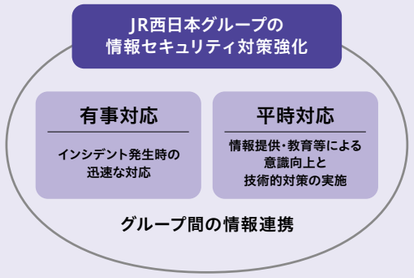
情報セキュリティ

情報セキュリティに関するJR西日本グループの考え方

JR西日本グループは、情報資産をさまざまな脅威から守るために「JR西日本グループ情報セキュリティポリシー」を定めてこれを遵守し、グループ会社間の情報共有と相互連携により、グループ全体で情報セキュリティ対策を継続的に行っていくことを宣言しています。

近年、サイバー攻撃によるリスク・被害は増大し、かつ高頻度になっており、政府も国家戦略としてサイバーセキュリティの強化を要請しています。

JR西日本グループもテレワーク拡大やDX進展に伴う脆弱性の拡大と、攻撃の巧妙化、脅威の増大に対し、デジタル戦略4つの柱の内の1つとして情報セキュリティに取り組んでいます。



JR西日本グループのセキュリティ体制

最高情報セキュリティ責任者（CISO）を委員長とした情報セキュリティ委員会を設置し、その下部組織として「重要インフラ部会」、「JR西日本グループCSIRT」を運営しています。

その他、外部機関との連携も活用しつつ、グループ全体のセキュリティレベル向上に取り組んでいます。

情報セキュリティ委員会の設置

JR西日本グループ内のセキュリティに関する取り組み実績の報告に加え、社内外の動向をもとにJR西日本グループのセキュリティレベル向上のための取り組み方針を決定しています。

重要インフラ部会の運営

鉄道運行に関わるシステムをはじめとした制御系のシステムや、ICOCA等の社会インフラを支える重要なシステムに対し、リスクの洗い出しとその対策について、特に重点的に実施しています。

JR西日本グループCSIRTの運営

セキュリティインシデントの未然防止や、発生時の被害拡大防止を目的とした組織「JR西日本グループCSIRT※1（JRW-CSIRT）」を構築し、情報連携・教育等による意識の醸成及びインシデント発生時の迅速な対応に取り組んでいます。

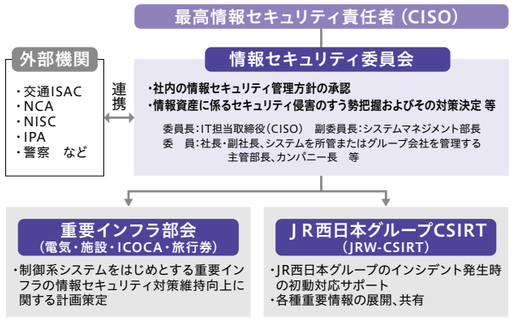
※1 CSIRT（シーサート）：Computer Security Incident Response Teamの略。
コンピュータセキュリティに係るインシデントに対処するための組織の総称。

外部機関との連携

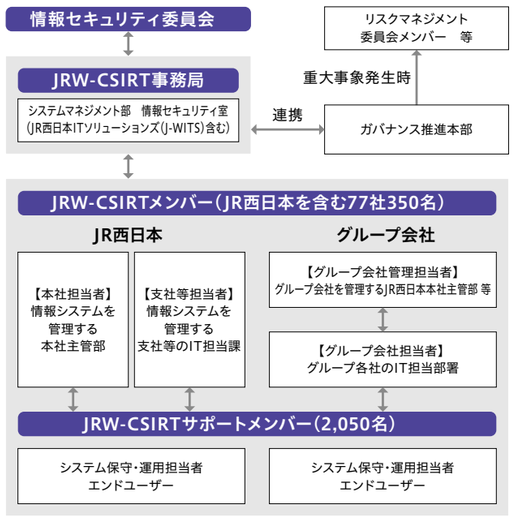
当社は交通ISAC※2に加盟しており、平時から他社と情報セキュリティに関する情報交換を積極的に行っています。また、NCA※3（日本シーサート協議会）が主催するセキュリティに関するワーキング等にも積極的に参加しています。

