JR西日本グループ

もっとつながる。未来が動き出す。

第6回IT協会 DigitalDays2026 基調講演

大阪・関西万博に向けた
グループ全体で信頼をつなぐ
持続可能なセキュリティ態勢の構築

西日本旅客鉄道株式会社
株式会社JR西日本ITソリューションズ

アジェンダ

1　会社・事業概要

2　推進体制

3　テーマ設定の理由

4　取り組み詳細

5　効果、成果

6　今後の課題と展望

1

会社・事業概要

会社概要

（2025年4月1日 時点）

- 社　　名　西日本旅客鉄道株式会社
- 設　　立　1987年4月1日
- 社 員 数　45,450人（連結）　24,580人（単体）
- 子 会 社　145社（うち連結子会社60社）
- 事業内容　運輸業（鉄道･バス･船舶）
  流通業（物販･飲食･百貨店）
  不動産業（SC･賃貸販売業）
  その他（ホテル･旅行業 etc.）

京阪神だけでなく、是非、
北陸、和歌山、山陰、中国、
福岡にお越しください！

「IT Report 2026」の発行

IT部門の活動結果及び今後の活動方針をまとめた**年次報告書「IT Report 2026」**を発行しています（当社HPに掲載）。

【P3】当社の提供する様々なサービスと表彰

コロナ後、グループ各社の会員・ポイントを統合、WESTER軸にサービス拡大

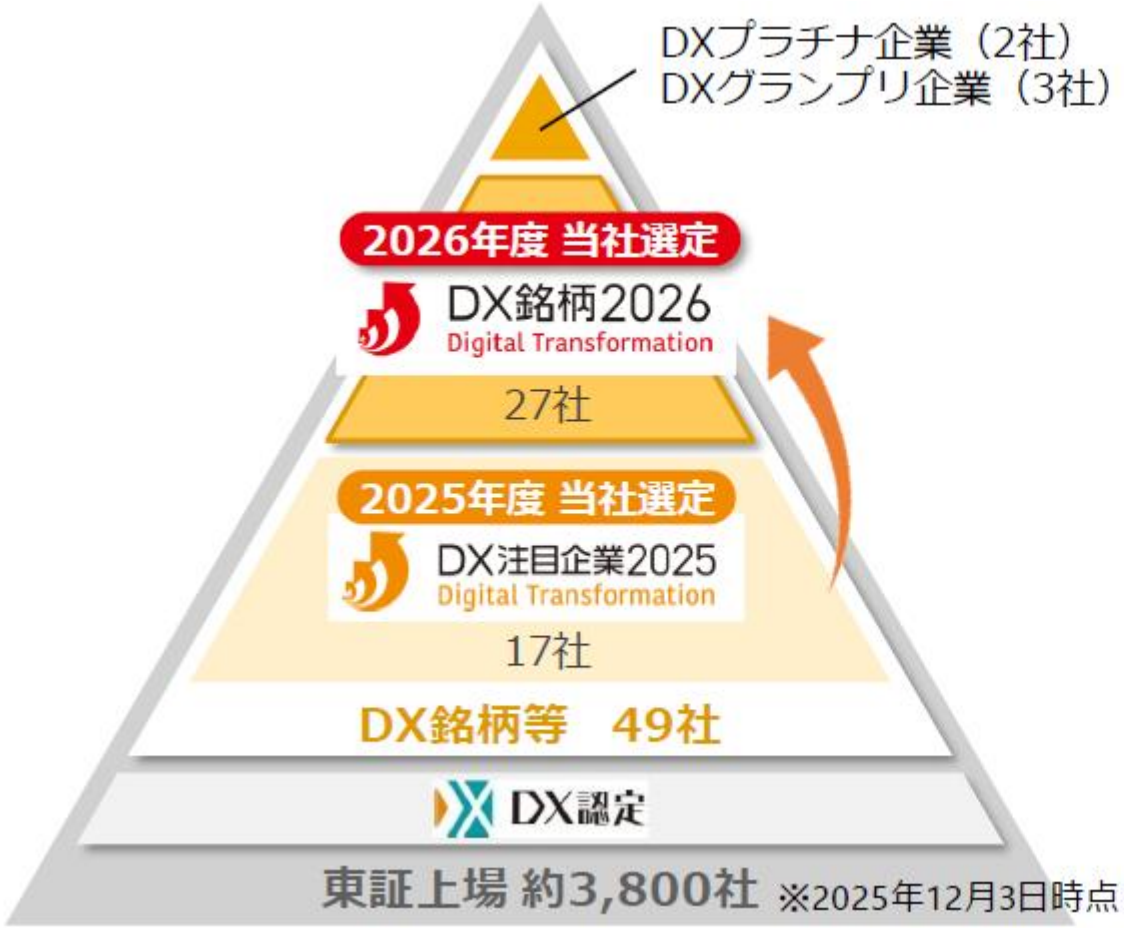
国内鉄道事業者で初の第二種資金移動業登録、<u>コード決済サービス開始</u>

りそなグループとの資本業務提携を発表
関西みらい銀行への出資を通じ、
地域経済の活性化に向けた事業連携を推進

【P16】「DX 銘柄 2026」に初選定

経産省、東証およびIPAは、東京証券取引所に上場しているDX認定を受けた企業の中から、企業価値の向上につながるDXを推進するための仕組みを社内に構築し、優れたデジタル活用の実績が表れている企業を「DX銘柄2026」として選定しています。

JR西日本は、2025年に「DX注目企業2025」に選定されたことに続き、2026年にはさらに上位の「DX 銘柄2026 」に選定されました。経営戦略にDX活用が明確に位置づけられている点や、WESTERサービスをはじめとしたDXがすでに価値創出に貢献している点、グループ横断でDXに取り組み、技術やノウハウが共有されている点が評価されました。



【P119】情報セキュリティの取り組みに対する評価

情報セキュリティの取り組みが「IT賞（経営・業務改革）」を受賞

「大阪・関西万博に向けたグループ全体で信頼をつなぐ持続可能なセキュリティ態勢の構築」が、公益社団法人企業情報化協会（IT協会）が主催する「2025年度（第43回）IT賞」において「IT賞（経営・業務改革）」を受賞しました！

IT協会からのメッセージ

徹底して組織的、人的、技術的に対策を講じている企業はほんの一握りと考えられる。加えて、他社の参考になるよう、セキュリティ施策を公開する姿勢も高く評価できる。

サイバーインデックス企業調査において一つ星を獲得

サイバーセキュリティへの情報発信および取り組みが積極的であると評価され、一般社団法人日本IT団体連盟（IT連盟）が格付けする「サイバーインデックス企業調査2025」において一つ星を獲得しました！

自己紹介

西日本旅客鉄道株式会社
技術理事／CISO／サイバーセキュリティ責任者
共創ソリューション本部　システムマネジメント部長　甲斐　康弘
情報処理安全確保支援士（登録番号第025068号）

1991年～JR西日本入社、広島支社（販売促進・収入管理・指令業務等）

事務系採用だけど、数学専攻だったことから、財務部に異動

1997年～財務部（会計・税務・システム・設備投資管理の他、各種PJT）

財務ERP導入PTチームリーダ、J-SOX導入PT責任者、
経理子会社設立　等

2008年～JR西日本伊勢丹、2015年～西日本JRバス（各4年間）

京都伊勢丹（経理担当部長）：大阪三越伊勢丹開業
西日本JRバス（企画担当取締役）：貸切バス子会社設立、
不動産開発　等

50才でIT部門へ

2019年～システムマネジメント部へ、現在に至る（セキスペ・プロマネ）

2

推進体制

推進体制

- JR西日本にCISOを委員長とした**情報セキュリティ委員会**、**重要インフラ部会**、**グループCSIRT事務局**を設置
- **グループ各社（80社）にも情報セキュリティ委員会、CISO、CSIRTを設置**　**※CSIRTは現業機関にも配置**
- **グループ会社を支援するグループセキュリティアドバイザー（5名）を編成**

