第三者証明書
クラウドサービス提供情報セキュリティ対策

№２０２５－ＪａＳＲＯ－５０２
令和８年１月１５日
一般社団法人 日本セキュリティ格付機構
JaSRO（Japan Security Rating Organization）

一般社団法人日本セキュリティ格付機構は、三谷産業株式会社のクラウドサービス提供における情報セキュリティ対策に関する調査を実施しました。

本書において、以下に掲載した事案が事実であることを第三者として証明します。

１．調査概要

企業・団体名	三谷産業株式会社
調査スコープ	クラウドサービス(仮想基盤サービス)
調査対象	クラウドサービス提供における情報セキュリティ管理
調査事項	クラウドサービス提供における情報セキュリティ管理状況（※１）
リファレンス	総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）２０２１年９月」
調査日	２０２５年１０月１日～２０２６年１月７日
本書交付日	初版交付日：２０２５年１０月１６日　改訂版交付日：２０２６年１月１５日
利用期限	２０２５年１０月１６日から１年（※２）
証明 ID コード	100002301155S2501

※１　調査の方法は、責任者等へのヒアリング、規程および台帳類の閲覧、関連設備の視察を用いております。

※２　当証明書は、調査実施日における事象について事実であることを証明するものであり、継続的に当該事象が必ず存在することを保証するものではありません。また、調査対象の仕様変更や社会環境の変化に応じ、緊急時には随時、また平常時には年一回の再調査による点検を推奨しています。

●お問い合わせ先　一般社団法人日本セキュリティ格付機構　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

２．確認結果

（１）経営管理

① 三谷産業グループとしての統制に加えてクラウドサービスを提供しているアウトソーシング事業のためのＩＳＭＳ推進組織である情報セキュリティフォーラムが機能しており、管理組織体制、情報セキュリティ規程類の整備、情報資産の識別、リスクアセスメント、人的セキュリティ、物理的アクセス管理、アクセス制御、委託先（子会社）管理、インシデント対応・危機管理、コンプライアンス等、非常に高いレベルで統制が進められている。現場部門では、お客様からの預かり資産を確実に守るため、物理的アクセス管理やITサービスの運用管理等が着実に実施されている。

② リスクへの対応、事業継続計画（ＢＣＰ）の取り組みとして、リスクマネジメント委員会が設置され、リスクマネジメントに係る計画等の重要事項の承認及びマネジメントレビューが実施されている。

③ 当該サービスを提供しているデータセンターの建物・設備は、「総務省：公共ＩＴにおけるアウトソーシングに関するガイドライン」「ＩＤＣイニシアティブ：ＩＤＣ活用ガイドライン（高品位規格）」の指針、「ＦＩＳＣ：金融機関等コンピュータシステムの安全対策基準　（Ⅶ.設備基準　１　コンピュータセンター）　２０２４年３月（第１２版）」に準拠したデータセンター専用の建物・設備である。また、「日本データセンター協会：データセンターファシリティスタンダードVersion3.0」の評価項目およびＩＴサービスの継続対策に対してのプロセス内容・品質、および企業統治について、第三者による客観的な評価を実施している。

④ データセンターの運用を担当しているコンフィデンシャルサービス株式会社は、２０２０年８月ＩＴＳＭＳ認証を取得し、データセンターにおける顧客向けサービスの提供をサポートするサービスマネジメントシステムを運用し、サービス可用性、完全性を管理している。

（２）事業継続管理

① 自然災害（地震・台風・洪水・雪害等）の発生を想定した対応策の策定および定期的な見直しを実施している。地震対策マニュアルの策定、グループ全社震災訓練の実施、新型インフルエンザ対策マニュアル策定，新型コロナウィルス感染症対策マニュアル策定等を実施している。

② 業務事故（火災、輸送事故、環境汚染物質の流出、当社データの流出・紛失等の業務活動に起因するリスク等）への対応策の策定及び定期的な見直しを実施している。情報セキュリティ格付「ＡＡＡis（トリプルA）」継続認定、情報セキュリティ制度の導入及び運用、情報セキュリティ事故点検の実施、車両運行管理システムの導入及び運用等を実施している。

