マテリアリティ

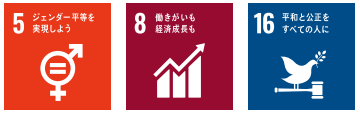
Data Security データセキュリティの強化

目標	2021年度の進捗	2022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	■ 実現すべきセキュリティレベルを設定し、その整備を進めると同時に、有事発生に即応できる管理体制構築に着手 ■ 全従業員を対象としたITセキュリティ教育を定期的に実施（受講率：87%）	■ サイバーセキュリティ対策の運用を継続 ■ 従業員教育の実施を継続 ■ 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

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

目標	2021年度の進捗	2022年度の取組み／今後の施策案等
■ 女性の管理職登用の促進 ■ 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：32% ■ 各国におけるハラスメント防止、ダイバーシティ&インクルージョン研修のニーズ・実施状況を調査 ■ 調査結果から次年度以降のグローバルでの研修プログラムを検討	■ ダイバーシティに関する社内方針・規程類を制定 ■ 女性の管理職登用の促進を継続 ■ マイノリティグループからの採用の推進を継続 ■ 人権・機会均等に関する従業員教育の推進を継続

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



目標	2021年度の進捗	2022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	■ KWE供給者行動規範を国内外のサプライヤーに周知。（署名率：82%）	■ KWE供給者行動規範の周知徹底を継続 ■ 重要項目（安全衛生、労働、ベンダー管理、環境コンプライアンス）に関するガイドラインを作成 ■ 供給者への監査・調査を実施

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

VOICE

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セキュリティを強化していきます

当社グループは、多種多様な働き方の実現と同時に、ITセキュリティの強化にこれまでも取り組んできました。昨今のビジネス環境の急激な変化、さらには巧妙かつ高度化するセキュリティへの脅威に対しては、迅速かつ適切な措置を講じていく必要があります。そのため、「ゼロトラストセキュリティプラットフォーム」の構築を進めるとともに、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、ユーザーへの教育も継続的に実施しています。お客様や取引先から信頼いただけるビジネスパートナーとして評価いただけるよう、今後も、ITセキュリティの強化に取り組んでいきます。

常務執行役員
コーポレート・インフォメーション
テクノロジー部長(CIO)
齊藤　眞

進捗&計画

フェーズⅠ―2020年～―

■KWE Group IT Security Policyの制定

フェーズⅡ―2021年～―

■セキュリティレベルの測定 ■セキュリティ管理体制の構築開始 ■訓練・教育の実施開始

フェーズⅢ―2022年～―

■インフラの標準化
■定期的なアセスメントの実施開始

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」「ウイルス侵入対策」を実施しています。

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、運用します。

従業員教育の実施

当社グループ従業員全従業員を対象としたフィッシングメール対策訓練を実施しているほか、その結果を踏まえたeラーニング等でのフォローアップを、四半期に一度実施しています。

定期的なセキュリティ・アセスメントの実施

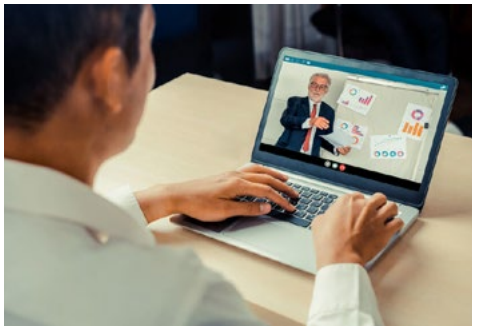
当社グループのデータセキュリティについて第三者によるセキュリティ・アセスメントを定期的に実施し、その結果を基に、情報セキュリティの専門スタッフによる施策の立案・実施を行っています。

その他のリスク低減策

システム障害のリスク低減を図るため、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、システムの安定運用に努めています。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。

従業員教育の実施状況等（2021年度～）

時期	内容
2021年9月	フィッシングメール対策訓練を実施 対象：欧州を除く全拠点（9,614名） 訓練内容：メール内にリンク先を記載、リンク先ページでID/パスワードの入力を誘導するフィッシングメールを送信
2021年12月	訓練結果を踏まえたeラーニングを実施 受講率：87%（全拠点）
2022年5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おける目標と達成状況

フォローアップeラーニング受講率

目標： 100%

2021年度受講率： 87%