最高情報セキュリティ責任者（CISO）

情報セキュリティ委員会

委　員　長　：情報セキュリティ担当役員（CISO＝技術理事　システムマネジメント部長）
副 委 員 長　：システムマネジメント部　情報セキュリティ室長
委　　員　：会長・社長・副社長、各役員・部門長、カンパニー長　等

重要インフラ部会
（運行・電気・出改札・ICOCA・Wesmo！等）

部会長：各部門長
事務局：情報セキュリティ室　等

JR西日本 情報セキュリティ室
JR西日本ITソリューションズ（J-WITS）
・JRW-CSIRT事務局（約30名）
・グループセキュリティアドバイザー（5名）
・グループIT業務支援

支援

JR西日本各部門　**グループ各社**

JR西日本グループ経営層
JR各部門長、グループ各社社長・CISO・委員会

JRW-CSIRTメンバー
（80社 520名）
JR各部門、グループ各社のセキュリティ担当

JRW-CSIRTサポートメンバー
（80社 2,100名）※現業機関にも
各箇所（現業機関含む）のセキュリティ担当

JR西日本グループ全社員等
（約50,000名）
役員・社員の他、同一環境の委託・派遣社員等

連携

グループリスクマネジメント委員会
↕
ガバナンス推進本部

連携（顔の見える関係性）

外部機関
・NCO　・国土交通省
・警察機関　・IPA
・交通ISAC　・NCA　他

※万博期間中は、NCO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）」への参加、博覧会協会との情報共有などを追加的に実施

「鉄道事業法施行規則」改正対応に向けた推進体制

- 「鉄道安全管理規程」に**サイバーセキュリティの確保を明文化**
- **サイバーセキュリティ確保に関する体制を新たに追加**し、**CISO（現在はシステムマネジメント部長）をサイバーセキュリティ責任者に指定**

■ 鉄道安全管理規程に新たに追加する内容

経営の責任者の責務	✓ 輸送の安全の確保に係る責任の対象に、**サイバーセキュリティの確保を追加**
管理者の役割・所掌	✓ 対象となる重要インフラの管理者に、**サイバーセキュリティ確保の具体的役割を追加**
サイバーセキュリティ責任者の指定	✓ 輸送の安全の確保に関する体制に、**サイバーセキュリティ責任者を追加**
サイバーセキュリティに関する責務、実施項目、管理方法等	✓ サイバーセキュリティ責任者の責務 ✓ 事業の実施及び管理の方法 – サイバーセキュリティ侵害の**防止対策の検討** – **業務の確認**（及び外部能力の活用） – **規程等の整備** – サイバーセキュリティ侵害の**報告及び対応** – 安全管理体制の維持のための**教育・訓練**

■ 輸送の安全の確保に関する体制

輸送の安全の確保に関する体制(サイバーセキュリティ確保に関する体制を除く)

- 社長
  - 鉄道本部長(安全統括管理者)
    - 主管部長（一部）箇所長
    - 主管部長（一部）箇所長
  - 経営戦略本部長

- 運転管理者：運輸部長、新幹線運輸部長
- 乗務員指導管理者：乗務員の所属する箇所長

サイバーセキュリティ確保に関する体制

- 社長
  - 鉄道本部長(安全統括管理者)
    - 安全推進部長
  - **サイバーセキュリティ責任者(CISO)**
    - 主管部長（一部）箇所長
      (イノ部長、電気部長、新幹線電気部長等)
    - 支社長等（一部）箇所長
      (大工所を除く支社長等)

※サイバーセキュリティ責任者は、安全の「管理者」とせず、「その他必要な責任者」と位置づけ、緊急事象発生時以外は総合安推会議等に絞って出席する

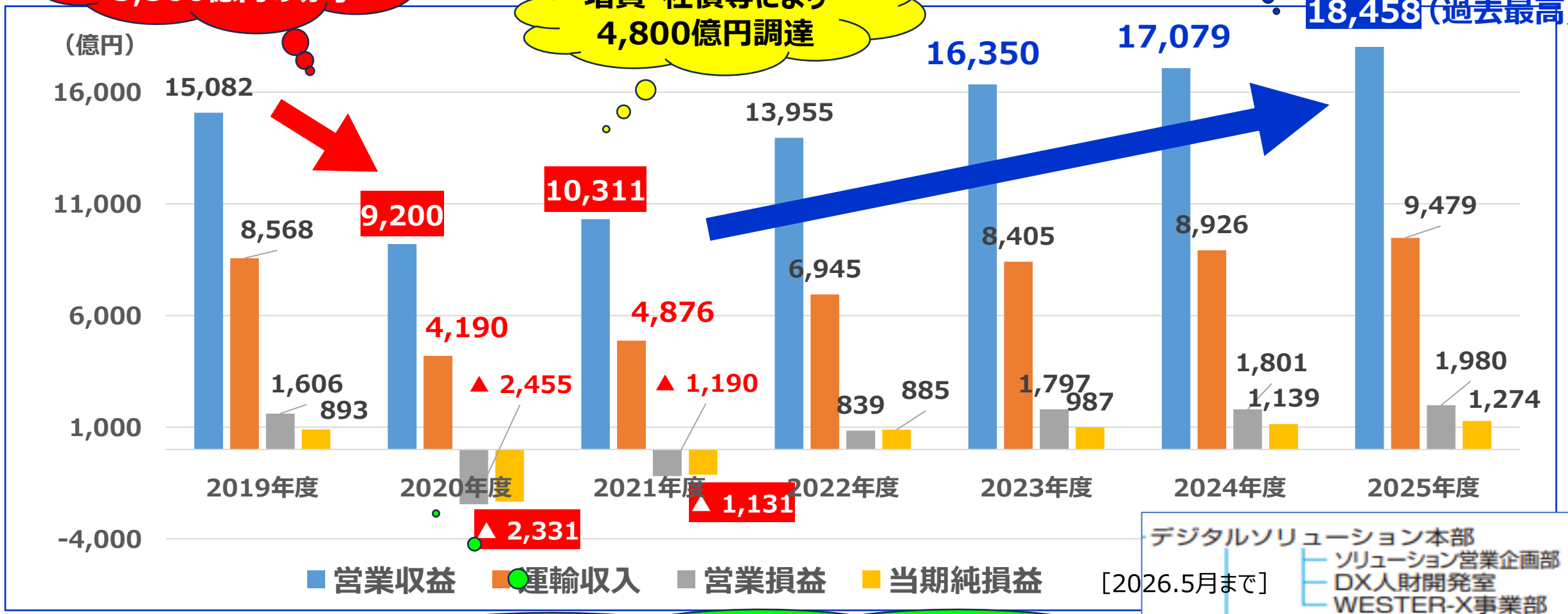
3 テーマ設定の理由

コロナからの変革・復興、進化・成長

2年間で、
1兆円超の売上消失
3,500億円の赤字

増資・社債等により
4,800億円調達

3年連続で営業収益
過去最高を更新中



2020年10月「グループデジタル戦略」公表
同11月、社長をトップとするデジタルソリューション本部発足

［2026.5月まで］

- デジタルソリューション本部
  - ソリューション営業企画部
  - DX人財開発室
  - WESTER-X事業部
- システムマネジメント部
  - 情報セキュリティ室
- ビジネスデザイン部
  - JCLaaS事業部

課題の背景

➢ コロナ禍からの変革・復興に向け、デジタル戦略を拡大していた矢先、

グループ会社で重大セキュリティインシデント発生

✓ 重要インフラの鉄道を基幹事業とする当社グループの**サービス停止は、地域社会に大きな影響を及ぼす。**

✓ 重要インフラグループとして、**お客様に安心・信頼してサービスをご利用いただくことが我々のミッションであり、事業成長や企業力の強化につながる。**

地元開催の万博を控え、セキュリティをグループ共通の重要な経営課題と捉え、グループセキュリティガバナンスを抜本的に見直したい！

当時の委員会資料（目的、役割、具体策、KPI等抜粋）

第32回 情報セキュリティ委員会

2022年7月5日
デジタルソリューション本部 IT部

○目　的

・情報セキュリティを取り巻く急激な環境変化（リスク・被害の増大、一方で防衛技術は向上）と、グループ会社における重大インシデント発生を受け、セキュリティ強化策の方向性及び主な具体策について決定する。（決定後は直ちに実行に移し、順次、導入）

