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。

ポストコロナへの挑戦を加速する当社グループにおいて、「攻め」のデジタル戦略と「守り」の情報セキュリティは両輪です。グループ全体で適切な情報セキュリティを確保し続けることが、安全なサービスの提供と、お客様の安心・信頼につながります。翌年度には当社事業エリアにおいて2025大阪・関西万博が開催されます。変化する環境に対応し、グループの仲間、社外のパートナー様と連携し、対策をアップデートし続けていきます。

推進責任者 技術理事 デジタルソリューション本部システムマネジメント部長(CISO)
甲斐 康弘(情報処理安全確保支援士(登録番号第025068号))

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など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。

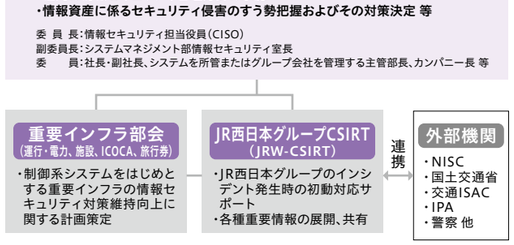
● JR西日本グループCSIRTの運営

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・教育などによる意識の醸成およ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。各社に対応窓口となるJRW-CSIRTメンバー(80社約400名)、各箇所にJRW-CSIRTサポートメンバー(約2,100名)を配置し、体制の拡充を図っています。

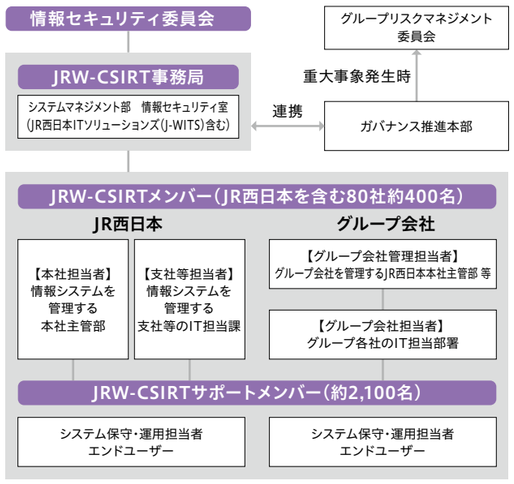
● 外部機関との連携

交通ISAC※2への加盟、日本シーサート協議会(NCA)※3が主催するワーキングへの積極的な参加、内閣サイバーセキュリティセンター(NISC)や警察機関との情報連携などを通してセキュリティの強化に努めています。

■ 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、全社員に向けたセキュリティ訓練・教育を実施するとともに、特定の対象者に合わせた教育も実施しています。

● 全社員向け

グループ会社を含むJRW-CSIRT加盟会社の全社員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しています。また、2015年度よりIT部門の活動結果および今後の活動方針を年次報告書として毎年発行し、IT部門の具体的な業務内容を知ってもらうための取り組みを行っています。

■ IT部門で発行する「IT Report」

● 箇所推進リーダ向け

経営層・部門長

グループ会社を含むJRW-CSIRT加盟会社の経営層(約210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層

JRW-CSIRT加盟会社の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。また、インシデント発生時の初動対応と各組織内の教育・啓発活動を担うCSIRTサポートメンバー(約2,100名)を対象に、情報セキュリティの基礎知識やCSIRT活動の目的・内容を理解するための研修を実施しています。

重要インフラに関わる担当者、責任者

重要インフラ事業者を対象としたNISC主催のサイバー演習(分野横断的演習)に参加し、障害対応体制の検証などを行っています。

● 高度専門人財を目指す社員向け

独立行政法人情報処理推進機構(IPA)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、JR西日本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	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)
	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

