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、総務省の「クラウドサービスの安全・信頼性に係る情報開示指針」を踏まえ、当社の利用環境や運用実態に合わせて項目の見直しを行い独自に作成したものです。

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。

情報開示項目			内容	当社回答
1	開示情報の時点	開示情報の日付	開示情報の年月日（西暦）	2026年10月1日
事業所・事業				
2	事業所等の概要	事業者名	事業者の正式名称（称号）	アールシーソリューション株式会社
			法人番号	3011101034016
3		設立年月日	事業者の設立年月日（西暦）	2002年8月8日
4		事業所	事業者の本店所在地	〒160-0023 東京都新宿区西新宿8丁目14番21号 双英ビル3階・6階
			事業者ホームページ	https://www.rcsc.co.jp/
5		主な事業の概要	事業者の主な事業の概要	防災・減災ソリューション ・情報提供サービス ・システム開発 ・運用・保守 ・コンサルティング
コンプライアンス				
6		情報セキュリティに関する組織体制の状況	情報セキュリティに関する責任者の有無と、「有り」の場合は責任者名・役職	有り 弊社ISMSに基づき、実施しています。
			情報セキュリティに関する組織体制の有無	有り 弊社ISMSに基づき、実施しています。
7	個人情報	個人情報の取扱い	個人情報の取扱いに関する規程等の有無と、「有り」の場合は記載箇所	有り 弊社プライバシーポリシーにて公開しています。 https://www.rcsc.co.jp/privacy
8	守秘義務	守秘義務契約	守秘義務に係る契約又は条項の有無	有り 就業規則に記載があります。
			守秘義務違反があった場合のペナルティ条項の有無	有り 就業規則に記載があります。
9	従業員教育等	従業員に対するセキュリティ教育の実施状況	従業員に対するセキュリティ教育実施に関する取組状況	弊社ISMSに基づき、実施しています。
10	文書類	情報セキュリティに関する規程等の整備	情報セキュリティに関する基本方針・規程・マニュアル等の状況と文書名	弊社ISMSに基づき、更新・管理しています。
11		事業継続に関する規程の整備	事業継続に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	有り 文書名は非公開。
12		リスク管理に関する規程等の整備	リスク管理に関する基本方針・規程・マニュアル等の有無と、「有り」の場合は文書名	有り 文書名は非公開。
サービス基本特性				
13	サービス内容	サービス名称	本ASP・SaaSのサービス名称	BCP-PREP・防災クラウド
14		サービス開始時期	本ASP・SaaSのサービス開始年月日（西暦）	BCP-PREP　2023年10月 防災クラウド　2017年9月
15		サービスの内容・範囲	本ASP・SaaSのサービスの内容・特徴	ホームページで各サービスを紹介しています BCP-PREP　https://bcp-prep.com/ 防災クラウド　https://www.rcsc.co.jp/bousai-cloud
			他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容	無し
16		サービス提供時間帯	サービスの提供時間帯	24時間365日
17		サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲（契約内容に依存する場合はその旨記述）	ご要望に応じて有料で対応いたします。詳細は弊社営業担当にお問合せください。
18		移行支援	本サービスを利用する際における既存システムからの移行支援の有無（契約内容に 依存する場合はその旨記述）	ご利用に関するご質問は問合せフォームから、または弊社営業担当にお問い合わせください。 BCP-PREP　https://bcp-prep.com/#section08 防災クラウド　https://www.rcsc.co.jp/sales-form
19	サービスの変更・終了	サービス（事業）変更・終了時等の事前告知	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	利用規約に従い、本サービスの廃止を行う場合には、1か月前までにご連絡します。
			告知方法	主にメールにて連絡。利用規約には弊社が適当と判断する方法と記載しております。
20		サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無と、「有り」の場合はその概要	無し
21	契約の終了等	情報の返却・削除・廃棄	契約終了時等の情報資産（利用者データ等）の返却責任の有無と、受託情報の返還 方法・ファイル形式・費用等	無し 契約終了後ただちに登録データを削除します。（アクセスログ除く）
			情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等	契約終了後ただちに登録データを削除します。（アクセスログ除く）
			削除又は廃棄したことの証明書等の提供	無し
22	サービス料金	料金体系	初期費用額	BCP-PREP　ホームページでご案内しております https://bcp-prep.com/ 防災クラウド　費用に関するご質問は問合せフォームから、または弊社営業担当にお問い合わせください。 https://www.rcsc.co.jp/sales-form