・対策を迅速かつ効果的に推進するため、「経営層」「JRW-ITセキュリティ部門」「システム利用部門（≒各社主管部門）」「システム開発・運用部門（≒各社IT部門）」「利用者」それぞれの役割と責任を明確化・共有する。

各組織の役割と責任

	経営層・CISO ※1	セキュリティ部門（JRW-IT部門）	システム利用部門（≒各社主管部門）	システム開発・運用部門（≒各社IT部門）※2	利用者
1 組織的対策	ガバナンス体制の構築・運用（方針決定、CSIRT等体制、PDCA評価等）	ルール策定、全体統括、インシデント監視・対応支援［CSIRT事務局］	情報資産のリスク評価（計画時・変化点）・棚卸、インシデント対応	システムのリスク評価（計画時・変化点）・棚卸、インシデント対応	インシデント報告
			BCP策定・対応（業務）	BCP策定・対応（システム）	
2 人的対策	リソース配分	全体教育・訓練、リーダ育成	利用者教育、リーダ育成支援	開発・運用者教育	リテラシー向上
3 技術的対策		全体対策策定・実行、シェアードサービス提供	リスク評価に基づくセキュリティ要件決定	セキュリティ要件に基づく対策実装	ルール順守

セキュリティ強化策の方向性（課題）及び主な具体策［1/2］

↓ 本日、決定したい内容

方向性（課題）		主な具体策	補足
1 組織的対策			
経営者のセキュリティ感度の向上（経営責任としての意識付け）	①	・カンパニー制を踏まえたセキュリティガバナンス体制の再構築	・カンパニー統括、主管部による所管会社への経営リソース・取組支援 ・セキュリティに係る業績評価指標検討
	②	・情報セキュリティトップ研修の開催（JR各部門、グループ会社のトップ）	・ガバナンス/テック両面
システム計画時・変化点でのリスク評価	③	・セキュリティ審議の導入（リスクの高い個人情報、インターネット接続を対象）	・JR導入済、グループ各社での審議を仕組化・支援（チェックリスト、人材育成、アドバイザリー等）
インシデントの早期検知・対応体制の構築	④	・JRW-CSIRTの体制強化（グループ全体を対象） ・公表等対応基準の策定	・攻撃の早期検知や分析・対策を講じる24時間体制の専門組織をJRセキュリティ部門に構築
2 人的対策			
インシデ…向上			
社員の意…シー向上			

本取組みを通じて達成するKPI

重大インシデント「ゼロ」

※重大インシデント：顧客個人情報の漏洩やWebサイト改ざんによる顧客への被害発生、1時間以上のサービス停止等で経営上の影響が重大なもの

- 未然防止
  - ・自主点検適合率「98.2% → 100%」
  - ・セキュリティ審議実施率（重要システム）「100%」
  - ・メール訓練開封率半減「5.9% → 3.0%」
  - ・脆弱なテレワーク環境（多要素認証、閉域）「ゼロ」
  - ・脆弱性管理「緊急度高への対応100%」
  - ・情報セキュリティリーダ認定「全組織に配置」
- 被害の最小化
  - ・インシデント早期検知体制「カバー率100%（※）」
  - ・メール訓練開封時の報告率「17.1% → 100%」
  - ・インシデント対応訓練「CSIRTメンバー100%」
  - ・バックアップ（重要システム）「複数世代化100%」

※各社・各部門が自己責任で構築する体制を含む

- 再発防止
  - ・同一原因のインシデント「ゼロ」

戦略意義～そんなに簡単に重要な経営課題と捉えてもらえるのか？

小さな会社でやる必要があるのか？　**人財もいないし、予算もない！**　**難しくて分からない**・・・

- **タイミング（平常時であればなかなか浸透しないが、）**
  - ✓ コロナ禍での未曽有の経営危機を受け、**IT・サイバー環境の劇的な変化を実感**
  - ✓ **グループ内で重大インシデントが発生したという事実**
- **役割・責任の考え方（一方的にグループ会社にのみ押し付けない）**
  - ✓ グループ会社のインシデントも、**我々コーポレート部門にも責任（1人称）**
  - ✓ グループ統一の取り組み・ツール等を**用意し、導入支援を行う　と宣言**
- **やってほしいことの明確化（技術的対策だけでなく、組織的対策・人的対策に焦点）**
  - ✓ 各組織の役割と責任を明確化し、**グループ共通のKPI**として設定
  - ✓ **社員一人ひとり**に取り組んでもらいたいことを示すことで、自分ゴト化
- **位置付けの明確化（グループ事業方針等への組み込み、トップメッセージ）**
  - ✓ セキュリティは**「必要なもの・やらなければならないもの」ではなく、経営・事業に資するもの、攻めを拡大・加速させるためのもの！**

