

### データに対するアクセス遮断と統制

お客様の大切なデータを保護するためのセキュリティ政策

お客様がデータ復旧を依頼するにあたって考慮しなければならない事項は、データ復旧技術力、費用と時間などがまず思い浮かぶと思います。確かに重要な事ですが同じくらい重要な事がその復旧会社のセキュリティシステムです。

復旧会社は様々なお客様の情報を扱うとてもデリケートな業務です。そのセキュリティシステムは大企業のデータセキュリティ水準あるいはそれ以上のセキュリティ水準で復旧作業が行わなければなりません。

徹底したセキュリティシステム構築は作業プロセス全般にわたった明確な手続きと統制が最優先です。当社のセキュリティ政策はお客様が安心して任せることができる会社という経営理念から、明確なプロセスの確立と統制で完成されています。

### [データセキュリティについて](#)

#### 物理的な区間分離・出入統制

外来のお客様と社内スタッフの出入を物理的に分離して、1次的なセキュリティを適用しています。

指紋認識出入システムを導入し、スタッフは自分のIDを付与され出入りをチェックし出入記録は自動的にセキュリティサーバーに保存されます。社内のエリアを統制区域、保護区域、一般区域で業務空間を分配して、物理的に接近ができないような構造を設けています。

#### 復旧作業室の多重セキュリティ

復旧作業室も指紋認証によって2段階のゲートを設け管理されています。特に復旧室の設備は外部ネットワークとの接近を防ぐために物理的にネットワークが遮断されています。お客様本人が直接訪問して、認証を通じてデータ確認する場合以外は外からの接近が不可能です。

復旧したデータはファイル暗号化システム(EFS)で暗号化されているので認証なしではファイルの読み込みはできません。

復旧作業室のセキュリティは外部からの侵入者に対する空間的な遮断、ネットワークの物理的遮断、接近権限の統制など多重の保護装置によって維持されています。

### [データに対する遮断と統制](#)

#### 全ての物理障害まで自社内対応

弊社は全ての物理障害の症状にも自社内対応をしております。

自社内で対応可能という事は高度なセキュリティ対策も可能です。受付から納品まで全プロセスが徹底した自社のセキュリティ政策内で行われており、安全で明確な管理が出来ております。

DATA OKは、日本国内最高レベルの復旧技術、復旧設備、エンジニアはもちろんセキュリティにも万全な体制を備え、PC関連・復旧関連企業の数社から外注業務も受けています。

### [物理障害の例](#)