情報セキュリティへの取り組み

株式会社ワイズ

当社の情報セキュリティへの取り組みについてのご紹介します。

「技術的対策」

社内システムに「ぜい弱性診断」を行い、最新かつ有用な情報を入手し、安全なシステムであり続けるため、対策を取っております。

「人的対策」

社員に対しては情報を取り扱うための教育を行い、定期的にテストを実施するなどの仕組みを取り入れております。

「物理的対策」

システム設置場所は安全な条件を満たす場所を選定し、事故や自然災害等の脅威からシステムや情報を守る対策を取っております。

「組織的対策」

各部門間の連携を取ることにより、アクシデントへの対応に備えた組織体制を整備しております。また、予防対策も取っております。

情報セキュリティ基本方針

当社は、情報社会の脅威からお客様情報を守るために管理された安全なサービスを提供するための方針を作成しております。

今日のインターネット社会は、犯罪、過失、事故、自然災害等の脅威に対する対策を急務としております。当社ではお客様の情報を守るために安定したサービスを提供すべく方針を整えております。

1. 適切な技術的・組織的各種管理策を講じ、情報資産に対する不正侵入、改ざん、情報漏えい、破壊などによるサービス提供への影響が発生しないよう努めてまいります。
2. 万一、何らかの問題が発生した場合、迅速に原因究明を行い、その被害を最小限にとどめるよう努めてまいります。
3. 社員に対して、情報セキュリティの確保に関する必要な教育・訓練を行ない、啓発を図ってまいります。
4. 社員に対して、情報セキュリティおよびサービス管理における方針・目標を理解させると共に、情報セキュリティおよびサービス管理の継続的改善に努めてまいります。
5. 上記活動を継続的に実施、改善し、情報セキュリティ管理体制およびサービス管理体制の確立を図ってまいります。

以　上、

情報セキュリティ対策

当社は以下のとおり、セキュリティ対策を講じており、セキュリティ事故の未然防止に努めています。

情報セキュリティ	-	・当社の情報セキュリティについては定期的な管理運営体制を役員会にて報告・管理することにより常に改善しております。 ・個人情報保護規程（JIS Q 15001）を取得し、情報保護の教育・管理を周知しています。
物理的セキュリティ	入退館管理	・サーバルームおよび本社の入退館および入退室を分けたセキュリティカードにて管理・記録しています。
人的セキュリティ	情報セキュリティ教育	・情報取り扱いのセキュリティ教育を定期的に実施し、教育しています。 ・新入社員教育、専門職研修などの教育を実施しています。
	誓約書	・入社時および退職時は全社員を対象として、「誓約書」を交わしています。
ネットワーク管理	ネットワークセキュリティ	・次世代型のファイア・ウォールを導入し、アプリケーション毎の不正通信を遮断しています。 ・ウイルスゲートウェイを導入し、ウイルスの侵入・外部への攻撃を防止しています。 ・リモートからのアクセス制限およびファイアウォールを導入することにより、「コンピュータウイルス」等からの脅威からWebサーバを保護しています。
クライアント管理	社外持ち出しPC管理	・社外持ち出しPCは端末毎に利用管理を行い、セキュリティソフトにより漏洩を防止しています。
	業務PC管理	・WSUS （ウィンドウズサーバーアップデートサービス）の導入により、セキュリティパッチの最新化を維持しています。 ・ウイルス対策ソフトの集中監視システムを導入しており、ウイルス検出・感染時の初動対応が速やかに実施できる環境を整備しています。
インシデント管理	セキュリティホットライン	・セキュリティホットラインを整備しています。 （24時間365日受付可能　※留守番転送含む）
	セキュリティ事故管理	・セキュリティ事故は全てレベル分けを行い、情報セキュリティ室にて一元管理され、イントラにて情報開示を行うことにより、同一原因によるセキュリティ事故の低減を図っています。