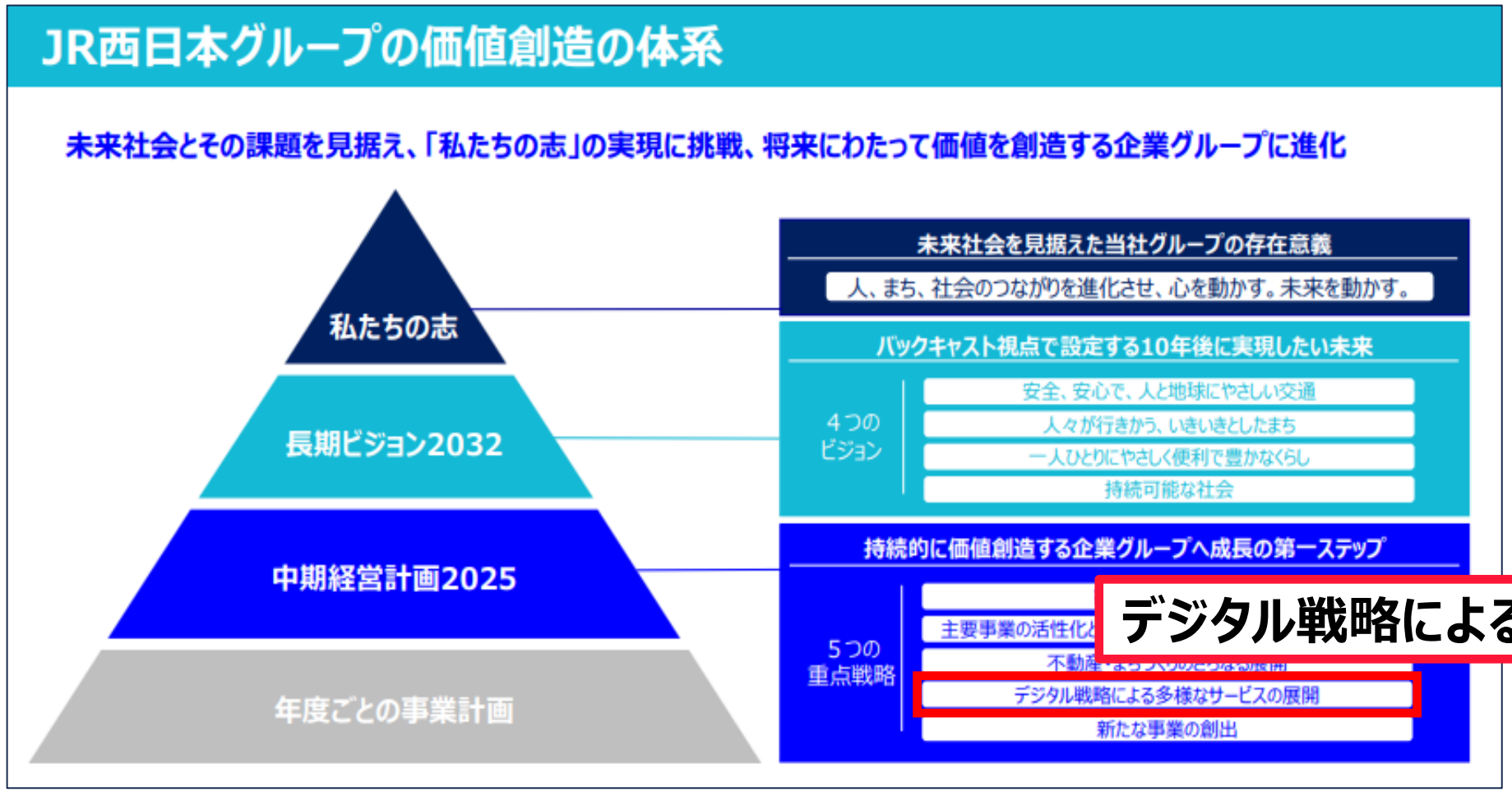
グループ事業方針等への組み込み

- 2023年4月、ポストコロナを見据え**「グループの価値創造体系（「私たちの志」とその実現に向けたビジョン・重点戦略）」を再定義**

- **デジタル戦略を重点戦略と位置付けるとともに、「グループ事業方針」において、デジタル戦略の構成要素として「情報セキュリティ・レジリエンスの強化」を明記**

- **セキュリティを攻めのデジタル戦略との両輪と位置付けたことで、セキュリティの取り組みも共感を得、グループ全体で推進可能に！**

グループ事業方針等への組み込み



「長期ビジョン2032」
「中期経営計画2025」
より抜粋

「中期経営計画2030」
ではより一層重視！

デジタル戦略による多様なサービスの展開

デジタル戦略 2.0

「グループ事業方針」（2023年度）より抜粋

⑤デジタル技術、DX・ICT基盤の整備、**セキュリティ・レジリエンスの強化**

・**デジタル戦略を支える安全で信頼されるセキュリティシステムの構築、**レジリエンスの強化

革新性～セキュリティの持続的強化を可能とする企業文化の醸成

➢グループセキュリティガバナンスの抜本見直しにおいて、

「技術」に加え、無限の進化・成長の可能性を持つ「組織」「人」に焦点をあて、

万博対応という一過性の取り組みとせず、

セキュリティの持続的強化を可能とする企業文化の醸成を目指す！

組織的対策・人的対策にあたってのポイント

	特徴/方針	具体的打ち手
共通	・進化・成長に無限の可能性 ・結果として、IT・デジタルの利活用を促進させ、生産性向上、働き甲斐向上につながる	―
組織	・鉄道を基幹事業とする当社グループは一体感・連携による推進力が強み ・各組織のトップの共感を得ることがスタート ・グループ各社を孤立させない、信頼を得る ・グループ会社でのインシデントも個社の問題ではなく、グループ全体の問題として取り扱い	・各社にセキュリティ委員会/CISO設置 ・トップ研修・グループ社長会、トップメッセージ、業績評価指標 ・グループ統一の対策、ツール・サービス・脅威インテリジェンス調査の提供、支援・伴走により、グループ会社の負荷軽減 ・各箇所へのCSIRTメンバー配置
人	・「最大の弱点」であり「最後の砦」でもある ・組織の隅々、一人ひとりまで行き届かせる	・全役員・社員向けの研修・メール訓練 ・リーダ育成 ・高度専門人財の確保・育成

4 取り組み詳細

組織的対策

- トップメッセージやトップ研修、グループ共通KPIに基づく業績評価・表彰等により、**各組織トップを巻き込んだセキュリティ強化のPDCAサイクルを確立**

- **グループ80社を対象に、**各トップ参画のインシデント対応訓練によるレジリエンス向上、EDR導入や脆弱性管理ツール・脅威インテリジェンス調査によるリスク低減により、**万博前にセキュリティ強化**

- **現場レベルまでCSIRTメンバーを配置**することで、**取り組みを組織の隅々まで広めることができる体制**を構築

組織的対策① トップ研修

➢ **全役員・部門長、グループ会社社長・CISOを対象に　4回/年　開催**

万博開幕前後のサイバー攻撃の状況

➢ **万博開幕前後の特別警戒期間［4/10（木）～4/14（月）］において、グループ全体で監視レベル・即応態勢を強化**

【 国内全体の状況 】

◆ 4月10日　Anonymous Chinaによる犯行声明をXで３件確認
- **通信会社、銀行、航空会社をシャットダウンさせた旨の投稿**

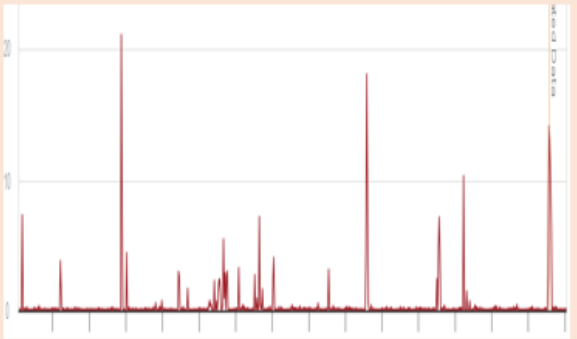
◆ 4月11日　セキュリティベンダ（Akamai社）が**上記犯行と思われる攻撃を観測**

【 当社グループの状況 】 攻撃予告、探索活動確認 ⇒ 警戒態勢継続！

◆ 3月31日　**当社を狙うDDoS攻撃の予告に関する情報入手**
- 「ICOCA」への攻撃について言及あり

◆ 4月10,11,14日　**当社へのサイバー攻撃を検知、警戒態勢継続！**
- おでかけネット、westjr.co.jpへのDDoS攻撃、脆弱性探索活動
- 1秒あたり7,000を超えるアクセス

⇒ 事前対策によりサービス影響なし（DDoS対策「CDN/WAF」）
攻撃の激化に備え、事業部門に連携（BCP/Sorryページ準備）
攻撃元IPアドレスの遮断措置を実施（攻撃の特徴に応じた対処）



直近1か月間のDoS攻撃トレンド
（断続的に一定規模の攻撃あり）

万博終了後も継続

2025年度第1回研修の例

組織的対策② グループ各社に対する業績評価指標

➢ グループ会社の業績評価指標の1つにセキュリティを組み込み

分類	項目	2025年度
組織的対策	(1)重要システムの自主点検活動適合率	100%
	(2)重要システムのセキュリティ審議実施率	100%
人的対策	(3)標的型攻撃メール訓練 対象者全体に占める未報告者の割合	1%未満 または 1名以下
	(4)情報セキュリティリーダ認定者の割合	10%以上
技術的対策	(5)重要システムのバックアップ取得状況	100%
	(6)脆弱なテレワーク環境	0件
	(7)脆弱性対応計画の報告漏れ件数	0件
	(8)インターネット公開しているサーバ・ NW機器及びADサーバの脆弱性対応率	100%
	(9)脅威インテリジェンスを活用した 攻撃面調査における重要項目の対応率	100%
	(10)インシデント早期検知体制(カバー率)	100%

万博終了後も継続

（項目はアップデート）

組織的対策③ トップ参加のインシデント対応訓練

➢ **シナリオ作成～当日訓練までシスマネ部メンバーが伴走、JRは各役員・部門長、グループ各社は社長・CISO等が参加** ▶ **万博終了後も継続（復旧に焦点）**

