JR東日本におけるデータ利活用の取組みと情報セキュリティ対策

Data utilization and information security measures in JR East

東日本旅客鉄道株式会社　総合企画本部　システム企画部
アナリシス・セキュリティセンター所長
西村　佳久

1. はじめに

JR東日本グループでは、2012年10月に策定した「グループ経営構想V～限りなき前進～」のもと、「変わらぬ使命」と「無限の可能性の追求」の経営の柱を推し進めるとともに、「地域に生きる。世界に伸びる。」という理念の実現に向け取り組んでいる。

その中でシステム企画部では、情報システム部門として「中期情報システム戦略」を策定し、以下の5点を柱に据え、経営構想の実現に向けて取り組んでいる。（図1）

中期情報システム戦略　5本柱

(1)品質の高い情報システムの提供
(2)システム経費の最適化
(3)情報セキュリティレベルの更なる向上と
　ITガバナンスの強化
(4)ICTを活用した業務革新
(5)システム部門の人材育成と組織のあり方

図1　当社の中期情報システム戦略の5本柱

本稿では、主に「(3) 情報セキュリティレベルの更なる向上とITガバナンスの強化」及び「(4) ICTを活用した業務革新」の2つの柱の推進と、それを通じた人材育成を進めている、システム企画部アナリシス・セキュリティセンター（ASC）内の「アナリシスソリューショングループ」及び「セキュリティマネジメントグループ」の取り組み内容について述べる。

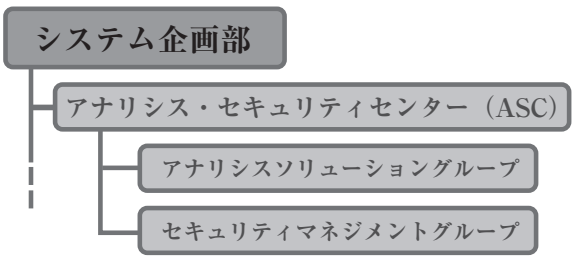

図2　アナリシス・セキュリティセンター

2. ICTを活用した業務革新

2.1　アナリシスソリューショングループの取り組み

昨今社会では、センサ技術やネットワーク技術の発展から、消費者の動向や設備の動作状態をはじめ、様々なデータを膨大に取得・保存できるようになった。また、それらの保有データを分析することにより、これまで見えなかったことへの気付きから新たな取り組みを始めることができるようになった。

当社においても、図3の例に示すように設備のメンテナンスデータや営業情報など多様なデータを保有しており、従来から各系統で分析し、業務改善、コストダウン等に取り組んできたが、組織全体でのデータ利活用にまでは至っておらず、次のような課題があった。

- 分析できていないデータがある
  取得はしているものの分析に至っていないデータがあり、活用が不十分
- データ分析ノウハウが継続しない
  必要に応じてデータ分析を行っているので、ノウハウが組織として未蓄積
- 分析能力のレベル差
  各部門で個別にデータ分析を行うため、データ分析能力にレベル差がある

アナリシスソリューショングループは、メンテナンスデータをはじめとして当社で取得・蓄積を行っているデータのほか、社外も含めた様々なデータを用いて新たな付加価値を産み出すチームとして、メンテナンス業務の改善やコストダウン、業務効率化などの「業務革新（効率性・生産性向上）」分野を中心に、社内各部門横断的に課題を解決する取り組みを行っている。

図3　保有データの例

2.2　データ利活用案件

アナリシスソリューショングループにおいて、現在取り組んでいるデータ利活用案件の一部について紹介する。

(1) 発電業務支援

当社は、自営の火力・水力発電所を有しており、自営発電所からの電気は自営送電網を通じて列車運行等に使用されるほか、電力会社と連系し電力会社の送電網に供給される。(図4)

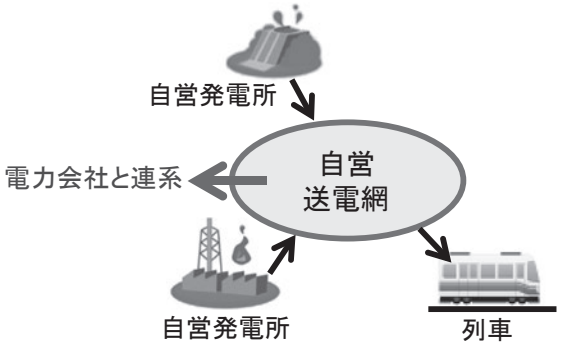

図4　当社自営電力の流れ

この際、列車運行等による電力使用量を正確に予測し、使用実績との差を小さくすることで、電力会社との連系に係るインバランスを低減することができる。

電力使用量予測は従来、指令員の手作業で行っていたが、今回、「過去実績」、「気温」、「曜日」等のデータを用いた重回帰分析モデルを作成したところ、高精度(2014年度の予測と実績では、R^2(※)の値が0.99以上)かつ短時間で予測を実現可能であることがわかった。(図5)