③ その他企業を取り巻くリスク及びオポチュニティ（財務、戦略、経済・社会的要因、法務、内部人的要因、外部人的要因、長期的な社会変動（気候変動、人口動態の変化、技術の進化））に対する対応策の策定及び定期的な見直しを実施している。

（３）人事管理

① 三谷産業グループ企業倫理憲章にてコンプライアンスを宣言し、「コンプライアンスガイドライ

●お問い合わせ先　一般社団法人日本セキュリティ格付機構　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org

ン」にて関係法令を示して、関係部門および法務部門が法令改正等の監視を実施している。コンプライアンス教育は継続的に実施され、情報セキュリティフォーラム、内部統制推進委員会にて評価改善が行われている。

② 社員が安心して働ける環境づくりとして、独自の研修制度、奨学金手当支給制度、カウンセリング制度、社宅・寮制度、育児介護休暇制度、継続雇用制度、テレワーク制度の充実等に取り組んでいる。

（４）クラウドサービス提供における情報セキュリティ対策実施状況確認事項

総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）２０２１年９月」は、クラウドサービスの情報セキュリティ対策として、クラウドサービス提供事業者が実施すべきセキュリティ対策等をまとめたガイドラインである。三谷産業株式会社のクラウドサービスでは、そのガイドラインに示された対策項目について対策を講じている。なお、以下の表では、クラウドサービス提供における情報セキュリティ対策のうち、「Ⅱ．共通編」、「Ⅳ．PaaS/IaaS 編」の対策を対象として、基本区分に該当する対策の実施状況について整理して掲載している。

なお、当該クラウドサービスは、日本国内の自社資源でのみ提供している。他組織である供給者のサービスを利用したクラウドサービスは提供していない。他国の資源、サービスの利用や他組織である供給者のサービスの利用に関するリスクがない。

領域	目的	対策項目	実施状況
Ⅱ．共通編 Ⅱ．1．情報セキュリティへの組織的取組の基本方針	Ⅱ．１．１．組織の基本的な方針を定めた文書	・方針の作成・承認・配布 ・方針の変更	・基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布している。 ・経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知している。
Ⅱ．共通編 Ⅱ．２．情報セキュリティのための組織	Ⅱ．２．１．内部組織	・情報セキュリティ責任者 ・システム一覧 ・相反する職務と責任の分離	・ＩＳＭＳ管理において、情報資産の保護と情報セキュリティプロセスの実施に対する責任を明確に規定し、その責任者を記述している。 ・情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載している。 ・システム設計・構築及びサービス運用・設定の実務を行うものと認可を行うものの役割と責任を明確にしてい

●お問い合わせ先　一般社団法人日本セキュリティ格付機構　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

			る。さらに、開発・保守の実務を行うものと運用を行うものの役割と責任を明確にしている。又、重要なシステム変更に対しては特別な承認手続きを実施している。
	Ⅱ．２．２．モ モバイル機器及びテレワーキング	・モバイル機器の方針 ・テレワーキングでの情報保護	・モバイル機器に適合した認証方法を提供して、アクセス制御を確実に実施している。モバイル機器との通信は暗号化している。 ・テレワーキングでアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施している。
Ⅱ．共通編 Ⅱ．３．サプライチェーンに関する管理	Ⅱ．３．１．サプライチェーン事業者間の合意	・リスク対策と文書化 ・サービスの監視 ・リスク評価とレビュー ・関連情報の保護 ・侵害通知 ・変更管理	・サプライチェーン事業者が提供するクラウドサービスは利用していない。
	Ⅱ．３．２．サプライチェーン事業者の選定	・選定・契約	・サプライチェーン事業者が提供するクラウドサービスは利用していない。
Ⅱ．共通編 Ⅱ．４．資産の管理	Ⅱ．４．１．資産に対する責任	・資産の管理責任 ・事業者間の引継ぎ ・バックアップ	・資産の管理ポリシーと管理水準を規定し、ファシリティ性能、情報セキュリティ品質、IT サービス継続について、第三者機関による評価や確認を行い利用者に提供している。 ・利用者が契約を終了する場合、利用者の情報資産は利用者の責任で事業者間の引継ぎや削除することとしている。 ・情報、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、定期的に実施し、バックアップ内容を検査している。具体的には、利用者ごとに仮想環境を提供しており、仮想環境毎のバックアップ（１回／日）を実施している。また、バ