インシデント対応訓練の実施概要

- 訓練シナリオは6つのSTEPで構成
- 経営トップは、**STEP2・3・6において議論・意思決定**

STEP1 知得	「システムが利用できない」「データが暗号化されているようだ」との報告を受ける。
STEP２ 対応方針検討～速報	・業務に**深刻な影響が出ている/出る見込みである。** ・復旧するまで**相当の時間がかかる。** といった報告を受け、 **速報等の初動をとるとともに対応方針を検討する。**
STEP３ 公表	**社外からの問合せ、SNSでの犯行声明を受け、公表の要否・内容を検討する。**
STEP４ 調査	原因と影響範囲を調査する。
STEP５ 調査結果～復旧	攻撃の全容が明らかになり、システムを正常に復旧する計画を策定する。
STEP６ 復旧・最終報告	システム/データは**復旧したとの報告を受け、サービス・業務の再開を検討する。**

出改札システムを対象とした訓練の様子

【訓練を終えての経営層の声】

- 訓練で**一連の対応を体系的になぞる**ことで、万一の際に慌てずに済む
- みんなで訓練し振り返ることで様々な視点を入れて更に改善しつつ**自分ゴト化**できた

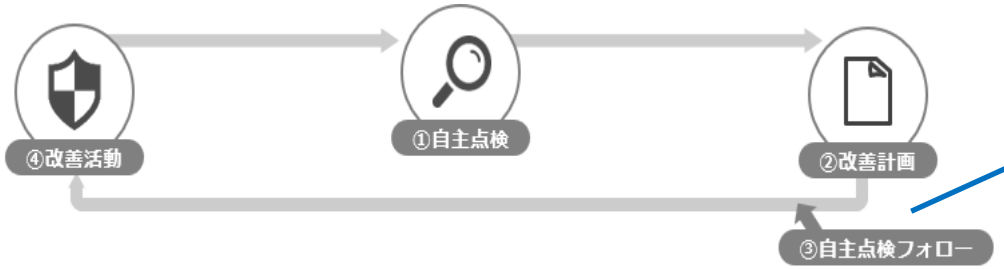
組織的対策④ グループガイドラインに基づくPDCA

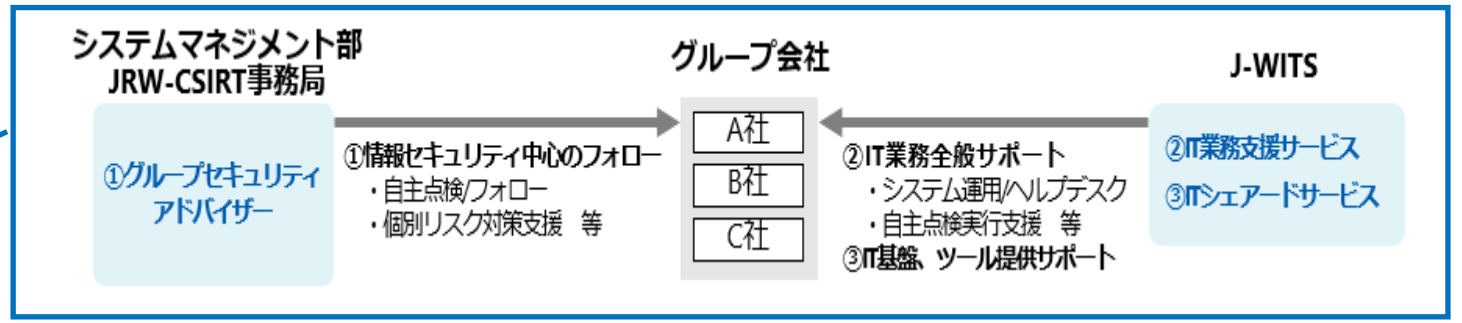
➢「JR西日本グループ情報セキュリティガイドライン」に基づく、**グループ全体で統一した対策**

■ **システム台帳**：グループ各社の情報システムを登録、**全数千システム**、システム構成、保有情報資産・重要性等

■ **ガイドライン**：情報セキュリティ管理基準（経産省）をベースに策定、毎年、実効性を高めるためにブラッシュアップ

■ **チェックリスト**：同ガイドラインに基づき策定**（システムを11分類、各40項目程度）**
JR各部門、グループ各社において、台帳登録システムを対象に自主点検を実施し、**グループセキュリティアドバイザーにより構成する専門チームが、実務層から経営層までの各レイヤと連携し、自主点検フォローから課題設定、改善活動まで伴走（PDCAサイクルを一緒に回す）**





▶ 万博終了後も継続、グループセキュリティアドバイザー体制強化

組織的対策⑤ 脆弱性対応のPDCA

➢ 脆弱性管理ツール、脅威インテリジェンス調査結果等への対応も**PDCAサイクルを一緒に回す**

■ グループ全体を対象に**脅威・脆弱性に対する「調査」「対応」を繰り返し実施（四半期ごと）**

JR西日本 セキュリティ部門

最新の情報に基づく調査

- 脆弱性管理ツール
- 攻撃面調査
- ダークウェブ モニタリング 等

JR各部門、グループ各社

新たな脆弱性・脅威に対応

- リスクの分析・評価
- 対応方針決定
- パッチの適用 等

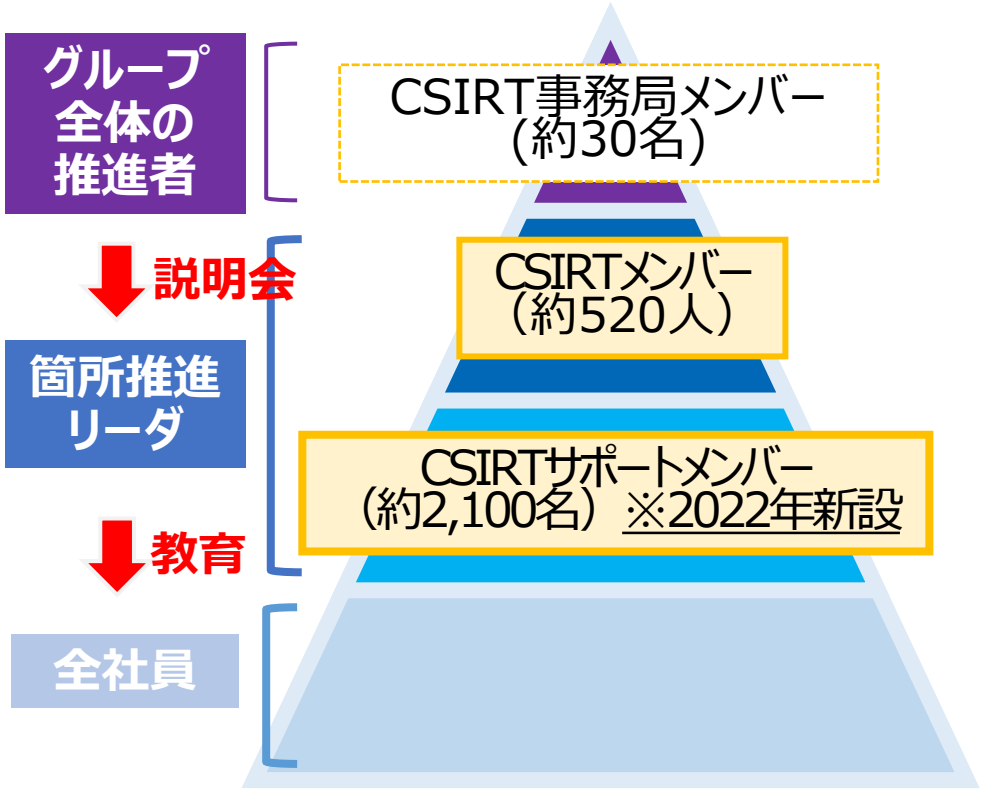
※自主点検/脆弱性等対応は各部門長、グループ各社社長・CISO承認のうえで提出とすることで、経営層による実務者サポートを推進