■ 情報セキュリティ研修開催の様子

鉄道会社にセキュリティ人材として貢献したい

2023年7月から1年間、IPA産業サイバーセキュリティセンター(ICSCoE)の中核人材育成プログラムに第7期生として参加しました。当社は鉄道を中心としたサービスを展開しており、その影響範囲の大きさからサイバー攻撃の理解と対策が急務と感じ、自らこのプログラムへの参加を希望しました。ICSCoEでは実際に手を動かして制御システムの仕組みとサイバーセキュリティに関する技術や知識について学びました。加えて、企業が攻撃を受けた際のビジネス継続のための考え方や復旧方法についても学びました。今後は情報処理安全確保支援士としてサイバー攻撃から事業を守るため、技術とマネジメントの両面で貢献していきたいと考えています。

デジタルソリューション本部
システムマネジメント部
情報セキュリティ室
西澤 優里

※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。
※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 日本シーサート協議会(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

情報セキュリティ

安全なシステム開発を行うための取り組み

JR西日本グループでは、システム・サービスをセキュアに開発・運用するために、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。

● 重要なシステムの審議活動の実施

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、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。

■ システム開発における投資決定までのフロー

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「JR西日本グループ情報セキュリティガイドライン」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、JR西日本グループ全体の3,302システムに対し、合計144,753項目のセキュリティ自主点検活動を実施し、継続的にセキュリティ対策を強化しています。

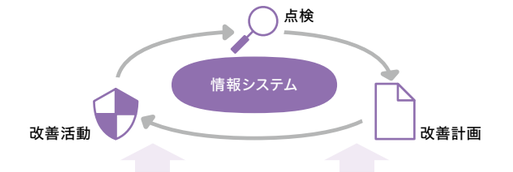
● セキュリティ自主点検活動のフォローの実施

重要な点検項目についてはJRW-CSIRT事務局がすべてのJRW-CSIRT加盟会社を対象に直接点検を実施しています。各箇所と状況確認のコミュニケーションを行い支援することで、リスクの早期改善を図っています。

● ガイドラインを満たすITシェアードサービスの提供

各社における改善活動を支援するため、ガイドラインを満たすシェアードサービスや共通システム・ツールを提供することで各組織における自主点検やツール導入などの負荷を軽減しています。

■ 情報システムのセキュリティ対策の継続的な改善の取り組み



ITシェアードサービス（ガイドラインを満たす共通サービス）	自主点検フォロー活動の取り組み
インターネットセキュリティサービス・メールサービス・公開Webサイト基盤サービス 等	JRW-CSIRT事務局の直接点検によるリスクの早期改善

システムマネジメント部・J-WITSはITシェアードサービスの提供・自主点検フォロー活動の取り組みで改善活動を支援

JR西日本グループにおけるデータ利活用の取り組み

「JR西日本グループデータ利活用ポリシー」に基づきデータを効率的かつ安全に共有、活用するためにグループ全体でデータガバナンス体制を構築し、データ取引の「利活用促進」と「安全性確保」の両立を図っています。その実現に向けて年3回の研修のほか、以下の取り組みを実施しています。

● 「利活用促進」に向けた取り組み

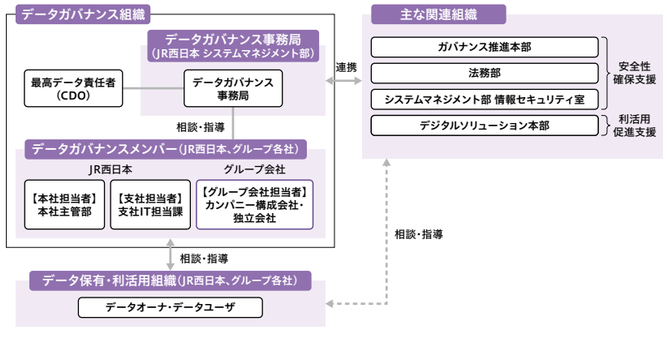
月1回の他社事例紹介などの啓発活動、当社グループが保有するデータをまとめた「データカタログ」の作成による見える化を実施しています。