●お問い合わせ先　一般社団法人日本セキュリティ格付機構　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

			ックアップについてはリカバリ訓練も実施している。
	Ⅱ．４．２． 情報分類	・資産目録 ・データ識別 ・資産の取扱い	・利用者の情報資産とクラウドサービスを運用するための情報資産を分類し管理している。仮想化した資産についても利用者ごとに明確に区分して管理している。 ・利用者の情報資産は利用者ごとに明確に区分して管理している。また、管理状況については、利用者、クラウドサービスの種類によらず、最重要と定義し管理している。加えて、利用者のデータ及びクラウドサービスから派生したデータを明確に識別し管理している。
	Ⅱ．４．３． 情報セキュリティポリシーの遵守、点検及び監査	・レビュー ・点検	・情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行っている。また、組織の情報セキュリティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に実装されていることをレビューしている。 ・情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的（一年毎）に、クラウドサービスの運用を含めた管理策の監査を実施している。また、第三者評価（認証、格付等）等を用いて定期的に点検している。なお、システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、実施している。
	Ⅱ．４．４． アクセス管理	・アクセス制御方針	・各種アクセス制御権限、内部統制が機能した権限付与プロセス、ＩＤ管理フレームワークをアクセス制御ガイドラインに規定し運用している。

●お問い合わせ先　一般社団法人日本セキュリティ格付機構　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

		・アクセス制御	・特権的アクセス権を管理する担当者と特権的アクセス権を使用して作業する担当者を分離し、定期的に特権的アクセス権使用者の確認と認証情報の変更を実施している。 ・秘密認証情報については、管理者のみ扱うこととして管理している。 ・クラウドサービスに供するシステム及びアプリケーションに対して、第三者による不正アクセスを防止し、適正な利用を確保するためのアクセス制御措置を提供可能としている。
		・ユーティリティプログラムの使用 ・プログラムソースコードへのアクセス ・アクセス制御となりすまし対策	・ユーティリティプログラムで使用する特権ＩＤは、利用者に提供していない。特権ＩＤの利用は、管理ツールを使用して認証処理と操作記録の取得を行い管理している。 ・プログラムソースコードへのアクセスを制限している。 ・ID・パスワードを用いる場合は、その運用管理方法とパスワードの有効期限を規定している。また、場所や装置からの接続を認証する方法等によって、アクセス制御となりすまし対策を行っている。
	Ⅱ．４．５． 構成管理	・構成管理のポリシーと手順	・目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び構成管理ポリシーと関連する対応策の実施手順を策定している。
Ⅱ．共通編 Ⅱ．５．従業員に係る情報セキュリティ	Ⅱ．５．１． 雇用前	・雇用契約	・雇用予定の従業員に対して、情報セキュリティ上の要求及び責任を提示・説明のうえ、それらに対する明確な同意を得たうえで雇用契約を締結している。
	Ⅱ．５．２． 雇用期間中	・教育・訓練 ・契約違反	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための教育・訓練を実施している。 ・従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えている。
	Ⅱ．５．３． 雇用の終了又は変更	・アクセス権・資産の取扱い	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にしている。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

