達人Cubeセンターでの安全管理措置

「達人シリーズ」各製品の安全管理措置機能は次の通りとなります。
なお、達人Cubeセンターは、日本国内にあるデータセンター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。

利用場所	区分	要件詳細	概要説明	備考
達人Cubeセンター（データセンター）	**共通**	・第三者機関認定	ISO27001〔ISMS認証〕（情報セキュリティ）、Pマーク(個人情報保護)、ISO22301(事業継続)の認証を取得しています。	
		・運用規定	運営にあたっては、資格取得しているISO27001〔ISMS認証〕（情報セキュリティ）、Pマーク(個人情報保護)、ISO22301(事業継続)等に準拠したルールを策定しています。	
	組織・運用面	・品質、稼働状況の把握、評価	運用規定に基づいて、情報セキュリティや個人情報保護、機器類の稼働状態、システムの性能、リソース使用状況等を運用品質目標を定め、24時間365日の運用監視および定期的報告等により監視しています。 また、運用状況の評価は、定期的な内部監査や第三者機関審査等で行っており、必要に応じて適切に見直しを行っています。	障害が発生時や定期保守等でのセンターの稼働に影響がある場合は、ホームページおよび達人Cubeのお知らせで開示いたします。
		・障害等の対応	災害やシステム障害、セキュリティ事故等の障害の発生等の有事の際の影響を最小限に抑え、サービスの再開及び提供が行えるよう、障害の検知・原因特定・対処・サービス提供再開等の対応プランやリカバリプランを策定しています。 また定期的にプランの訓練を実施しています。	
		・可搬媒体管理	可搬媒体及びノートPC、携帯機器等は、データセンターが所有する特殊な機器を除き、一切の使用を禁止しています。 また、データセンタ外からの持ち込みについては厳重にチェックされる運用となっております。	
		・各種媒体、機器等の廃棄	各種媒体や機器等の廃棄は、ライフサイクルに応じて設置、修理、破棄を決められた手順に従い実施しています。特にお客様データを保管していたストレージデバイスについては、「クリティカル」として厳格な基準を設け、故障やライフサイクルの終了等で外部に持ち出す際、セキュアゾーン内でワイプもしくは消磁処理行った後に物理に破壊します。 また、これらの作業における実施の証跡について、レポートを確認しております。	
		・人的教育	運営に携わる人員に対して、運用規定に則り、導入教育、および定期的（年1回以上）の教育を実施しています。	
		・物理的アクセス	運用規定により、作業の正当性、アクセスの範囲を厳格に審査し、必要最小限のアクセス許可を発行します。また、作業実施内容、証跡について監査しています。	
	設備・環境面	・入退室管理	データセンターは権限を持つ担当者が申請し、承認された場合、指定された期間、許可されたマシンルームのみ入室する権限を与えられます。 データセンター内での担当者の行動はすべて監視され、定期的にチェックされます。	
		・災害対策	環境および地理的評価を実施し、洪水、異常気象、地震活動などの環境リスクを軽減するためにデータセンターの場所を慎重に選択しています。	
		・火災対策	煙検出センサーを使用した、自動火災検出システムおよび鎮火システムが設置されています。	
		・電源設備	電力は、完全に冗長化され、電力障害時に運用を維持するための電力供給を可能とするバックアップ電源がデータセンターに備わっています。	
	システム面	・アクセス制御、認証（センターシステム）	作業の役割を分離しており、データセンターの従事者はシステム（インフラ以上のレイヤー）にアクセスすることはできません。 センターシステム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。また、作業に対しては、必要な都度システム管理者から作業の承諾を取得し、作業内容に応じた最小限の権限で実施する運用になっています。 また、システムへのアクセスログを記録しており、定期的なバックアップによる保管と監査を行っています。	
		・外部からの不正アクセス対策（センターシステム）	アプリケーションファイヤーウォール（WAF）、ファイアウォール/IDS/IPS等で、外部からのネットワークの不正アクセスの検知とアクセス防止をしています。	
		・アクセス制御、認証（ユーザ利用領域）	センターでは、契約単位でユーザ利用領域（[事業者データベース]及び[個人情報収集データベース]）が設定されており、ユーザ固有のコードを元にした復号化の仕組みによりユーザ環境からのアクセスのみ可能としています。 また、この領域のアクセス・操作ログは契約者側の領域内で記録されており、契約者のみが確認できるようになっています。 なお、データセンターの従事者、およびセンターシステムの従事者は（複合化された状態の）ユーザ利用領域にアクセスすることはできません。	
		・外部からの不正アクセス対策（ユーザ利用領域）	外部からの不正アクセス対策により、攻撃者がユーザ利用領域にアクセスできる可能性を低減させています。 また、ユーザ利用領域は暗号化と復号化が施されているため、不正にアクセスした場合でも、内部のデータ自体を解析することは不可能となっています。	
		・データの保全（ユーザ利用領域）	日次でデータセンターのバックアップを行っています。 なお、万が一データの復旧が必要になる場合は、ユーザ利用領域単位でバックアップしたポイントでの復旧となります。	
		・データの削除（ユーザ利用領域）	データの削除は、ユーザ環境からの契約者の操作により可能となります。 なお、各サービスの契約解除後は、システム運営者であるNTTデータが、利用契約に基づいて一定期間後に契約者のデータ保存領域自体の削除を行います。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。	
		・災害対策	回線多重化、遠隔地バックアップの取得、代替機材の準備等の対策を行っており、有事の際の影響を最小限に抑え、サービスの再開及び提供が行えるよう計画を制定しています。	