マテリアリティ

Data Security データセキュリティの強化

目標	2023年度の進捗	2024年度以降の取組み／施策案等
■ ITセキュリティ・アーキテクチャの強化 ■ ITセキュリティ意識の向上	■ グループ全従業員を対象としたeラーニングを4回実施 ■ フィッシングメール対策訓練を5回実施 ■ サイバーセキュリティ対策において従業員教育のさらなる拡充、定期的なセキュリティ・アセスメント等を実施 ■ グループ共通のITプラットフォームの確立とグループ全体のセキュリティ向上に向けて立ち上げたUnusプロジェクトのもと、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 ■ 従来のマルウェア、スパムメール対策に加え、不審メール対策も強化	■ 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、その結果に基くセキュリティ施策を専門スタッフが立案・実施 ■ ITセキュリティの強化に向けて迅速かつ適切な措置を継続 ■ 生成AIの活用による競争力や業務効率の向上と同時に、リスク対応策も強化の体制を構築

Diversity and Equal Opportunity
ダイバーシティと機会均等の推進

目標	2023年度の進捗	2024年度以降の取組み／施策案等
■ 管理層への昇進における機会均等の促進 ■ マイノリティグループからの採用の推進 ■ 人権・機会均等に関する従業員教育の推進	■ 従業員エンゲージメントサーベイを開始 ■ グループ全体の女性管理職比率:34.0% ■ 人権、機会均等に関するeラーニングを全世界の従業員に実施 ■ テレワーク制度と育児短時間勤務制度の内容を拡充	■ KWEグループダイバーシティと機会均等に関する基本方針の浸透 ■ 各地域の状況に応じた施策の推進

Social Impacts in the Supply Chain
責任ある調達の推進

目標	2023年度の進捗	2024年度以降の取組み／施策案等
■ サプライチェーンにおいて倫理的、社会的、環境的責任を果たす	■ 「サプライヤー安全衛生統一基準」の策定を推進 ■ 国連グローバル・コンパクトに近鉄グループとして参画 ■ パートナーシップ構築宣言へ参画 ■ 人権デューデリジェンス部会を発足	■ 「人権方針」の策定を推進 ■ 人権デューデリジェンス関連項目を含むチェックリストに基づき、サプライヤー調査を推進

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

Progress

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。

そして2023年3月には、グループ共通のITプラットフォームの確立に向けてUnusプロジェクトを立ち上げました。グループ全体のセキュリティ向上を重要テーマに掲げる本プロジェクトのもと、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ることで、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とともに、当社グループの持続的な成長につなげていきます。

サイバーセキュリティ対策

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。

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、2023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が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5回実施しました。

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。

上記に加え、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2023年10月には、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ました。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。

従業員教育の実施状況等(2023年度～)

時期	内容
2023年6～7月	フィッシングメール対策訓練を実施
2023年7～8月	情報セキュリティに関するeラーニングを実施
2023年8月	フィッシングメール対策訓練を実施
2023年9～10月	フィッシングメール対策訓練を実施
2023年10月	情報セキュリティに関するeラーニングを実施
2023年12月	フィッシングメール対策訓練を実施
	情報セキュリティに関するeラーニングを実施
2024年2月	フィッシングメール対策訓練を実施
2024年3月	情報セキュリティに関するeラーニングを実施