Ⅱ．共通編 Ⅱ．６．情報セキュリティインシデントの管理	Ⅱ．６．１． 情報セキュリティインシデント及びぜい弱性の報告	・組織内報告 ・クラウドサービス事業者とクラウドサービス利用者間の報告 ・インシデントの評価と分類 ・フィードバック ・証拠の収集・取得	・資産管理の責任を明確にするとともに、管理責任者を明確にし、報告すべき情報セキュリティ事象の内容と連絡先をエスカレーションルールにより規定し、実施している。 ・利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組みを整えている。 ・情報セキュリティ事象の取扱いルールを規定し、情報セキュリティインシデント分類の明確な基準を定めている。 ・情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いている。 ・情報セキュリティ事象発生時の証拠となり得る情報の収集、取得及び保存のための手順を定め、適用している。
Ⅱ．共通編 Ⅱ．７．コンプライアンス	Ⅱ．７．１． 法令と規則の遵守	・関連法規と記録 ・利用可否 ・ソフトウェア製品 ・不正アクセス・流出からの保護 ・暗号化	・個人情報、要配慮個人情報、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定したうえで、その要求に基づき適切な情報セキュリティ対策を実施している。また、クラウドサービスの提供及び継続上重要な記録について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理している。また、日本国内の資源・サービスでのみ、当該サービスを提供しており、利用者に対しては、利用規約、ＳＬＡで明確に記述し、契約終了時の取扱いについては契約書に記載している。 ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可外の目的によるシステム及び情報処理施設の使用を制限している。 ・知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の遵守を確実にするための適切な手順を実施している。 ・記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護している。また、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供している。 ・暗号化機能は、関連する全ての協定、法令及び規制を遵守して用いている。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

Ⅱ．共通編 Ⅱ．８．ユーザサポートの責任	Ⅱ．８．１． 利用者への責任	・責任 ・SLA ・情報提供	・利用規約・ＳＬＡにて、クラウドサービスの情報セキュリティマネジメントの責任範囲、サービスレベル、個別対応可能な範囲を明確にしている。 ・クラウドサービス検討者に対してＳＬＡを開示している。利用者の求めに応じて、ＳＬＡの遵守状況を提示している。さらに、第三者機関により情報セキュリティ対策状況を確認し、文書化し公開している。 ・提供しているクラウドサービスに対し、利用者からの苦情、懸念又は質問を受け取り、対応するためのプロセスを構築している。
	Ⅱ．８．２． 保守	・システム保守ポリシーと手順 ・保守管理 ・保守ツール ・リモート保守 ・保守要員 ・保守要員による保守 ・タイムリーな保守	・システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及び保守ポリシーを策定、文書化し、関係する組織に配布している。 ・保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録をレビューしている。 ・システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況をレビューしている。 ・提供しているクラウドサービスでは、リモート保守は行っていない。 ・保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持している。 ・必要なアクセス権限を持たない要員による保守活動を監督するために、必要なアクセス権限と技術的能力を有する職員を指定している。 ・システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行っている。
Ⅱ．共通編 Ⅱ．９．事業継続マネジメントにおける情報セキュリティ	Ⅱ．９．１． 情報セキュリティの継続	・情報セキュリティ継続計画の策定と実施 ・情報セキュリティ継続の検証、レビュー及び評価	・大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持している。 ・情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証している。
	Ⅱ．９．２． 緊急時対応計画	・緊急時対応計画の策定と手順	・目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、緊急時対応計画の実施手順を策定し、文書化している。
Ⅱ．共通編 Ⅱ．１０．その他	Ⅱ．１０． １．暗号と認証	・方針 ・情報提供 ・暗号鍵の作成と管理	・情報を保護するための暗号利用に関する方針を、策定し、実施している。 ・暗号を用いたアクセス制御を提供しており、暗号強度等の情報を利用者に公開している。 ・組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄している。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