▶ 万博終了後も継続、フロンティアAIの劇的な進化を踏まえた対応強化

- ➢ **攻撃機能向上を踏まえた課題：パッチ適用の早期化**
- ➢ **防御機能向上を踏まえた課題：未知の脆弱性発見・パッチ適用の自動化**

組織的対策⑥ JRW-CSIRT

- 情報セキュリティ室に事務局を置き、JR各部門、グループ各社に**CSIRTメンバー（80社、520名 ※部門・会社単位、管理職＋担当者）**と**サポートメンバー（80社、2,100名 ※箇所単位**、管理者＋担当者）を配置
- 研修やインシデント対応訓練に参加する他、各組織におけるリテラシー向上、インシデント対応を担当**（現業機関含む各箇所において、メンバーが中心となり全社員に直接教育を行うことで、組織の隅々まで行き届かせる）**
- JRW-CSIRT事務局は、**四半期ごとの「CSIRTレポート」発行**、**各エリアでの意見交換会開催**等を通じて、グループ全体の一体感を醸成し、日頃の取り組みをサポート



JRW-CSIRTサポートメンバーとの意見交換

研修に加え、JRW-CSIRTサポートメンバーとの意見交換を行い、活動のフィーチャリング及び好事例については他組織に水平展開しています。

3名が情報セキュリティマネジメント試験に合格した京橋統括駅との意見交換の様子

万博終了後も継続、箇所長の意識向上

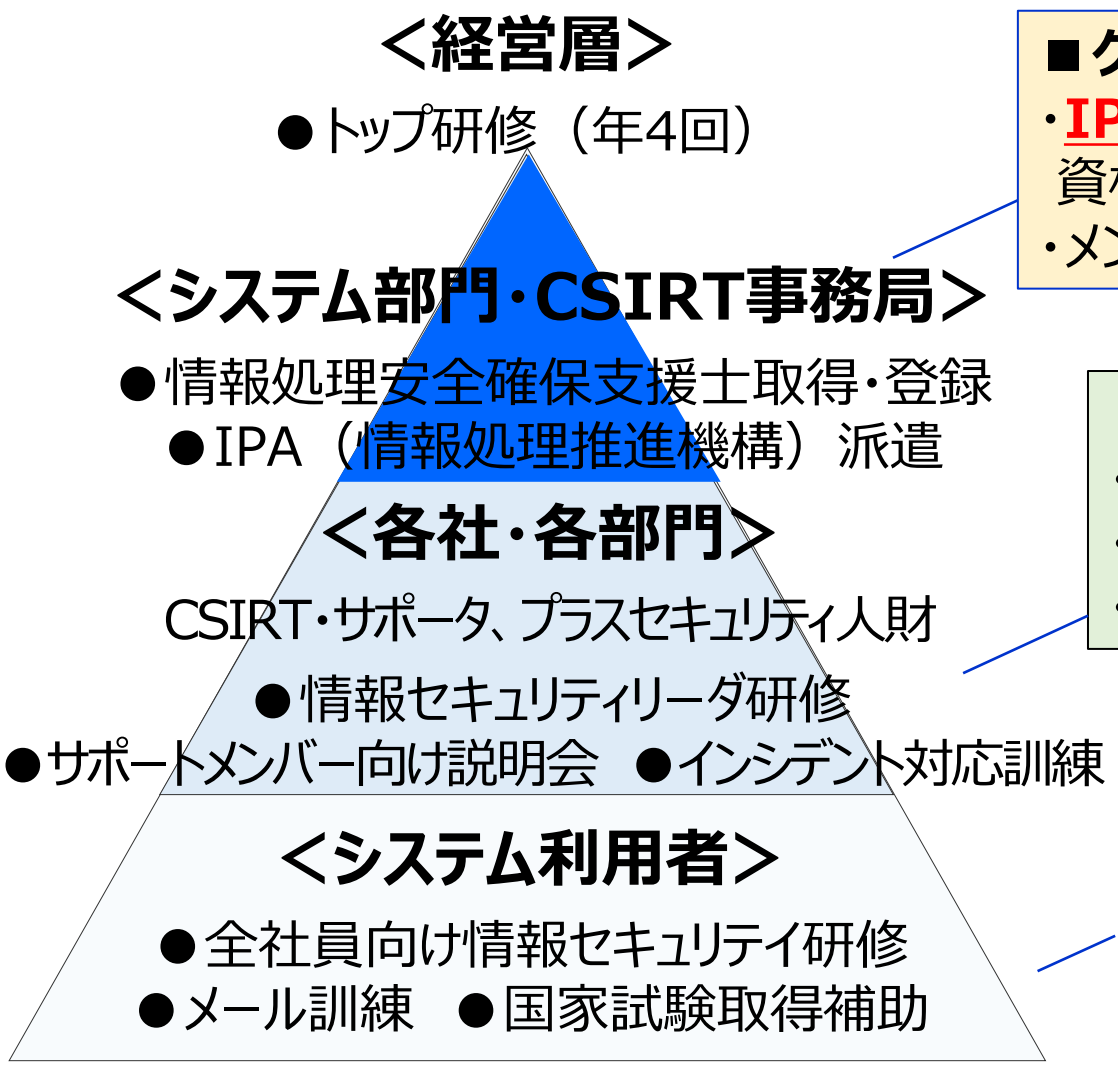
人的対策

- セキュリティの**「最大の弱点」**であり**「最後の砦」**でもある

- グループの特情や階層等に合わせた**独自の自前研修、認定証・キャラクターステッカー等により関心を高め、**多数のリーダ育成を目指す

- 攻撃メールが巧妙化する中で**「開封したことを叱らず、報告を褒める」**との考え方を繰り返し伝え、**報告文化を醸成**

人的対策① 人財育成



■グループ全体の推進者：
・**IPA中核人材育成プログラム**（1年間）派遣/毎年、
資格取得支援、高度専門人財の社会人採用、社内ポスト公募
・メンバーの活躍を社内外に積極的にアピールし、**フィーチャリング**

■各組織の推進リーダ：
・**リーダ研修（独自・自前資料）**によるリーダ認定者の育成
・全８回の動画視聴と各確認テスト満点で認定（10時間）
・**認定書授与、認定ステッカー配布**

■資格取得支援制度の例（JR西日本）
・**一時金支給：**
合格 → 受験料＋20,000円、**不合格 → 受験料**
・**情報処理安全確保支援士等の高度資格合格者：**
職務手当10,000円/月

万博終了後も継続、強化：関係省庁への人財派遣、社内CTF大会開催

人的対策② マスコットキャラクターの活用

マスコットキャラ(にし～さ～)を活用した啓発活動

JRW-CSIRTのマスコットキャラ「にし～さ～」を活用し、情報セキュリティを身近に感じてもらえるよう啓発活動を実施しています！！

▼JRW-CSIRTの認知度向上や情報セキュリティを学ぶモチベーション向上のためにステッカー配布

にし～さ～

▶ **万博終了後も継続**

人的対策③ 全役員・社員対象のメール訓練・教育

➢ JRW-CSIRT加盟会社の全役員・社員（50,000人）を対象とした標的型メール訓練（4回/年）

・危機意識の醸成と初動対応力の向上を目的

・**「開封しない」以上に、「開封したら速報する」を重視**したKPI設定とメッセージの発信 **「報告ありがとう！」**

・2025年度は被害が拡大する**フィッシングメールを模したメール訓練を実施**

➢ 50,000人を対象とした教育（直接教育と確認テスト、各トップメッセージ）

【まとめ】絶対に守ってほしい不審メール対策 10のポイント

・万博開催にあたり当社グループを標的とするサイバー攻撃が増加しますが、一人ひとりが不審メールに適切に対応し、お客様に安心・信頼してご利用いただけるサービスを提供しましょう！