※2 交通ISAC：交通・運輸分野全体の集団防御力の向上に資する活動を推進する団体
※3 NCA：日本で活動するCSIRT 間の情報共有および連携を図る団体

■JR西日本グループのセキュリティ体制



■JRW-CSIRTの体制



リスクマネジメント、情報セキュリティの取り組みに関する情報は以下のページをご参照ください
リスクマネジメントの取り組み（情報セキュリティ含む）
▸ https://www.westjr.co.jp/company/action/risk_management/
JR西日本グループ情報セキュリティポリシー
▸ https://www.westjr.co.jp/guide/security.html

社員のリテラシー向上に向けた取り組み

JR西日本グループでは、社員のリテラシー向上に向けた取り組みとして、全社員（約44,000名）に向けた標的型攻撃メール訓練やセキュリティ教育を実施するとともに、以下のように特定の対象者に合わせた教育も実施しています。

経営層向け

グループ会社も含めた経営層（約200名）を対象にサイバー攻撃の脅威と対策、および経営層がセキュリティ対策において果たすべき役割について理解することを目的とした研修を実施しています。

情報セキュリティに関わる担当者向け

JR西日本グループ内のJRW-CSIRTメンバーや情報システム主管者（約2,900名）などを対象に、情報セキュリティ施策を主導する人財の育成を目的とした研修を実施しています。平常時のセキュリティ対策の必要性を伝える内容に加え、JRW-CSIRTメンバー（約350名）を対象にセキュリティインシデント発生時の対応訓練も実施しています。

重要インフラに関わる担当者、責任者向け

重要インフラ事業者を対象としたNISC（内閣サイバーセキュリティセンター）主催のインシデント対応訓練に参加しています。

高度専門人財を目指す社員向け

IPA（独立行政法人情報処理推進機構）主催の「中核人材育成プログラム」へ1年間社員を派遣し、セキュリティ人財の育成を行っています。また、外部研修への参加や資格取得を支援する制度を設け、特にセキュリティに関する学習を慫慂した結果、グループ内の情報処理安全確保支援士試験合格者数は約50名となりました。

■デジタル戦略を推進する人財育成と研修一覧

高度人財	実施内容	IPAへの人財派遣、外部研修への参加支援制度等
	レベル	・情報処理安全確保支援士相当の知識がある
箇所推進リーダー	実施内容	情報セキュリティトップ研修（対象：経営層・部門長） 情報セキュリティリーダ研修（対象：箇所CSIRTメンバー等） 情報セキュリティサポータ研修（対象：箇所CSIRTサポートメンバー） CSIRT業務説明会（対象：箇所CSIRTメンバー） インシデント対応ワークショップ（対象：箇所CSIRTメンバー）
	レベル	・箇所において、情報セキュリティ施策の主導や、所管システムのセキュリティ対策が実施できる
全社員	実施内容	全社員向けセキュリティ研修、標的型攻撃メール訓練
	レベル	・個人情報・機密情報を適切に取り扱いできる

安全なシステム開発を行うための取り組み

当社およびグループ会社では、セキュリティバイデザインの考え方に基づき、システム開発の構想段階でセキュリティ対策について検討・承認する取り組みを実施しています。特にセキュリティ対策が重要であると考えられるお客様の個人情報を取り扱うシステムや社外ネットワークとの接続点を持つシステムなどを対象としており、ベースラインアプローチ、リスクベースアプローチの双方の観点から確認を行うことで必要なセキュリティ対策を講じる取り組みを実施しています。

PDCAサイクルの定着

必ず守るべき具体的なセキュリティ基準を定めたガイドラインを整備し、技術動向や過去のインシデントを踏まえて改善しています。これに基づき、毎年、当社およびグループ各社で2,880システムに対し、合計118,646項目の自主点検を実施し、継続的にセキュリティ対策を強化しています。