要最小限に限定し、すべての管理者アカウントにおいて多要素認証（MFA）を義務付けております。また、管理者によるすべての操作ログを取得・記録・保管し、厳重に管理しております。
4	ネットワーク・システム運用セキュリティ（BCP・高可用性含む）			
4-1	高可用性・冗長化（BCP）	単一障害点（SPOF）を排除するため、サーバー、DB、NW等を複数アベイラビリティゾーン（AZ）等で冗長化し、SLA/SLOを定義・監視していること。	△	SLO（サービスレベル目標）を定義し、システム稼働率および応答性能等の常時監視を実施しております。現状、サーバー・DB構成は単一AZ（または一部単一構成）運用となっておりますが、定期的な自動バックアップ（スナップショット）の取得および障害時の迅速な復旧手順・環境再作成プロセスを整備することで、定義したSLO内でのサービス復旧が可能な体制を維持しております。
4-2	DoS/DDoS・スパイク対策	アクセス集中や悪意あるDDoS攻撃に対し、レートリミット（接続制限）、CDN、WAF等による保護を実施していること。	△	専用のCDNやWAF等のトラフィック制御ツールの導入には至っておりませんが、サーバのCPU使用率やリソース状況等の常時モニタリング（監視体制）を実施しております。アクセス集中や異常負荷によるリソース逼迫の兆候を早期に検知し、迅速な状況把握や対応を行える体制を整えております。
4-3	ログ管理・監視	システムログ、アクセスログ、APIリクエストログを取得し、不審な挙動の早期検知や追跡が可能な体制を整えていること。	○	APIへのアクセス状況やエラー発生状況、不審なエラーコード等をモニタリングすることで、異常なアクセスや予期せぬ挙動を早期に検知し、インシデント発生時の原因追跡が可能な体制を整備しております。
4-4	脆弱性管理・マルウェア対策	定期的なOS/ミドルウェアのパッチ適用、脆弱性診断の実施、およびマルウェア感染・実行を防止する対策（権限分離等）を講じていること。	○	セキュリティホールや脆弱性に関するリスク情報を常時収集し、重要度に応じたセキュリティパッチの迅速な適用を実施しております。また、システム運用における不要な特権の排除や最小権限の原則（権限分離等）を徹底し、マルウェアの感染・不正実行リスクを軽減する対策を講じております。
5	データ保護・安全な開発・委託先管理			
5-1	データの暗号化	通信経路（TLS1.2/1.3等）および保管時（DB・ストレージ暗号化等）において、適切な暗号化を適用していること。	△	顧客の個人情報に繋がるような重要データについては、すべてストレージレベルで暗号化されたデータベース（DB）に格納し、厳重に保護しております。 一部システム用のデータベースにおいてはストレージ暗号化を未有効としておりますが、インターネット不通のプライベートサブネット（VPN/VPC配下）での運用を徹底し、外部からの直接アクセスを完全に遮断しております。さらに、アクセス権限の最小化や接続元IPアドレスの厳格な制限、定期的なアクセス権限の棚卸し等を組み合わせることで、システム全体の安全性を高度に担保しております。
5-2	マルチテナント隔離	企業ごとのデータ（安否確認データ、緊急連絡先等）が論理的・物理的に分離され、他顧客からの参照・書き換えを防止していること。	○	データベース上で企業ごとに論理的にデータを識別・分離し、システム（プログラム）層において自社以外のデータへのアクセスを遮断するアクセス制御を適用しております。他顧客からのデータ参照・改ざんが発生しない安全なマルチテナント構造を確立しております。
5-3	データ完全性・信頼性・バックアップ	保管・通信データの改ざん・破損を防止する措置を講じるとともに、定期的なバックアップを取得し、データの完全性・信頼性を担保していること。	○	保管データおよび通信データの完全性を確保するため、暗号化ハッシュ検証等の適切な保護措置を実施しております。また、目標復旧時点（RPO）に基づき重要データの定期的な自動バックアップ（スナップショット等）を実施・保管しており、データ破損やインシデント発生時にも速やかに正常な状態へ復元できる体制を維持しております。
5-4	安全な開発・委託先管理	安全なコーディング規約に基づく開発、リリース前のWeb/API脆弱性診断、および再委託先（クラウドベンダー等）への同等セキュリティ義務付けを行っていること。	○	開発プロセスにおいて安全なコーディング規約を遵守し、リリース前にはソースコードの静的解析ツールを用いた自動スキャン等を実施することで、潜在的な脆弱性やセキュリティ上の不備の早期発見・修正を徹底しております。なお、システム開発の外部再委託は行わずすべて自社内で完結・管理しているため、適切な品質・セキュリティ水準を保持しております。