

# 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

No.2021-JaSRO-502

令和3年10月14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
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」 ～利用者との接点と事業者間連携における実務のポイント～
調査日	2021年9月30日～2021年10月14日
本書交付日	2021年10月16日
利用期限	本書交付日から1年 (※2)
証明 ID コード	10000230115S2101

※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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

### 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 I S M S 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 設備基準（コンピュータセンター）平成 31 年 3 月（第 9 版改訂）」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 Version 2.3」の評価項目および IT サービスの継続対策に対するプロセス内容・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 I T S M S 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、新型コロナウイ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（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）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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

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、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管理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～利用者との接点と事業者間連携における実務のポイント～平成26年4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管理項目について管理策を講じている。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。

領域	目的	管理項目	実施状況
6. 情報セキュリティのための組織	6.1 内部組織	6.1.1 情報セキュリティの役割及び責任	I SMS 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。
		6.1.2 職務の分離	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。
	6.2 モバイル機器及びテレワーク	6.2.1 モバイル機器の方針	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。クラウド利用者に対して、利用上の運用規定の順守を依頼している。
	6.3 クラウド利用者とクラウド事業者の公平な取引を	6.3.1 クラウドサービスの情報セキュリティマネジメントに係わる提供条件の明確化	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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

	確保するための措置	6.3.2 利用者接点とサプライチェーンにおける情報提供・供給	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の順守状況を提示している。問合せに迅速に対応するためコールセンターを開設している。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。
8. 資産の管理	8.1 資産に対する責任	8.1.1 資産目録	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。
		8.1.2 資産の管理責任	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。
		8.1.5 クラウド利用者からの預託された情報の返却	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削除することとしている。
	8.2 情報分類	8.2.1 情報の分類	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。
		8.2.3 資産の取り扱い	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。
	9. アクセス制御	9.1 アクセス制御に対する業務上の要求事項	9.1.1 アクセス制御の方針
9.1.2 ネットワーク及びネットワークサービスへのアクセス			クラウドサービスに供するネットワークに対して、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。
9.2 利用アクセスの管理		9.2.3 特権的アクセス権の管理	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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

		9.2.4 利用者の秘密 認証情報の管理	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。
	9.4 システム 及びアプリケー ションのアクセ ス制御	9.4.1 情報へのアクセ ス制限	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。
		9.4.4 特権的なユー ティリティプログラ ムの使用	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。
	9.5 仮想化さ れたクラウド サービスのアクセ ス制御	9.5.1 仮想化資源の 分離の確実な実施	仮想資源を構成するソフトウェアの脆弱性を定期的に確認し、適切に管理しており、利用環境の分離が適切に実施されるための措置を講じている。
10. 暗号	10.1 暗号による 管理策	10.1.1 暗号による管 理策の利用方針	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。
		10.1.2 鍵管理	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。
12. 運用の セキュリティ	12.1 運用の手 順及び責任	12.1.1 操作手順書	利用者に対して、クラウドサービスの情報セキュリティ関連機能を含めた操作マニュアルを提供している。また、問合せに迅速に対応するためコールセンターを開設している。
		12.1.2 変更管理	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。
		12.1.3 容量・能力の 管理	提供しているクラウドサービスの資源に求められる容量・能力の監視・調整を実施している。月次で、資源状況を把握し管理している。
	12.2 マルウェア からの保護	12.2.1 マルウェアに 対する管理策	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。
	12.3 バックア ップ	12.3.1 情報のバック アップ	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。複数利用者に同一仮想環境を提供しているサービスでは、利用者にお