	Ⅱ．１０． ２．開発プロセスにおけるセキュリティ	・開発プロセスにおける情報セキュリティへの取組	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組んでいる。
Ⅳ. PaaS/IaaS編 Ⅳ．１．運用における情報セキュリティ	Ⅳ．１．１． 運用管理	・情報セキュリティ監視手順の策定 ・運用管理端末 ・稼働・障害監視 ・追加報告 ・定期報告 ・時刻同期 ・パスワード管理 ・クラウドサービスの変更管理 ・リソース監視 ・環境分離 ・マルウェア対策 ・イベントログの取得 ・ログの保護 ・作業記録 ・ソフトウェア導入 ・技術的ぜい弱性	・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めている。また、クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ･ストレージ、情報セキュリティ対策機器、通信機器の時刻同期方法を規定し実施している。また、運用・管理に関する手順書を作成し実施している。 ・運用管理端末に、許可されていないプログラム等のインストールを行わない。また、ウイルスチェックを行っている。 ・クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行っている。稼働停止や異常を検知した場合は、クラウドサービス利用者に速報するとともに、フォローアップする追加報告を行っている。また、結果を評価・総括して、管理責任者に報告している。 ・クラウドサービスの提供に用いる管理機能を持つアプリケーション、プラットフォーム、サーバ･ストレージ、情報セキュリティ対策機器、通信機器の監視結果(障害監視、死活監視、パフォーマンス監視)について、定期報告書を作成して利用者等に報告している。 ・パスワード管理については、アクセス制御ガイドラインに規定し、良質なパスワードで運用している。 ・システムの変更は規程に基づき、作業毎に作業手順書を作成し関係者および情報セキュリティ責任者によるレビュー・承認を経て作業を実施している。重要なシステム変更に対しては特別な承認手続きを実施している。また、クラウドサービスに影響を与える可能性のある変更について、利用者に情報を提供している。 ・要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測している。また、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視している。 ・開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離している。 ・クラウドサービスに供する情報処理施設等へのマルウェアの感染防止を実施している。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

			・クラウドサービスとして必要なイベントログの取得を実施している。また、特権利用の作業は管理ツールにより認証処理と操作記録の取得を行い管理している。 ・ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護している。 ・運用システムに関わるソフトウェアの導入を管理するための手順を定め、実施している。 ・クラウドサービスの提供に供するネットワーク及びＩＴ機器に対して定期的に外部機関によるペネトレーションテストを行い、脆弱性の把握と必要な対策を実施している。
	Ⅳ．１．２．システム及び情報の完全性	・原本性確保 ・セキュリティ侵害の検知	・各種手順等情報資産の電子データについては、文書管理システムにて原本性の確保を行っている。 ・インターネットからのアクセスに対して、IPS 機能によりセキュリティ侵害の対策を行っている。
	Ⅳ．１．３．媒体の保管と廃棄	・媒体保管 ・廃棄 ・輸送	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行っている。 ・機器及び媒体を正式な手順に基づいて廃棄している。 ・情報を格納した媒体は、輸送途中の認可されていないアクセス、不正使用又は破損から保護している。
Ⅳ. PaaS/IaaS 編 Ⅳ．２．プラットフォーム、サーバ・ストレージ	Ⅳ．２．１．プラットフォーム、サーバ・ストレージの情報セキュリティ対策	・ウイルス対策	・クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージについてウイルス等に対する対策を講じている。 ・利用者がクラウドサービス上にインストールするシステムについては、利用者にて実施していただくこととしている。
	Ⅳ．２．２．プラットフォーム、サーバ・ストレージの運用・管理	・可用性 ・リソース	・ファシリティとしての冗長性と合わせて、ネットワークを含むシステムを冗長化している。 ・クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存している。
	Ⅳ．２．３．データの保護	・バックアップ ・バックアップ情報の完全性	・利用者ごとに仮想環境を提供しており、仮想環境毎のバックアップ（１回／日）を実施している。また、バックアップについてはリカバリ訓練も実施している。 ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認している。
Ⅳ. PaaS/IaaS 編	Ⅳ．３．１．ネットワーク	・ネットワーク構成 ・管理者の権限 ・不正アクセス防止	・ネットワーク構成図を作成している。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定している。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

