サス鉄ナブル! JFE

『工場のインシデント対応訓練シナリオ』の実践から学ぶ

-制御系SIRTを含む組織内関係者が取り組むべき実務的な訓練とは(JFEスチール取り組み内容)-

2025年02月05日

JFEスチール株式会社　荒木 一匡

自己紹介

氏名　荒木 一匡（あらき かずまさ）
出身　広島県 福山市（現在は岡山県倉敷市在住）
年齢　38歳
専攻　情報処理工学
所属　ＪＦＥスチール(株)西日本製鉄所 倉敷制御部
(兼務)サイバーセキュリティ統括部

OT部門とセキュリティ部門を兼務

職歴

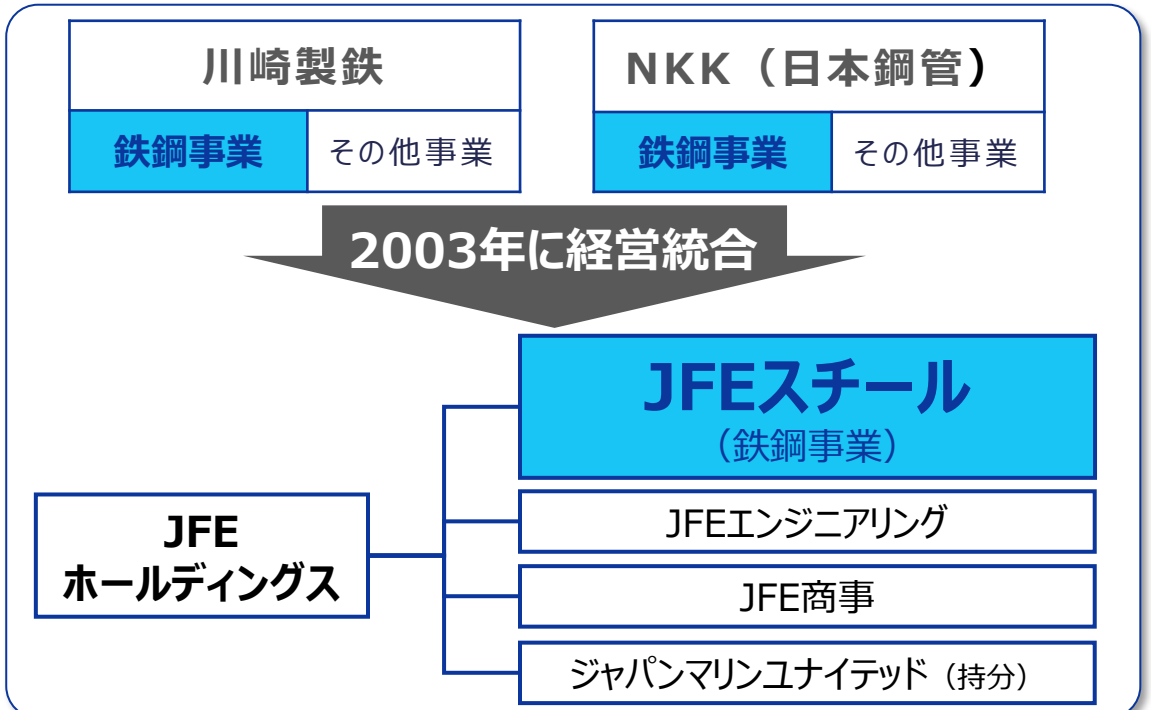
・2009年04月　JFEスチール(株)入社　西日本製鉄所(倉敷地区)制御部 配属。
熱延プロセスのプロセスコンピュータ保全業務、設備工事業務に従事。
・2020年02月　全社制御部門のOTセキュリティWGに参加。
・2021年07月　ICSCoE派遣(5期)にて産業サイバーセキュリティについて学ぶ。
・2022年07月　帰社。全社制御部門のOTセキュリティWGにて対策立案・実行を行う。
・2023年05月　サイバーセキュリティ統括部兼務。