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

			いてバックアップが可能となっている。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。
	12.4 ログ取得及び監視	12.4.1 イベントログ取得	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。
		12.4.2 ログ情報の保護	ログ情報の記録の削除や改ざん、取得設定情報の変更は、管理者のみがアクセス可能としている。
		12.4.3 実務管理者及び運用担当者の作業ログ	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。
	12.5 運用ソフトウェアの管理	12.5.1 運用システムに関わるソフトウェアの導入	利用者が、クラウドサービス上にインストールするソフトウェアについて、マルウェアに感染していないかの確認も含め、利用規約等に規定している。
	12.6 技術的ぜい弱性管理	12.6.1 技術的ぜい弱性の管理	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。
	12.7 情報システムの監査に対する考慮事項	12.7.1 情報システムの監査に対する管理策	定期的（半年毎）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。
13. 通信のセキュリティ	13.1 ネットワークセキュリティ管理	13.1.4 仮想ネットワークにおいて重視すべき脆弱性	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。また、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。
	13.2 情報の転送	13.2.2 情報転送に関する合意	クラウドサービスの提供において外部とのデータ連携を必要とするサービスの提供は行っていない。
		13.2.4 秘密保持契約又は守秘義務契約	海外のサービスを利用したクラウドサービスの提供は行っていない。
15. 供給者関係	15.1 供給者関係における情	15.1.1 供給者関係のための情報セキュリティ方針	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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

	報セキュリティ	15.1.3 ICTサプライチェーン	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。
	15.2 供給者のサービス提供の管理	15.2.1 供給者のサービス提供の管理及びレビュー	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。
		15.2.2 供給者のサービス提供の変更にたいする管理	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。
16. 情報セキュリティインシデント管理	16.1 情報セキュリティインシデントの管理及びその改善	16.1.2 情報セキュリティ事象の報告	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。
		16.1.4 情報セキュリティ事象の評価及び決定	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。
		16.1.7 証拠の収集	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を目的として「システム利用監視ガイドライン」により記録の取扱いを規定している。
17. 事業継続マネジメントにおける情報セキュリティの側面	17.2 冗長性	17.2.1 情報処理施設の可用性	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。
18. 順守	18.1 法的及び契約上の要求事項の順守	18.1.1 適用法令及び契約上の要求事項の特定	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いる。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。
		18.1.2 知的財産権	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いる。また、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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

		18.1.3 記録の保護	日本国内の資源・サービスでのみ、クラウドサービスを提供している。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を目的として「システム利用監視ガイドライン」により記録の取扱いを規定している。また、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。
		18.1.4 プライバシー及び個人を特定できる情報(P I I)の保護	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いる。個人情報については、Pマーク認定を取得し個人情報保護法に則り管理している。
		18.1.5 暗号化機能に対する規制	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いる。日本国内の規制に従っている。
	18.2 情報セキュリティのレビュー	18.2.1 情報セキュリティの独立したレビュー	定期的（半年毎）に、情報セキュリティ監査を実施している。また、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。
		18.2.2 情報セキュリティのための方針群及び標準の順守	定期的（半年毎）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、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。
		18.2.3 技術的順守のレビュー	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。

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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

### 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 (AAAs) 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せん)	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。 <u>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。</u> 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】	<u>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AAAs (トリプルA) を取得・維持。</u>
【ITサービス継続対策評価】	<u>「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。</u>
【ファシリティに関する評価】	<u>「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 Version2.3」をリファレンスとし、第三者による客観的な評価を実施。</u>
【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、海拔も高く (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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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】	<p>以下の指針に準拠したデータセンター専用の建物・設備。</p> <p>「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)」  <u>「FISC：金融機関等コンピュータシステムの安全対策基準 設備基準（コンピュータセンター）平成31年3月（第9版改訂）」</u></p>
【大地震にも耐える免震構造】	<p>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。</p>
【運用マネージメント】	<p>ISMS（ISO27001）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（ISO20000-1）認証取得、サービス可用性と完全性を運用管理。</p>
【万全のセキュリティ管理レベル】	<p>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、作業に必要な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。</p>
【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)	<p>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。</p> <p><u>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。</u></p> <p>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。</p>
【万全の雷対策】	<p>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。</p>

●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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

# 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）による消火設備を備えており、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】	<u>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。</u>
【信頼性の高いネットワーク接続】	<u>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ます。</u> 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員・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、新型コロナウイルスに対して、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>

第三者証明書は、被調査組織等から入手した情報に依拠して形成した当機構の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。当機構は、第三者証明書に関するクレーム、訴訟その他の紛争、被調査組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、第三者証明書に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。