No.	分類	確認内容
1	不審メールの理解	不審メールやURLクリック等でウイルス感染した場合、速やかに対処しなければ会社全体にウイルスが拡散する。
2		フィッシングによるID・パスワード乗っ取り対策として、正規のログインページをお気に入り登録して利用する。
3		パソコンだけでなく、スマホやタブレットでもウイルスに感染したり、偽サイトに誘導される。
4	不審メールの見分け方	身に覚えのないメールが届いた場合、添付ファイルの開封やURLをクリックせずにメールを削除する。
5		普段やり取りしている相手でも、内容やメールアドレスに違和感がある場合、電話等で発信元に確認する。
6		万博のような注目イベントが開催される場合、「ボランティア募集」「入場券当選」等を語る不審メールが増加する。
7	開封時の対応	不審なメールを開封したり、URLをクリックした場合、メールを削除したり、画面を閉じてもウイルス感染は防げない。
8		不審なメールを開封したり、URLをクリックした場合、端末を直ちにネットワークから遮断する。
9		不審なメールを開封したり、URLをクリックした場合、会社指定の連絡先（ヘルプデスク等）に電話で速報する。
10	サポート詐欺	パソコン等に警告画面が表示された場合、会社指定の連絡先（ヘルプデスク等）に電話で速報する。

注意喚起ポスター

万博終了後も継続、

・強化：フィッシング型

・新規：社長名

5

効果、成果

効果・成果

- **各組織トップの自分ゴト化**により、グループ全体で経営の重要課題であるとの認識を共有、**IT領域でも安全を最優先する企業文化を醸成。**トップの強力なリーダーシップもあり、**3年間で態勢を構築**

- **これらの取り組みを通じ、**2024年度グループ全体の**インシデントは9割減、**WESTERを始めとした**デジタル戦略を加速させ、同年度連結営業収益は2期連続過去最高**と、**企業力の向上に貢献**

  - **2025年度も万博期間を含め、重大情報セキュリティインシデントゼロ**
  - **同年度連結営業収益は3期連続過去最高**

- 万博対応に留まらず、**セキュリティの持続的強化を可能とする企業文化の醸成につなげた**

効果・成果① 組織的対策

➢ トップ研修（役員・部門長、グループ会社社長・CISO、4回/年）

▶ 継続開催中

・2022年度以降、**計12回開催**（2025年8月時点）

➢ グループ各社に対する業績評価指標の1つとして情報セキュリティを設定、表彰

・**KPI達成状況**（2024年度）

項目	目標	達成状況
早期検知・脆弱性管理対応体制	**90%以上** EDR72社・脆弱性63社	**◎達成：100%** （EDR80社（済）・脆弱性70社（見込））
メール訓練 未報告者割合	**1%未満**	**◎達成：0.8%** （全4回の訓練結果の平均）
情報セキュリティリーダ 認定者数	**10%（4,800人）**	**◎達成：6,595名** （★ﾘｰﾀﾞ:6,298名 ★★ﾏﾈｰｼﾞｬ:227名 ★★★ｽﾍﾟｼｬﾘｽﾄ:70名）

▶ 2025年度も達成

※2025年度は有資格者を配置しているグループ各社数を新たにKPIとして設定

・様々な機会を捉えてグループトップがメッセージ発信
・各組織トップのリテラシーが定着、経営課題として浸透

2024年度 表彰組織

上記KPI等に基づき、特に顕著な成績を達成している組織を優秀組織として表彰し、JR西日本グループ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ています。
2024年度実績をもとに、最優秀：4組織、優秀：5組織、奨励賞：１組織、に対して表彰を行いました。

表彰の様子（大阪電気工事事務所）

表彰の様子（JR西日本SC開発株式会社）

効果・成果② 組織的対策

➢ トップ参加のインシデント対応訓練の実施 ▶ 2026年度もトップ全員参加で計画

・各組織において重要システムを選定、シスマネ部メンバーを支援者に指定し**シナリオ作成～当日訓練まで伴走、約半年間の準備期間を経て100以上の組織で実施、1,000名超が参加**

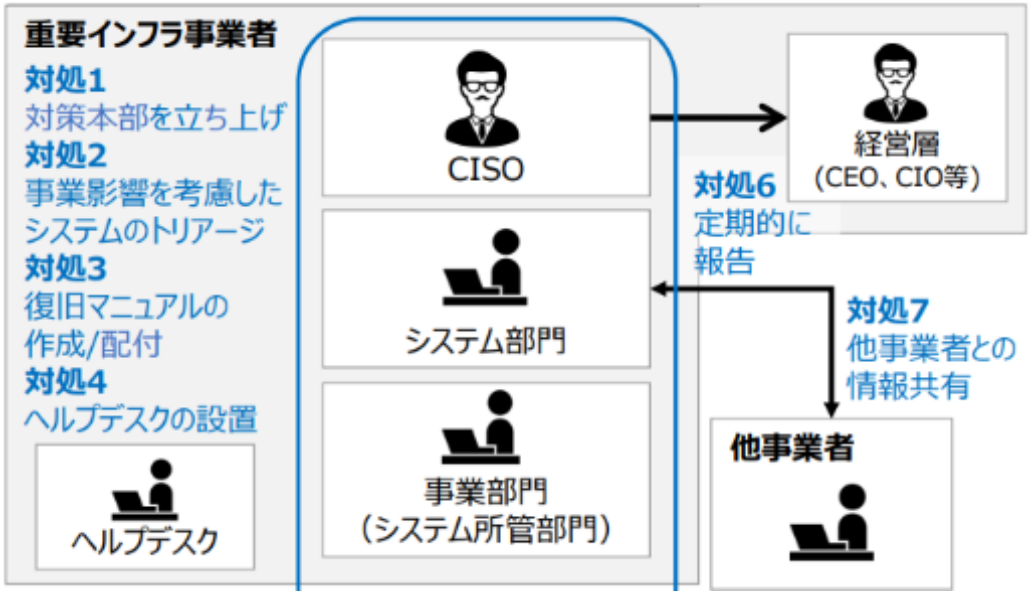
当社事例

■ **サイバーセキュリティ戦略本部　重要インフラ専門調査会（第39回）資料より**

事例６：セキュリティ製品の不具合に伴う複数システムへの復旧対応 1／2

14

- 重要インフラ事業者の各システムに順次導入していたセキュリティ製品パッチに不具合があり、当該パッチが配信された端末/サーバーが異常停止したことにより、複数のシステムが機能を停止した。
- 重要インフラ事業者は、対策本部の立ち上げ、情報システムのトリアージ、あらかじめ定めていたシステム大規模停止時の対応手順に基づいた必要な対処等により、重要インフラサービスへの影響を最小限に抑えた。



DDoS攻撃によりサービスが不安定になった場合でも、初動・復旧対応に対して、トップから評価されるように

6. 得られた気付き・教訓

- **適切な資産管理をベースとした各システムの復旧の優先順位付け**

  本事例では、資産管理が適切に行われており、事業継続の観点から、どのシステムを優先的に復旧させるべきなのか、速やかな対応優先度の判断が可能となった。

- **対応手順の整備と訓練の実施**

  経営層を含めたインシデント対応訓練を実施していたことで、経営層/部門/グループ会社間の情報共有や連携を速やかに実施できた。平時からシステム障害を見据えた対応体制や手順を整備し、訓練することにより「対応の型」というべきものを醸成しておくことが重要。

- **速やかな対応の結果生み出した余剰リソースの活用**

  本事例では、上記の対策によって組織全体でのインシデント対応を効率的に行えた結果、余剰リソースを生み出し、ヘルプデスクのようなリソースを大量に必要とする対応を実施可能にした。平時の対策実施が、緊急時のリソースを生み出すという副次的効果を発揮した。