● 「安全性確保」に向けた取り組み

「データ取引申請書」「チェックリスト」「契約書ひな形」を提供することで、誰もが適切にリスクを管理し抑え込むことを可能にしています。

また、相談窓口を設置し、データ利活用に係る相談を受け付けています。

■ データガバナンス体制



情報セキュリティに関するKPIの設定および優秀グループ会社の表彰

● 情報セキュリティに関するKPIの設定

JRW-CSIRT加盟会社を対象に情報セキュリティに関するKPI（重要業績評価指標）を設定し、セキュリティ対策の取組状況を定量的に評価しています。

具体的には、「ガイドラインに基づくシステム点検」「標的型攻撃メール訓練」「セキュリティ研修の受講者数」などの項目に対してグループ共通のKPIを設定することで各部門やグループ会社と共通の目標を共有し、一貫したセキュリティ対策の推進を行っています。

■ 情報セキュリティに関する主な目標指数（KPI）

- ●ガイドラインに基づくシステム点検
  対策項目の適合率　100%
- ●標的型攻撃メール訓練
  対象者全体に占めるメール開封後の未報告者の割合　1%未満
- ●セキュリティ研修の受講者数
  情報セキュリティリーダ認定者の割合　10%以上

● 優秀グループ会社の表彰

上記の情報セキュリティに関するKPIなどに基づき、「システム点検において対策項目の適合率100%」「標的型攻撃メール訓練において不審メールを模した訓練メールの開封者ゼロ」「社員数に対して情報セキュリティリーダ認定者数の割合が50%以上」など、特に顕著な成績を達成しているグループ会社を優秀会社として表彰を行っています。これによりグループ各社における情報セキュリティ活動のフィーチャリングを進め、情報セキュリティの取り組みに対するモチベーション向上に努めています。

■ 優秀グループ会社表彰の様子

2025大阪・関西万博に向けたセキュリティ対策の取り組み

2025年4月から開催される大阪・関西万博に向けて、激化するサイバー攻撃に対応するため、以下の取り組みを実施しています。

● インシデント発生時のサイバーレジリエンス向上の取り組み

JRW-CSIRT加盟会社に対して、各社で保有する重要システムの停止や機密情報の漏洩を想定した机上訓練を実施します。訓練では、システム担当者がインシデント対応の一連のプロセスを理解するだけでなく、経営者がインシデント発生時の経営判断を認識することを目的とし、経営トップも参加する形で実施します。

また、JR西日本グループや他社において早急に対処すべきインシデントやリスク情報があった場合、速やかにインシデント説明会を実施し、事象の理解を深め、迅速な対応につなげています。

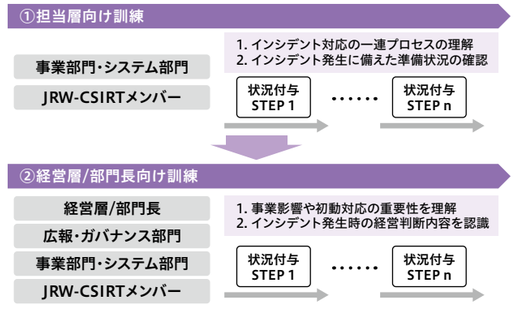
● アクティブサイバーディフェンスの取り組み

脅威インテリジェンス情報とアタックサーフェス管理を組み合わせて外部公開しているIT資産に対して攻撃者視点での分析を行い、最新のサイバー脅威を継続的に把握しています。また、発見した脅威に対して能動的に対策を行うことで予防的サイバーセキュリティを強化しています。

● 政府機関などとの連携強化

NISCによる大阪・関西万博に向けた官民連携を強化するためのパートナーシップの取り組み（JISP）に参加するなど、外部機関との連携を強化し、平時における情報共有、有事における迅速な対応を図っています。

■ インシデント対応訓練の取り組み



■ アクティブサイバーディフェンスの取り組み