マテリアリティ

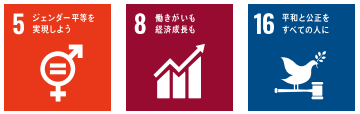
Data Security データセキュリティの強化

目標	2022年度の進捗	2023年度の取組み／今後の施策案等
■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	■サイバーセキュリティ対策の運用を継続 ■定期的なセキュリティ・アセスメントを立案・実施 ■データセンター/サーバー/ネットワーク等のリスク低減策を継続 ■従業員教育の実施（なりすましメール対応訓練、情報セキュリティに関する学習を年にそれぞれ3回実施）	■サイバーセキュリティ対策の運用を継続 ■定期的なセキュリティ・アセスメントを立案・実施 ■データセンター/サーバー/ネットワーク等のリスク低減策を継続 ■従業員教育の実施（なりすましメール対応訓練、情報セキュリティに関する学習を年にそれぞれ4回実施）

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

目標	2022年度の進捗	2023年度の取組み／今後の施策案等
■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	■グループ全体女性管理職比率:34.3% ■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	■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制定 ■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	2022年度の進捗	2023年度の取組み／今後の施策案等
■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	■調達におけるアセスメントを実施し、重要項目を特定（安全衛生、労働、ベンダー管理、環境コンプライアンス） ■安全衛生に関するチェックリストを作成（7つの分野、37項目）	■安全衛生に関するチェックリストをサプライヤーへ周知し、調査を実施 ■サプライヤー管理に関する制度の確立

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、お客様や取引先をはじめとするステークホルダーの皆様から信頼いただけるビジネスパートナーであり続けるために、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。

足元では事業環境の急激な変化が続いており、企業を取り巻くITセキュリティへの脅威も巧妙かつ高度化していることから、引き続き迅速かつ適切な措置を講じていきます。

具体的には、「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。

今後もITセキュリティの強化に取り組むことで、当社グループとステークホルダーのサステナビリティ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2022年度は3回実施しました。また、メールを経由したフィッシングメールが増加傾向にあることを踏まえ、フィッシングメール対策訓練を3回実施しました。

従業員教育の実施状況等（2022年度～）

時期	内容
2022年6～7月	フィッシングメール対策訓練を実施　対象:全拠点（10,765名） 情報セキュリティに関するeラーニングを実施
2022年11月～12月	フィッシングメール対策訓練を実施　対象:全拠点（11,994名） 情報セキュリティに関するeラーニングを実施
2023年2～3月	フィッシングメール対策訓練を実施　対象:全拠点（12,363名） 情報セキュリティに関するeラーニングを実施

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。

上記に加えて、より高度化、多頻度化するサイバー攻撃に備えて、AIおよび、ビック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って、迅速な対応を実現していきます。