Governance

情報セキュリティ

社会課題に対する考え方

企業経営を脅かすサイバー攻撃の手口は、多様化・悪質化しています。ターゲットも規模や業種を問わず拡大し、誰もが狙われる時代となりました。企業や組織においては情報セキュリティを重要な経営課題として捉え、一層、高度な取り組みを行なうことが求められています。アンリツグループでは、情報を適切に取り扱い、保護するため、国内・海外での情報共有、セキュリティレベルの均一化を進め、強固な管理体制を構築していくことが重要であると考えています。

方針

アンリツグループは事業活動を行う上で、お客さま、株主・投資家、取引先さま、社員など全てのステークホルダーの情報を適切に保護することが社会的責務であり、また、その情報が重要な資産であると認識しています。この観点で情報管理基本方針を制定し、セキュリティの維持・向上への取り組みを継続的に実施しています。

WEB *情報管理基本方針*

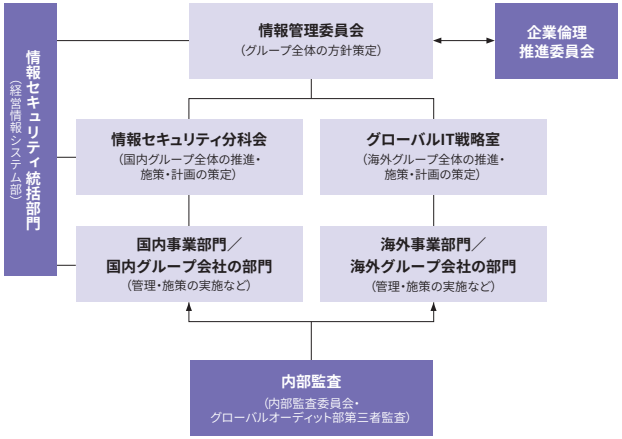
体制

アンリツは、各事業部門およびグループ会社の担当執行役員からなる情報管理委員会を組織して、グループ全体の情報管理に関する施策や投資などの方針を策定しています。

国内においては、情報管理委員会の下部組織として国内グループ会社の代表者からなる情報セキュリティ分科会を設け、ポリシーの制定、施策の実行、社員教育、インシデント発生時の対策と情報共有などを行っています。

海外グループ会社においては、地域統括会社のIT責任者がメンバーとなっているグローバルIT 戦略室を設け、セキュリティを含むITの統制強化に注力しています。

情報セキュリティ管理体制図



ISO27001認証取得状況

・日本：経営情報システム部／エンジニアリング本部共通技術部CADチーム
・EMEA：Anritsu A/S　サービス・アシュアランス・ビジネス関連部門

目標

▶ 侵入を前提としたセキュリティ対策の推進

サイバー攻撃の手口はますます多様化・巧妙化し、侵入を100%防ぐのは事実上不可能といわれています。侵入を防ぐ対策に加え、攻撃を受けた場合でも迅速な対応を行うことで被害を最小限に食い止めることが重要です。今後は事前と事後の対策をトータルに考えた取り組みを進めていきます。

▶ グローバルで強固かつ均一なセキュリティシステムの構築

グローバルに事業を展開するアンリツグループでは、世界中のオフィスをネットワークで接続し、情報の共有化を進めています。2021年度にM&Aを行った(株)高砂製作所も含めて、グローバルに統合されたセキュリティシステムの構築を推進していきます。

取り組み／活動実績

ランサムウェア対策の強化

昨今、ランサムウェアの被害が急増しています。製造業においては、一部の企業が被害を受けるとサプライチェーン全体に影響を及ぼすような事故が発生しています。ランサムウェアは、侵入を防止する一般的なセキュリティ対策だけではなく、感染を迅速に検知し復旧を行うことで業務への影響を最小限に抑えることも重要です。そのためにはセキュリティインシデントもBCPのリスクとして捉え、備えておくことが必要です。2021年度はこの対策として、システムの確実なバックアップと復旧時間の短縮化を目的に新たにバックアップサイトを構築しました。システムがランサムウェアに感染し障害が発生した場合でも、バックアップサイトで待機系システムを立ち上げることで業務への影響を最小限に抑えることができます。復旧時間もこれまでの1週間から1日に大幅短縮しました。

社員教育とフィッシングメール訓練の実施

毎年、eラーニングで全社員に情報セキュリティ教育を実施しています。2021年度は特にランサムウェアの脅威や電子メールの取り扱いについて教育を行いました。また、フィッシングメール訓練も以前より回数を増やして2～3カ月間隔で実施し、電子メールから侵入するサイバー攻撃に対する意識向上に努めています。

バックアップサイトの構築