セキュリティについて

データセンターは日本国内に設置されています。場所の開示はセキュリティの面から行っておりません。

区分	要件詳細	概要説明
データセンターの組織・運用面	・第三者機関認定	SOC1,SOC2,ISO14001,ISO27001,ISO22301,ISO9001,PCI-DSSを取得済です。
	・運用規定	上述の各種ISO認証の要求に準拠したルールを策定しています。
	・品質、稼働状況の把握、評価	各種サービスについては、社内KPIとして運用目標値を定めています。Globalでの目標も設定しており、各国にて目標達成に向け取り組んでおります。また各種認証を取得するために外部監査を行い品質向上に取り組んでおります。
	・障害等の対応	設備障害に備え各種ドキュメントを整備しており、設備故障や自然災害などを想定した訓練を定期的に行っております。
	・可搬媒体管理	データセンター側で管理する可搬媒体についてはポリシーに則り管理されています。
	・各種媒体、機器等の廃棄	データセンター側で管理する機器の廃棄はポリシーに則り廃棄されています。
	・人的教育	新規入場時研修に加え、セキュリティ、事業継続、労働安全など様々な教育を定期的に行っています。
	・物理的アクセス	最小限のアクセス制限を設けて運用しており、各アクセスポイントはアクセスコントロールシステムで管理されています。また共連れ防止を目的に、受付横にフラッパーゲートを設けております。
データセンターの設備・環境面	・入退室管理	入退館・入退室アクセス管理において、指紋認証を含めた多要素認証による確認が実施されており、ログ保管されています。受付は24時間有人対応となり、警備員が常駐しております。
	・災害対策	様々な災害を想定した訓練を定期的に行っています。また地域のハザードマップを参考にして、津波、高潮、洪水などのリスクを定期的に評価を行い対策を施しています。
	・火災対策	VESDA、自動火災報知機、煙感知機、ガス消化システム、消火器などを備えています。
	・電源設備	冗長化電源を提供しており、有事に備えUPSと発電機を備えています。また、定期的に実負荷試験を行い健全性の維持に努めています。
システム面（FRONTIER21）	・アクセス制御、認証	データセンターの従事者はFRONTIER21にアクセスすることはできません。また、センターシステム（FRONTIER21）の作業に当たる従事者は安全なネットワークを通じてアクセスします。
	・外部からの不正アクセス対策	ファイアウォールで、外部からのネットワークの不正アクセス防止をしています。
	・通信の暗号化	通信は、すべてSSL/TLSにより暗号化され、HTTPSを使用して送信しているため、第三者によるデータの盗聴や改ざんを防止できます
	・災害対策	代替機材の準備・データのバックアップ等の対策を行っており、有事の際の影響を最小限に抑え、サービスの再開および提供が行えるよう計画を制定しています。
	・アクセス制御、認証（ユーザ利用領域）	契約単位で事業所IDを発行し、ユーザ固有のIDとパスワードの仕組みによりユーザ環境へのアクセスを可能としています。また、IP制限機能によりアクセス元を制限することができます。
	・外部からの不正アクセス対策（ユーザ利用領域）	ファイアウォールで、外部からのネットワークの不正アクセス防止をしています。また、IP制限機能によりアクセス元を制限することができます。
	・データの削除（ユーザ利用領域）	データの削除は、契約者の操作により可能となります。なお、サービスの契約解除後は、利用契約に基づいて一定期間後に契約者のデータの削除を行います。 この際、格納されているデータに触れることはありません。