効果・成果③ 人的対策 ▶ 2025年度も取り組み推進

- ・多くの社員が自発的にスキルアップに挑戦
- ・現業機関にも有資格者リーダが増え、活躍

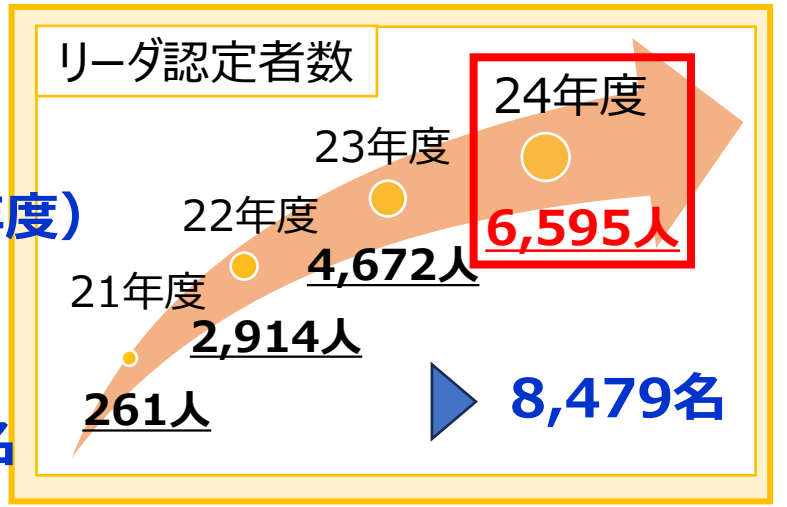
➢ グループ全体の推進者

- ・**IPA中核人材育成プログラム**（1年間）派遣：**8名**
- ・**高度セキュリティ人財の社会人採用等受入：9名**、社内ポスト公募：7名
- ・**情報処理安全確保支援士：74名**（CISO自身を含む、グループ全体）

情報セキュリティマネジメント試験合格者：392名

➢ 各組織の推進リーダ

区分	条件	認定者数	（2025年度）
★★★	情報セキュリティスペシャリスト （リーダ研修修了＋情報処理安全確保支援士試験合格）	70人	▶ 93名
★★	情報セキュリティマネージャ （リーダ研修修了＋情報セキュリティマネジメント試験合格）	228人	▶ 384名
★	情報セキュリティリーダ （リーダ研修修了）	6,297人	▶ 8,002名



➢ 現業機関における取り組み例（京橋統括駅）

京橋統括駅ではリーダ認定23名、うち3名はマネージャ認定を取得！

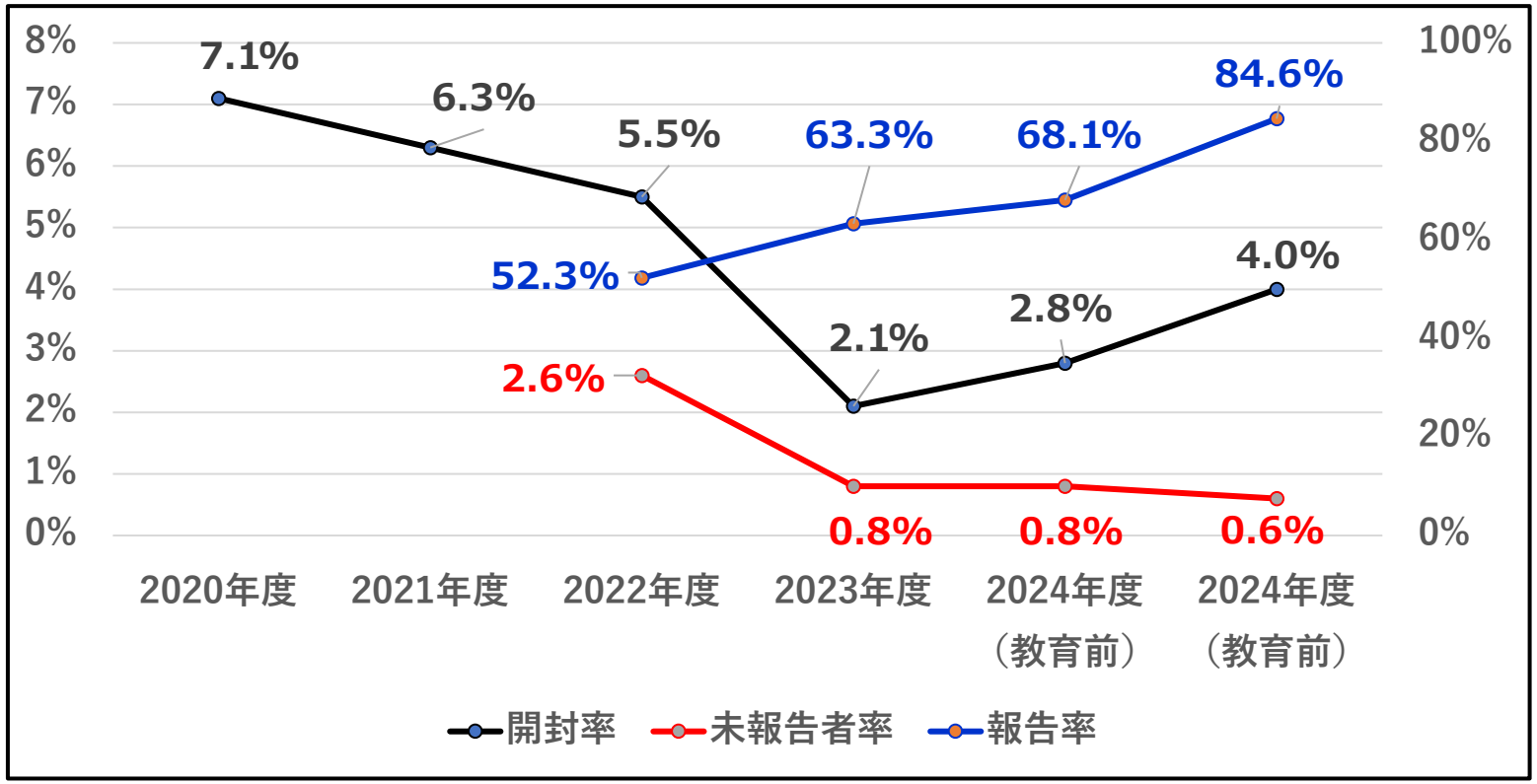
リーダ認定者　計6,479人 ▶ **8,479名**

岸田企画助役

社員に対してセキュリティ教育を行うときに、なぜセキュリティが大事なのか、どのような脅威に対してどのように対応すべきなのかを、自分の言葉で伝えられるようになりました！それと、今までよく分からずに使っていたPCの様々な仕組みが理解できるようになりました！　※「JRW-CSIRT Report」でも紹介

➢ メール訓練結果

	2020年度	2021年度	2022年度	2023年度	2024年度		
					教育前	教育後	記事
メールの開封率	7.1%	6.3%	5.5%	2.1%	2.8%	4.0%	文面の難易度UP
開封時の報告率	–	–	52.3%	63.3%	68.1%	84.6%	全社員直接教育により大幅UP
未報告者率	–	–	2.6%	0.8%	0.8%	0.6%	KPI「1%未満」達成



➢ **約50,000名を対象とした統一した教育（直接教育と確認テスト、各トップメッセージ）の結果**として、

・文面の難度化により「開封率」が増加したものの、

・開封時の**「報告率」が大幅に増加**し、

・開封後に報告をしない**「未報告者率」はKPI「1%未満」を大きく下回り達成！**

・「不審メールを開封しない」「開封したら速報（報告ありがとう！）」の文化が浸透

・メール訓練により、社員の意識も向上

6 今後の課題と展望

今後の課題と展望

- 「サイバー対処能力強化法（能動的サイバー防御導入法）」「経済安全保障推進法」「鉄道事業法」改正、「セキュリティクリアランス」等、新たな法制度対応と、**制度を最大限に活用するための体制・対応能力の整備**が、新たな重要課題
- サイバー攻撃の進化に対しては、エンドポイント対策に加え、**システム・ネットワーク全体で変化に対応し、対処可能な基盤・仕組み・体制を構築**
- **サプライチェーン**については、契約書へのセキュリティ項目の追加に加え、**実効性のある対策を順次推進中（委託先実地監査、チェックリストによる点検 等）**
- グループ全体リテラシー向上は、**グループ会社におけるキーパーソン・有資格者育成**を2025年度KPIとして新たに設定

＋フロンティアAIへの対応：官民連携、パッチ適用早期化、認証情報保護、レジリエンス

引き続き、お客様に安心・信頼してサービスをご利用いただくため、
グループ全体で持続的に情報セキュリティを向上していきます！

もっとつながる。未来が動き出す。

JR西日本グループ