Ⅳ．３．ネットワーク	における情報セキュリティ対策	・パケット検知 ・実施基準 ・通信の暗号化 ・サーバ証明書 ・情報セキュリティ特性 ・障害監視	・システム管理者及びネットワーク管理者の権限の割当て、使用を制限している。また、作業手順書を作成、関係者および情報セキュリティ責任者によるレビュー・承認を経て作業を実施している。なお、重要なシステム変更に対しては特別な承認手続きを実施している。 ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール等）を設置して対策を講じている。 ・不正な通過パケットを自動的に発見、若しくは遮断する措置を講じている。 ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えている。また、通信の暗号化を行っている。 ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施している。 ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定している。 ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報する仕組みを整えている。
	Ⅳ．３．２．情報の転送	・情報転送の方針及び手順 ・情報転送に関する合意 ・秘密保持契約又は守秘義務契約	・通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び対策を備えている。 ・組織と外部関係者との間で、業務情報のセキュリティを保った転送について、合意している。 ・情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、 定めに従ってレビューし、文書化している。
	Ⅳ．３．３．セッション管理	・セッションのライフサイクル管理 ・セッションの真正性 ・同時セッションの制御 ・セッションのロック	・セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)、通信セッションの真正性、各セッションの割り当て数の制御、アイドル時間を経過した場合セッションをロックする制御をファイアウォールによって実施している。
Ⅳ.PaaS/IaaS編	Ⅳ．４．１．建物の災害対策	・建物 ・電源 ・空調	・クラウド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システムが設置されている建物（情報処理施設）については、物理的及び環境上の危険を考慮して、システムが存在する施設の立地となっている。また、地震・水害に対する対策が行われている。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

Ⅳ．４．建物、電源(空調等)			・サーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じている。 ・サーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を備えている。
	Ⅳ．４．２．火災、雷、静電気からシステムを防護するための対策	・汚損対策 ・火災対策 ・雷対策 ・静電気対策 ・緊急遮断 ・非常用電源 ・非常用照明	・サーバ・ストレージ、情報セキュリティ対策機器等のシステムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じている。 ・サーバ・ストレージ、情報セキュリティ対策機器等のシステムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えている。 ・情報処理施設に雷が直撃した場合及び誘導雷が発生した場合を想定した対策を講じている。 ・クラウド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システムについて、作業に伴う静電気対策を講じている。 ・緊急時に利用者がシステムの電源を遮断したい場合は、事業者に連絡をいただき、実施することとしている。 ・一次電源が失われた場合に、長期間使用可能な代替電源への切り替えを支援する為の、無停電電源装置を用意している。 ・停電が発生した場合や、電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明をシステムに導入し、維持している。
	Ⅳ．４．３．装置の対策	・サポートユーティリティ ・ケーブル配線のセキュリティ ・装置の保守 ・資産の移動 ・構外にある装置及び情報資産のセキュリティ ・装置のセキュリティを保った処分又は再利用 ・無人状態にあるクラウドサービス利用者装置 ・クリアデスク・クリアスクリーン方針	・装置は、サポートユーティリティの不具合による、停電、その他の故障から保護している。 ・データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護している。 ・装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守している。 ・装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さないように管理している。 ・構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、 セキュリティを適用している。 ・記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを全て消去していること、若しくはセキュリティを保って上書きするなどの対策を検証している。 ・クラウドサービス利用者装置は、24 時間 365 日、有人により運用管理している。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

			・書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用している。
	Ⅳ．４．４．建物の情報セキュリティ対策	・オフィス、部屋及び施設のセキュリティ ・セキュリティを保つべき領域での作業 ・入退室記録 ・監視カメラ ・破壊対策ドア ・警備員 ・鍵管理 ・受渡場所 ・搬入と 搬出	・オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用している。 ・セキュリティを保つべき領域での作業に関する手順を設計し、適用している。 ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室の手順書と記録を作成し、適切な期間保存している。 ・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視している。また、監視カメラの映像をあらかじめ定められた期間保存している。 ・重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置している。 ・重要な物理的セキュリティ境界に警備員が常駐している。 ・サーバルームやラックの鍵管理を行っている。 ・荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、建物の構造や動線を考慮の上、十分な情報セキュリティ対策を講じたうえで管理している。 ・施設に搬入・搬出されるシステムコンポーネントに対して許可・未許可、モニタリング、及び管理を行い、それらについての記録を保管している。