今後は、当該モデルをシステムに組み込み実運用に繋げていくとともに、従来実施してきた前日時点での翌日分の使用量予測だけではなく、当日の各種情報を用いたより高精度な予測の実現を目指している。(図6)

※ R^2:決定係数。数値が1に近い程相関関係が高いことを示す。

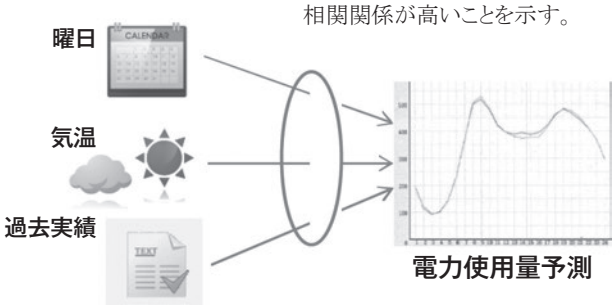

図5　電力使用量予測

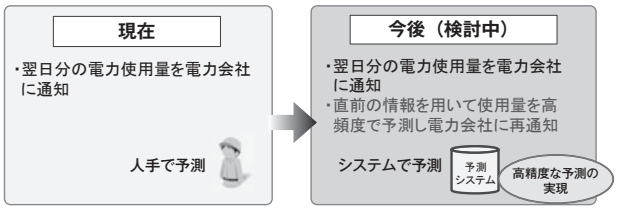

図6　電力使用量予測業務の現在と今後

(2) ホームドアメンテナンス改善

山手線などの駅に導入されているホームドアは、開閉動作時の電流値等の各種センサデータを常時記録している。これらのデータを分析することで、装置の稼働状態や構成部品の劣化状態の傾向を把握し、メンテナンス周期の適正化や故障の予兆検出を目指している。(図7)

図7　ホームドアセンサデータの分析

これまで、温度及び経過日数とドア駆動モータの動作電流値(ドアの負荷)変化の相関分析を行い、一部メンテナンス項目の周期延伸を実現した。さらに今後は、異常時の動作状態を試験環境にて模擬し、その時のモータの動作電流データを収集して正常時との差異を比較検証することにより、故障に至る以前の異常検出の実現を目指している。(図8)

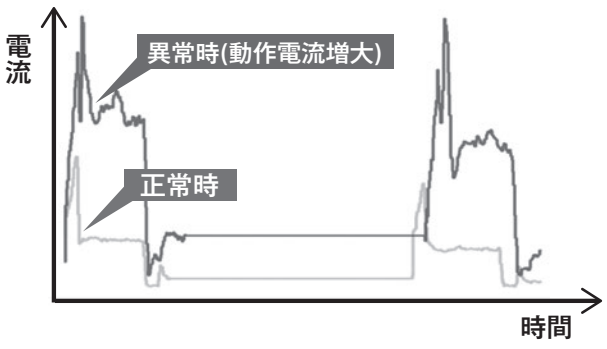

図8　電流データを用いた設備状態監視(イメージ)

(3) CBM システム用プラットフォームの検討

当社では、「スマートメンテナンス構想」を掲げ、設備メンテナンス業務の革新を目指しており、その一つとしてTBM（Time Based Maintenance）からCBM（Condition Based Maintenance）への転換を進めている。

その実現のためには、設備の動作状態を常時モニタリングして分析するシステム（CBMシステム）の導入が必要となる。CBMシステムは、大容量のモニタリングデータを扱うこととなるため、今後の各種設備に対するCBMシステムの導入によるデータ量増大を想定し、その要求を満たすプラットフォームを構築することとした。（図9）

