KDDI 株式会社

ＫＤＤＩホスティングサービスセキュリティポリシーについて

お客様がご利用されておりますホスティング環境を、あらゆる脅威から守るため、必要な情報セキュリティの確保に対する弊社の基本方針をご説明致します。

＜セキュリティの保たれた領域＞

下表に記しますセキュリティの保たれた国内データセンター内に設置しており、物理的なアクセス、妨害を防止しております。

防火設備	火災報知システム
	延焼防止システム (排煙設備･防火区画設備)
	ガス消化システム
電源設備	自家発電設備
	冗長構成によるUPS設備 (無停電電源装置)
空調設備	冗長構成のとれた空調システム
入退出管理	ICカード利用による入退室管理システム
	事前申請･登録･記録
ラック施錠	サーバ、ネットワーク機器を収容する全てのラックを施錠管理
有人監視体制	24時間×365日の監視体制
	監視カメラによる監視

＜アクセス制御＞

- ポートへのアクセスはセキュリティを保つため、提供しているサービス以外の不必要なポートについては全て遮断しております。
- 不正･大量アクセス等を検知した場合、設備とサービス品質を守るため接続元のアクセス制限を実施します。ただし、お客様の運用上支障が発生する場合は、申告により実施したアクセス制限や制限の一部を取り止めることを承ります。

＜第三者によるアクセスのセキュリティ＞

- 悪意ある第三者から保護するため、サーバ内でサービスを稼動･監視するプロセス（デーモン）は、サービス提供用プロセスを除き、不必要なプロセスは起動不可にしております。
- お客さまのコンテンツの安全性を高めるため、お客さまのホームディレクトリ環境下のみでCGI等の動作が可能となるように制限しております。
- 許可されていない利用者のアクセスを防止するため、メールについては SMTP Auth を導入しています。
- 大量のスパムメールに対しメールサービスを安定運用するため KDDI 独自のポリシーに基づき、スパマーからのメール着信を拒否しております。

＜運用管理＞

- 十分な処理能力および記憶容量の利用を可能にするため、容量･能力の需要を監視し、将来必要とされる容量･能力を予測しております。

- セキュリティ事件・事故に対して、迅速・効果的かつ整然とした対処を確実に行うため、必要なログ情報は全て収集し、一定容量を保管しております。
- 安全性確保のため、24 時間×365 日の体制でサーバの状態監視を行っております。
- 最新のセキュリティ情報の収集を行い、脆弱性につながるようなものは適切にパッチやバージョンアップ等による対応に努めております。

この他にも様々な施策を行っておりますが、詳細は KDDI セキュリティポリシー上公開出来ません。あしからずご了承ください。