３．アピールポイント

三谷産業株式会社アウトソーシングデータセンターは、「総務省：公共ＩＴにおけるアウトソーシングに関するガイドライン」「ＩＤＣイニシアティブ：ＩＤＣ活用ガイドライン（高品位規格）」の指針に準拠したデータセンター専用の建物・設備である。また、セキュリティ対策は、第三者による客観的な評価である情報セキュリティ格付けとして、中堅ＩＤＣ(Internet Data Center)ながら最高位（ＡＡＡis）を取得・維持している。強固なセキュリティレベルと合わせて、ファシリティについても優れた対策を講じている。さらに、ＩＴサービス継続対策についても、対策を講じている。なお、当該クラウドサービスは、日本国内の自社資源でのみ提供している。他組織である供給者のサービスを利用したクラウドサービスは提供していない。他国の資源、サービスの利用や他組織である供給者のサービスの利用に関するリスクがない。

ポイント	内容
【安心安全なクラウドサービス】（高い情報セキュリティを確保したクラウドサービスを提供しています）	クラウドサービス利用者の情報資産は、利用者ごとに仮想資源を割り当て明確に区分して管理している。このため、マルチテナント型のクラウドサービスでは得られない高い情報セキュリティを確保している。 **日本国内の自社資源でのみクラウドサービスを提供しており、他組織である供給者のサービスを利用したクラウドサービスは提供していない。** このため、他国の資源、サービスの利用や他組織である供給者のサービスの利用に起因するリスクがなく高い情報セキュリティを確保している。
【情報セキュリティ評価・認証】	**ＩＳＭＳ（ISO27001）認証に加え、第三者の客観的な評価として情報セキュリティ格付最高位ＡＡＡis（トリプルＡ）を取得・維持。**
【ＩＴサービス継続対策評価】	**「経済産業省：ＩＴサービス継続ガイドライン改訂版」をリファレンスとし、第三者による客観的な評価を実施。**
【ファシリティに関する評価】	**「日本データセンター協会：データセンターファシリティスタンダードVersion3.0」をリファレンスとし、第三者による客観的な評価を実施。**
【安全な立地】	ＩＤＣの立地は、東海、南海、東南海の地震の影響がなく災害の少ない地域性（石川県）と強固な地盤（Ｎ値 50 以上）に設置されており、海抜も高く(100m)水害は有り得ない。また、周囲に民家のない丘陵地にあり、爆発物等の危険施設もない。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org