			月額利用額	BCP-PREP　ホームページでご案内しております https://bcp-prep.com/ 防災クラウド　費用に関するご質問は問合せフォームから、または弊社営業担当にお問い合わせください。 https://www.rcsc.co.jp/sales-form
			最低利用契約期間	非公開 弊社営業担当にお問合せください。
23		解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	無し
24		利用者からの解約事前受付期限	利用者からのサービス解約の受付期限の有無と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	有り 利用規約には本サービスを解約する場合、希望月の前月10日までに、メールまたは電話を通じてその旨を連絡すると記載しております。
25	サービス品質	サービス稼働設定値	サービス稼働率の目標値	99.99%を目標に運用します。 （計画停止、当社以外のサービス起因の停止を除きます）
			サービス稼働率の実績値	BCP-PREP　昨年度のサービス稼働率は100%です。 防災クラウド　昨年度のサービス稼働率は100%です。
			サービス停止の事故歴	非公開
26		サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	有り 監視サーバーにて収集しています。
			ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要	有り 監視サーバーにて収集しています。
27		認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称	ISO/IEC 27001取得 　認証登録範囲：防災・減災ソリューション、情報提供サービス、システム開発、運用・保守、コンサルティング、適用宣言書（第5版） 　認証登録番号：IS185
28		脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	有り（※ソースコード静的解析およびアプリケーション検証） 開発プロセスにおいて安全なコーディング規約を遵守するとともに、リリース前の段階でソースコードの静的解析ツールを活用した自動スキャンを実施し、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。 また、システム開発の外部再委託は行わずすべて自社内の開発チームで完結・管理しているため、コードの品質およびセキュリティ統制が厳格に保たれる体制をとっております。
29		バックアップ対策	利用者データのバックアップ実施インターバル	日次でデータのバックアップを行います。 バックアップしたデータは、1世代分保管しており当社システム管理者のみがアクセス可能。
			世代バックアップ（何世代前までかを記述）	1世代
30		サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	サーバーは複数台で負荷分散しておりサービスが停止しにくい構成になっています。
			DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要	有り 弊社事業継続に関する基本方針・規程・マニュアルに従い対応します。
アプリケーション等				

31	連携	他のASP・SaaSとの連携状況に関する情報提供	他のASP・SaaSとの連携の有無と、「有り」の場合は情報提供の条件等	有り 弊社サービスは主にアマゾン ウェブ サービス（AWS）、さくらのクラウドを利用して提供しています。
32	セキュリティ	死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	有り 本サービスを構成するすべてのサーバー（Web/APIサーバー、データベースサーバー等）および主要なAPIエンドポイントを対象としております。HTTP/HTTPSリクエストおよびPingによる定期的なポーリング監視を常時（24時間365日）実施しており、応答遅延や停止等の異常検知時には即座に運用担当者へ自動アラート通知・緊急対応が行われる体制を整備しております。
33		時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	有り AWS、さくらのクラウドが提供する標準の時刻同期サービス（NTP）を利用し、常に正確な時刻を維持しています。
34		ウイルス対策	ウイルス対策の有無	有り サービス運用管理者が利用する運用端末はウイルス対策ソフトを導入しております。 当社サーバーにおきましては、ウイルス対策ソフトウェアの導入は行っておりません。ネットワークおよびシステム層における厳密なアクセス制御を施し、想定外のデータ流入をブロックする設計としているためです。
35		管理者権限の運用管理	システム運用部門の管理者権限の登録・登録削除の手順の有無	有り 弊社保守運用部門が管理者・利用者権限の管理を手順に従い実施しています。
36		ID・パスワードの運用管理	事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の状況	弊社サービスではスワード漏洩リスクを排除するため、パスワードを保持・発行せず外部認証基盤を利用しております。