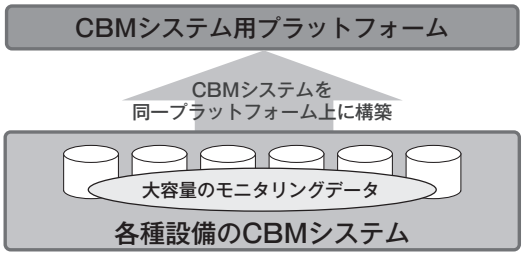

図9　CBMシステム用プラットフォームの構築

各種CBMシステムを同一プラットフォーム上に構築することにより、セキュリティの一元的な管理が可能となるほか、複数のシステム間でのデータ連携を容易にすることで、より効率的なデータ利活用が可能となる。（表1）

表1　プラットフォーム構築のメリット

項目	メリット
セキュリティ	◎プラットフォーム上で一元管理が可能
データ利活用	◎同一プラットフォーム上にて他のCBMシステムとのデータ連携が容易に可能 ◎輸送総合システムや設備管理システムなど、既存の他システムとのデータ連携が容易に可能

3. 情報セキュリティレベルの更なる向上

3.1　セキュリティマネジメントグループの取り組み

昨今、サイバー攻撃は増加の一途をたどっており、その手口も巧妙化してきている。今後のIoT社会の進展により、ネットワークにつながる対象の増加（図10）に伴い、セキュリティの脅威も増大していくことが予想される。

アメリカでは、これまで予想していなかったハンドルの遠隔操作や運転パネルの不正表示といった自動車へのハッキング事件が起き、急速にIoTのセキュリティへの関心が高まっている。

当社が担っている鉄道事業は重要な社会インフラであり、これまでその制御系システムは外部と隔離することでセキュリティを確保してきた。しかし、IoTを活用した保守やサービス提供などの外部ネットワークとの接続も出てきている。鉄道の運行にかかわる制御系システムにセキュリティインシデントが生じることで、重大な支障が生じないよう、OA機器等の情報系のシステムのみならず、運行等に係る制御系のシステムに対するセキュリティ対策も必要となってきている。

図10　IoT社会の進展

JR東日本グループのセキュリティの方針策定や、システムに対するセキュリティ対策実施、インシデント対応の窓口となるのが、アナリシス・セキュリティセンターのセキュリティマネジメントグループである。

3.2　取り組み内容

セキュリティマネジメントグループにおける主な取り組み内容を紹介する。

(1) 情報セキュリティ基本方針の制定

JR東日本グループでは、2009年12月に発生したJR東日本ホームページ改ざんを契機に、グループを挙げて情報セキュリティ対策に取り組んでいる。グループ各社の全社員が情報セキュリティの確保に対する共通認識を持つこととグループ全体のセキュリティレベル向上を目的に、「JR東日本グループ情報セキュリティ基本方針」を2014年10月に制定した。（図11）

この基本方針では、情報セキュリティ確保にあたっての基本的な取り組み姿勢を定め、グループ各社はこれに基づき社内規程等のルール整備を行っていくものとしている。

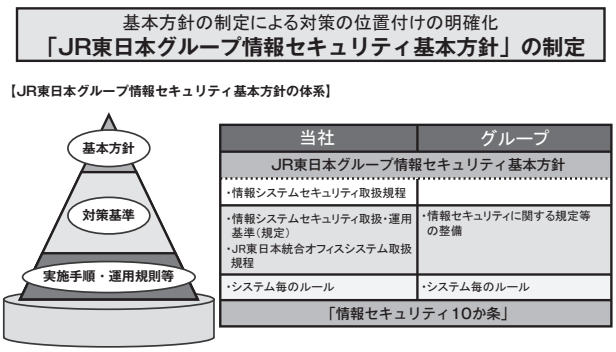

図11　情報セキュリティ基本方針

(2) JEIS セキュリティ対策室との連携

JR東日本のセキュリティ対策を進めるうえで、JEIS（グループ会社であるJR東日本情報システム）の役割は欠かせないものとなっている。

昨今、サイバー攻撃による脅威が拡大して、JR東日本グループ各社のセキュリティ事件・事故の防止、発生時の迅速な対応の必要性が高まる中、グループのセキュリティに関するリスクを低減していくため、専門的な組織として、JEIS内に「セキュリティ対策室」を2015年10月に設立した。

JR東日本のSOC（セキュリティオペレーションセンター）として、セキュリティ事件・事故をいち早く知得するため、様々な情報を確認及び分析し、プロアクティブ（先を見越した）な対応を行っているほか、セキュリティ事件・事故が発生した場合は、いかに影響範囲を特定して絞り込み、迅速に収束させるかという観点で、24時間運用のJEIS中央指令室と連携し、休日・夜間も緊急対応を行っている。また、地方機関でウイルス感染の事象が発生した場合には、JEISの各支店が直接赴くなどの対応を実施している。

