Social —Data Security—

Concept & Policy

顧客情報や個人情報、業務関連情報など、事業推進にあたり多くの情報を取り扱う当社グループは、2007年に「KWEグループ情報セキュリティ基本方針」を定め、運用してまいりました。2020年に、昨今の情勢を踏まえてISO27001に準拠した「KWE Group IT Security Policy」を制定し、管理体制の強化を図っています。

KWEグループ情報セキュリティ基本方針

KWEグループは、情報資産の機密性、完全性、可用性を維持しつつ、業務を円滑に維持遂行し、あらゆるステークホルダーからの信頼を高めるよう、情報セキュリティ水準の向上を図ります。

1. 情報セキュリティ水準を向上するため、組織・体制を構築します。
2. 情報セキュリティに関する法令、社内規程を遵守します。
3. 情報資産のリスクを継続的に評価し、情報セキュリティ対策を見直します。
4. 情報資産を、不正アクセスおよびコンピュータウィルス等の脅威から保護します。
5. 障害や災害発生時における情報資産の被害を最小限に抑え、復旧対策を実施します。

KWE Group IT Security Policy

概略

- 事業展開をしている国や地域において適切なITセキュリティポリシーを設定するとともに、確実に実現できる計画およびガバナンスを確立する
- 計画に基づいて適切な管理体制を構築する
- セキュリティ管理の適切性、妥当性、有効性を定期的にレビューする
- セキュリティコントロールの適合性、適切性、有効性を改善する

企業価値向上に向けて

マテリアリティ「Data Security」に注力する当社グループは、加速するビジネス環境の変化に伴いより巧妙かつ高度化するITセキュリティへの脅威に対応するべく、ITセキュリティの強化に継続的に取り組んでいます。

2020年にKWE Group IT Security Policyを制定後、2021年からはセキュリティレベルの測定やセキュリティ管理体制の構築、訓練・教育を本格化したほか、2022年は、インフラの標準化や定期的なアセスメントに注力しました。

また、「ゼロトラストセキュリティプラットフォーム」の構築を継続するとともに、クラウドの利活用においてもセキュリティを担保できるサービスを導入しているほか、従業員や取引先などユーザーへの教育も継続的に実施しています。

さらに、グループ全体のセキュリティ向上を重要テーマに掲げ、データセンターやサーバー・ネットワーク環境のセキュリティ・アセスメントを強化しています。

今後もITセキュリティの強化に向けて迅速かつ適切な措置を講じ、ステークホルダーから信頼いただけるビジネスパートナーであり続けることで将来の成長阻害要因を軽減し、当社グループの持続的な成長と企業価値向上につなげていきます。

サイバーセキュリティ対策のさらなる強化

情報セキュリティの視点から、ハード・ソフトの両面で「入口対策」「出口対策」「脆弱性対策」を実施しています。また、サーバーの運用状況に加え、セキュリティ面での異常の発生有無を24時間365日監視する体制を構築、運用し、インシデントの早期発見と是正を実現していきます。

2025年4～5月に当社システムで発生したサーバー障害の一連の経緯や内容を踏まえ、再発防止策のポイントを以下のように定めました。

1．セキュリティガバナンスの強化
2．新たな脅威への対策強化
3．ネットワーク集約化による被害拡大の防止
4．災耐性の強化による事業継続性の改善

従業員教育の実施

当社グループの全従業員を対象とした情報セキュリティに関するeラーニングを、2024年度は4回実施しました。また、メールを経由したサイバー攻撃も増加傾向にあるほか、生成AIによるフェイクニュース等のリスクが高まっていることを踏まえ、フィッシングメール対策訓練を2回実施しました。

従業員教育の実施状況等（2024年度）

時期	内容
2024年4～6月	2024 代表的な脅威について
2024年7～9月	ソーシャルエンジニアリング、多要素認証
2024年10～12月	フィッシングアラートボタンの使用方法
2025年1～3月	2024 Kevin Mitnickによるセキュリティ意識向上トレーニング

定期的なセキュリティ・アセスメントの実施

当社グループのデータセキュリティについて第三者によるセキュリティ・アセスメントを定期的に実施し、その結果を基に、情報セキュリティの専門スタッフによる施策の立案・実施を行っています。

その他のリスク低減策

サイバーセキュリティリスクの低減を図るため、データセンターの分散、クラウド化やネットワーク回線の二重化等により、可用性の確保に努めています。また、グループ各社の外部向けサーバーに対して脆弱性診断を実施し、機密情報漏洩リスクの軽減を図っています。上記のほか、より高度化・多頻度化するサイバー攻撃に備え、AIおよびビッグデータを活用したマルウェア、スパムメール対策機能を導入し、検出された脅威に対して自動化されたプロセスによる迅速な対応を実現していきます。さらに、Microsoft365のチャットボットに「不審なメールの見分け方」を誘導するシナリオを追加しています。従業員が不審なメールを受信した際、チャットボットの活用によりタイムリーに対処方法を判断することで、セキュリティ事故の未然防止に努めています。