37		記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、その保存期間及び利用者への提供可否	アプリケーション上の操作ログは取得しておりませんが、サーバー側でアクセスログ（IPアドレス、アクセス日時、リクエストURL）を記録しています。
			システム運用に関するログの取得の有無と、「有り」の場合は保存期間	有り ログは1ヵ月保存しています。
			ログの改ざん防止措置の有無	有り 当社システム管理者のみログへのアクセスを可能としています。
38		セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	有り 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。
39		暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	一部無し（※ただし、厳格なアクセス制限・ネットワーク分離による代替保護を実施） 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。
40		その他セキュリティ対策	その他、特筆すべきセキュリティ対策を記述（情報漏えい対策等）	不正アクセス防止のために全サーバーにパケットフィルタを設定しアクセスを制限しています。
ネットワーク				
41	回線	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類	なし
			ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	SaaS基盤（クラウド環境）からインターネットへの接続ポイント（出口）まで。
42		推奨帯域	推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲	なし
43		推奨端末	パソコン、携帯電話等の端末の種類、OS等	なし
			利用するブラウザの種類	なし
44	セキュリティ	ファイアウォール	ファイアウォール設置等の不正アクセスを防止する措置の有無	あり
45		不正侵入検知	不正パケット、非権限者による不正なサーバ侵入に対する検知等の有無と、「有り」の場合は対応方法	なし パケット単位での不正侵入検知（IDS/IPS）専用ツールは配置しておりません。代替措置として、クラウド基盤上のセキュリティグループおよびネットワークACLにより、許可されたIP・ポート以外の通信を厳格に遮断しております。また、管理者権限のアクセスには多要素認証（MFA）等を義務付けており、非権限者による侵入リスクを抑制しております。
46		ネットワーク監視	事業者とエンドユーザとの間のネットワーク（専用線等）において障害が発生した際の通報時間	一律の時間は定めておりませんが、ご利用者の業務への影響が軽微でないと判断される事案については、弊社内で定める優先度定義に基づき、最優先で連絡を行う手順となっております。
47		ユーザ認証	ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法等	利用者からのアクセスは全てアクセストークンや認証鍵を介して許可します。
48		なりすまし対策（事業者サイド）	第三者によるなりすましサイトに関する対策の実施の有無と、「有り」の場合は認証の方法	DMARCによる送信ドメイン認証を実施し、メール起点のなりすましを防止しています。 加えて、EV SSL証明書の導入を検討しています。
49		暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	有り 伝送データは全てHTTPS通信で暗号化しています。
サービスサポート				
50	サービス窓口（苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	電子メール：operation-maintenance@rcsc.co.jp
51		営業日・時間	営業曜日、営業時間（受付時間）	対応時間　9時～18時　(平日夜間、土、日、祝日及び弊社指定休日を除く) 受付時間　電子メールは24時間265日受付けております。
52		サポート範囲・手段	サポート範囲	サービスの操作方法全般
			サポート手段（電話、電子メールの返信等）	電子メールでのお問い合わせを受けつけます。
53	サービス通知・報告	メンテナンス等の一時的サービス 停止時の事前告	利用者への告知時期（1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）	サービス安定化のため計画的なメンテナンスを実施します。緊急の場合を除き2週間前に告知します。
			告知方法	原則メールで告知します。
54		障害・災害発生時の通知	障害発生時通知の有無と、「有り」の場合は通知方法及び利用者への通知時間	一律の時間は定めておりませんが、ご利用者の業務への影響が軽微でないと判断される事案については、弊社内で定める優先度定義に基づき、最優先で連絡を行う手順となっております。
55		定期報告	利用者への定期報告の有無（アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等）	稼働率や監視結果に関する利用者への定例報告（定期レポートの発行等）は実施しておりません。ただし、サービス障害やメンテナンスなど利用者に影響が生じると判断した事象につきましては、サービス公式サイト（Webサイト）等を通じて速やかに状況のご報告および情報開示を行う体制を整えております。