(3) CSIRT 構築に向けた取組み

昨年、経済産業省が策定したサイバーセキュリティ経営ガイドラインには、サイバーインシデントに対して対応する機関として、CSIRT（Computer Security Incident Response Team）の整備が重要10項目の一つとして掲げられている。

それを踏まえ、当社においてもCSIRTの構築を進めている。異常時のインシデント対応支援に加え、平常時における情報セキュリティに関する方針策定、教育、情報収集、NISC（内閣サイバーセキュリティセンター）や警視庁といった外部との情報連携などについても、セキュリティマネジメントグループが事務局となり活動・連携を実施している。

(4) セキュリティ向上対策

ＯＡ機器などの情報系システムについては、ファイヤーウォールの設置やウイルスソフトの導入といった基本的な対策に加え、入口、出口、内部、端末といった各パートにおける対策をおこなってきた（図12）ところであるが、継続的に最新の脅威に備えたセキュリティ向上ソリューションの導入検討も進めている。

一方で、列車の運行等に関わる制御系のシステムについて、これまでは外部との接点のないクローズドネットワークで構築されていたが、ネットワークが外部との接点を持ち始めているケースや、昨今、諸外国で見られる制御系システムにおけるサイバーインシデントの発生事例など、環境が大きく変化してきている（表2）ことから、その点を踏まえた対策を進めている。

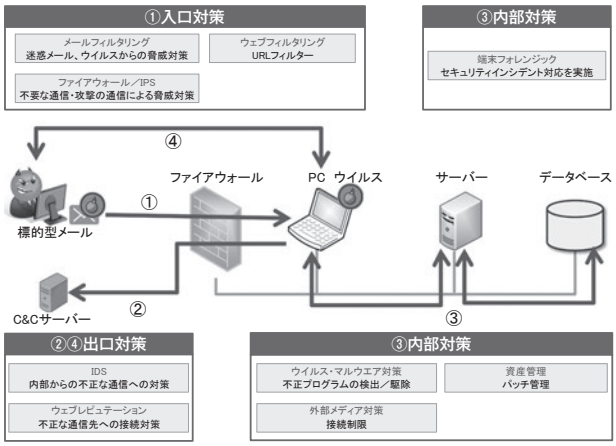

図12　情報系システムの脅威に備えたセキュリティ対策
（対策内容は一例）

表2　制御系システムの「情報システム化」の進展

過去	項 目	現在
クローズド環境 物理的に閉鎖的	環境	オープン環境へ変化 （外部ネットワーク接続・USB等の利用）
独自OS・アプリケーション 独自プロトコル	利用技術	汎用OS・アプリケーション 標準プロトコル
ほぼ無し	インシデント事例	増加傾向 （ウイルス感染、ハッキング等） ※海外だけでなく国内でも発生

「脅威は制御系システムにも波及する状況が到来」

(5) 内閣府が進めている「SIP」に対する協力

SIP（戦略的イノベーション創造プログラム）とは、社会的に不可欠で日本の経済・産業競争力にとって重要な課題に関して、基礎研究から出口（実用化・事業化）までを見据えて内閣府が推進する取り組みであるが、その中の「重要インフラ等におけるサイバーセキュリティの確保」（図13）について、当社でも協力している。

2020年の東京オリンピック・パラリンピックでの実用化を目指す、「制御系システムの新たなセキュリティ技術の開発」に対して、推進委員会への参加、社員派遣に加え、研究フィールドの提供も行っていく。

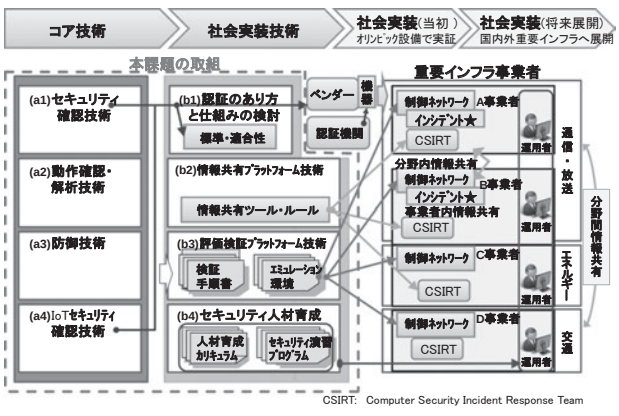

図13　SIP計画の全体像 ※SIPのHPの資料をもとに作成