

株式会社 DATA OK

代表取締役社長 青山 真

情報資産は、お客様にとって重要な財産であると私たちは考えております。復旧データの取扱いに関する規制は顧客の復旧データを安全に管理する事とデータ流出を防止するためのものです。

この規制は顧客の復旧データの取り扱いと管理に携わる担当者を対象にする指針書であり、該当の事項の厳守を目的とします。

顧客の復旧データ取扱い及び管理

復旧データの取扱い及び管理組織

データ復旧受付及び相談員

データ復旧受付及び相談員はデータ復旧の受付前後に発生する顧客との連絡、データの管理、確認、配送のために顧客の電話番号や住所などの個人情報に対する閲覧権限を持つ。復旧データの取り扱いはできない。

データ復旧作業エンジニア

データ復旧作業エンジニアは顧客からデータ復旧を依頼された場合データ復旧作業のために、顧客のデータの記録媒体に対するアクセス権限を持つ。

セキュリティ管理者

当社情報システムセキュリティの責任者は依頼者の情報保護を徹底するためにセキュリティ管理計画及び実施/改訂、セキュリティ教育実施、定期的セキュリティ点検実施、セキュリティ事故対応、システム導入の企画及び運営、データシステムセキュリティ検討を行う。

最高管理者

最高管理者は顧客セキュリティ政策の樹立、顧客情報セキュリティ業務の運営に関しての最高意思決定者である。最高管理者は組織全体の情報保護政策目標、目的及び優先順位などを決め、顧客情報保護政策の正常な運用ができるように意思決定を行う。

データ保護組織/管理

組織に係わる一般指針は組織及び職務管理指針に準ずる。

復旧データ管理指針

基本指針

定期的なセキュリティ点検を通じて復旧データ管理政策及びセキュリティ指針の厳守状況を確認し適切な復旧データ管理対策を講ずる。

ID、復旧データ管理パスワード

基本原則

復旧データ管理に対する ID とパスワード管理は次の原則で実施する。

パスワードは顧客別に発給する。

パスワードは他人に公知することができない。

パスワードのセキュリティ責任は該当の ID の使用者にある。

ID 及びパスワードが発給されるすべてのシステムは Default パスワード及び ID と同じパスワードを使うことはできない。

パスワード設定及び変更

パスワードは 4 字以上で設定する。(文字と数字混合)

変更時は 3 字以上変更し、直前のパスワードから予測できないように設定する。

ID 管理

顧客データ確認のために発給されたIDは顧客データ復旧と同時に発給する。
データ保存期間の満了した IDは迅速に削除する。

復旧データセキュリティ指針

アクセス権限

データ復旧サービス受付及び相談員

受付、相談員は業務遂行のため顧客個人情報(名前、電話番号、住所、電子メール等復旧申込書を通じて作成される部分)の閲覧はできるが、顧客の来社によってやむを得ず復旧相談員が顧客にデータを確認させる場合、必ずセキュリティ管理者を通じて顧客の IDとパスワードを受け取り、確認を手伝うが、担当者が顧客のデータを閲覧することはできない。

データ復旧作業エンジニア

復旧作業完了後復旧データの確認のために復旧エンジニアは顧客データのシグネチャーを通じて確認するようにする。

復旧されたデータの最終確認権限は依頼顧客にあるが、やむを得ず復旧エンジニアが確認をしなければならない場合には顧客の承認を受けた後、セキュリティ管理者を通じて 2次承認を受けなければならない。

セキュリティ管理者

セキュリティ管理者は顧客データの閲覧はできない。顧客データの ID及びパスワードの発給権限のみを持つ。

最高管理者

顧客データにはアクセスできない。プロセス別アクセス権限の承認に対する権限を持つ。

システム管理者の責任と権限

システム管理者が変更される場合、後任者はパスワードを変更する。

天災などの非常事態発生時に備えて適切な措置とプロセス化、緊急時マニュアルの作成を行う。

システム使用者に対するセキュリティ教育を実施する。

データセキュリティ指針

データは顧客固有のIDとパスワードを付与する。

使用者 ID、使用時間などアクセス記録を管理する。

アクセス権限管理プログラムは最高管理者のみ使用できる。

データ納品後、復旧データは1週間保管するが、1週間後にはアメリカ国防省のデータ完全削除基準によるデータ削除を行う。

復旧データセキュリティ点検

データの安全な保護のために、定期的にセキュリティ点検を実施する。

点検時期

毎月1回定期点検することを原則とする。

必要によっては非定期的にセキュリティ点検を実施することができる。

セキュリティ担当者やシステム運営スタッフが変わる場合には、セキュリティチェックリストのすべての項目を点検し確実に引き継ぐようにする。

復旧データセキュリティチェックリスト

ID管理

-顧客 ID発行、削除など管理

-パスワード管理

サーバー管理

-サーバーのアクセス制限

-運営システムのバグの調査

-セキュリティパッチの適用事項

PCセキュリティ

- ワクチンプログラムのインストール、使用現況
- 不法ソフトウェア使用現況
- FD(Floppy Disk),CDROM,外付ハードディスクなどの管理現況
- データセキュリティ
- −データ取扱者管理現況
- データアクセス制限

方針の評価と更新

復旧データセキュリティの調査とともに、ポリシーの実効性を定期的に評価し、改善が必要と認められた場合には、変更内容および実施時期の決定を行い、セキュリティレベルが高くかつ遵守可能な方針に更新する。

復旧データ管理責任者

- 名前：中山 博
- 部署：データ復旧事業部
- 職位：復旧チーム長
- E-mail：director@dataok.jp

お問い合わせ

株式会社DATA OK ([データ復旧研究センター](#))
〒101-0021 東京都千代田区外神田4-7-5石川興産ビル3F
T E L 03-6273-9099, F A X 03-6273-9898
E-mail: data@dataok.jp

復旧データ管理ポリシー 更新日：2008.04.25