第三者証明書
クラウドサービス提供情報セキュリティ対策

【専用建物・設備】	以下の指針に準拠したデータセンター専用の建物・設備。 「総務省：公共ＩＴにおけるアウトソーシングに関するガイドライン」 「ＩＤＣイニシアティブ：ＩＤＣ活用ガイドライン(高品位規格)」 **「ＦＩＳＣ：金融機関等コンピュータシステムの安全対策基準　(Ⅶ.設備基準　１　コンピュータセンター)　２０２４年３月（第１２版）」**
【大地震にも耐える免震構造】	サーバ棟は免震構造、管理棟は耐震構造とし、震度７の地震発生時でも継続してデータセンターの機能を維持。
【運用マネジメント】	ＩＳＭＳ（IS027001）認証に加え、情報セキュリティの格付け審査実施。さらに、設備の適合レベル維持、管理計画や運用要員育成計画は、情報セキュリティフォーラムにて「ＩＳＭＳ年間計画」に包含して経営陣に承認され、従業員及び関連する外部関係者に開示し、周知徹底。2020 年８月ＩＴＳＭＳ（IS020000-1）認証取得、サービス可用性と完全性を運用管理。
【万全のセキュリティ管理レベル】	６段階のセキュリティ区画（駐車場(レベル０)からサーバ室(レベル５)）の各レベルに応じて、ＩＣカード、暗証番号、金属探知機、生体認証、サークルゲート(共連れ防止)によりアクセス管理の実施。さらに、サーバラック鍵管理システムによりすべての鍵の持ち出しと返却を記録するとともに、作業に必要のない鍵の持ち出しを防止実施。複数台の監視カメラを設置し、屋外・屋内とも死角のないモニタリングと録画を実施。
【二重化、冗長化された強い電源】 (災害発生時および災害復旧期間における停電の影響を回避出来ます)	２系統受電（系統の異なる別々の変電所より受電)を行っており、変電所～受電設備は二重化（本線、予備線）、さらに受電設備からＵＰＳ入力の電源経路は系統毎に独立しており、ＵＰＳ～サーバ室ＰＤＵの電源経路は２経路以上設置。ＵＰＳは予備機により冗長化されており、保守点検時も停止することなく連続運転が可能。非常用発電装置はサーバ棟（免震）の屋上に設置し災害発生時の安全性を確保すると共に、７２時間以上の連続運転が可能な燃料を備蓄。 **同社グループ会社にて非常用発電装置の燃料（軽油）を取扱っており、自前で燃料の調達を行い安定した運用を継続することが可能。** 一連(本線受電～予備線受電切替～非常用発電切替)の停電テストと、停電発生時の要員行動教育、実地訓練を年２回以上実施。
【万全の雷対策】	全てのアースを積極的に接続する「統合接地方式」を採用し、落雷時の高電位差から発生する大電流による機器損傷を防止。

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org

第三者証明書
クラウドサービス提供情報セキュリティ対策

【万全の火災対策】	サーバ室には超高感度火災検知システムを設置、窒素系ガス（イナージェン）による消化設備を備えており、耐火構造による延焼防止対策を実施。
【安心を提供するデータ保管体制】	免震構造のデータ保管庫棟をサーバ棟と別の建物として保有しており、サーバとの同時被災を防ぎデータ媒体を安全に保管可能。
【信頼性の高いネットワーク接続】	通信回線を冗長化。又、同通信回線事業者の局設備をセンター内に設置しており同局設備までの物理回線もループ構成となっており経路も分かれている。さらに、災害やトラブル発生に備えて、基幹回線・基幹ＬＡＮ機器を完全二重化し、回線切断リスクを回避。二重化、冗長化された強い電源に接続。
【空調設備】	サーバ室毎にサーバ室と別区画の専用空調機室を備え、各室４台構成（Ｎ＋１）。ＩｏＴ温湿度センサー、ＡＩを活用し空調機の省エネ運転制御を行っている。停電時は非常用発電装置により運転が継続される。万が一、設備の入替が必要になった場合でも、無停止で作業が可能（追加設置スペース、予備配管、電源ケーブル設置）。全ての空調設備に、漏水センサーを装備。
【液浸冷却設備】	液浸冷却設備の専用区画に液浸冷却システムを備えている。高効率な冷却技術により、従来の空調設備に比べ消費電力の削減、高密度で発熱量が大きいサーバの冷却ができる。
【運用要員の確保】	当社グループ会社全社で、緊急事態発生時の全従業者・家族の安否確認体制が確保され、安否確認訓練を年４回実施。地震などの災害発生時や新型インフルエンザ、新型コロナウィルスに対して、当社グループ各社からのＩＴ要員確保を含めた事業継続計画を作成。
【緊急宿泊】	緊急時の簡易宿泊室（シャワー、ベット完備の個室）２室をセンター施設内に完備。その他宿泊先として、徒歩圏内（３分）の「石川ハイテク交流センター」を利用する事が可能。また、災害時に賃貸可能なオフィススペースとして、徒歩圏内に「いしかわクリエイトラボ」がある。

以上

●お問い合わせ先　**一般社団法人日本セキュリティ格付機構**　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org