会社紹介：JFEスチールとは

会社概要

名称(商号)　：JFEスチール株式会社
社長　：代表取締役社長　広瀬 政之
本社所在地　：東京都千代田区
従業員数(連結)　：43,081名（2024年3月末）

沿革



生産拠点（国内6カ所）

仙台製造所
・電炉-棒鋼・線材圧延設備を備える

本社
（東京）

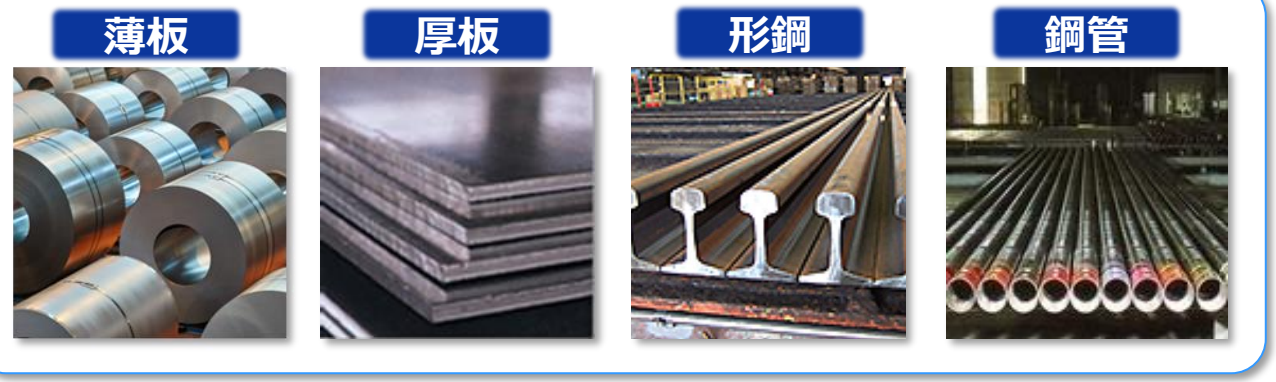
西日本製鉄所（倉敷・福山）
・世界最大級の一貫製鉄所（福山）
・主要製品：薄板、厚板、電磁鋼板、棒線、形鋼

知多製造所
・世界有数の鋼管工場
・鋼管品揃え世界一

東日本製鉄所（千葉・京浜）
・大都市隣接＆高級鋼製造を得意とした製鉄所
・主要製品：薄板、ステンレス、厚板、鉄粉、鋼管

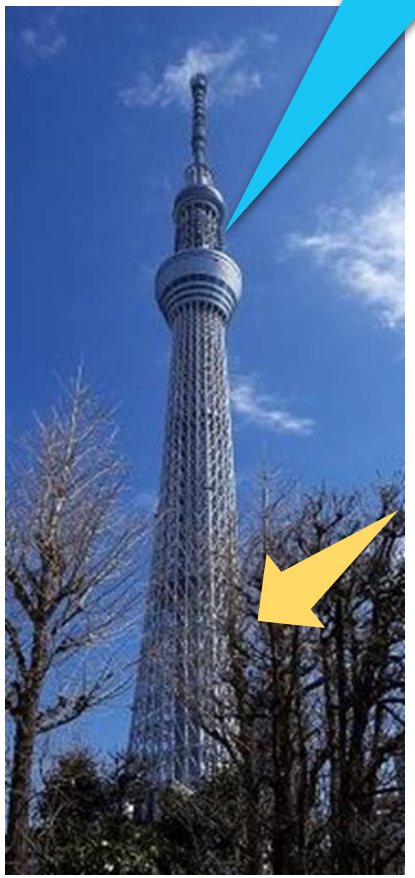
会社紹介：JFEスチールの製品

あらゆる産業の基盤素材として、鉄鋼製品を提供しています。
これら鉄鋼製品をお客様へ安定して供給することが当社のミッションです。



あらゆる産業へ

例えばココにも



脚部

大径極厚鋼管
外径2.3m
板厚10cm

事業主体：東武鉄道㈱
東武タワースカイツリー㈱

出典： 2023年度JFEスチール企業説明資料

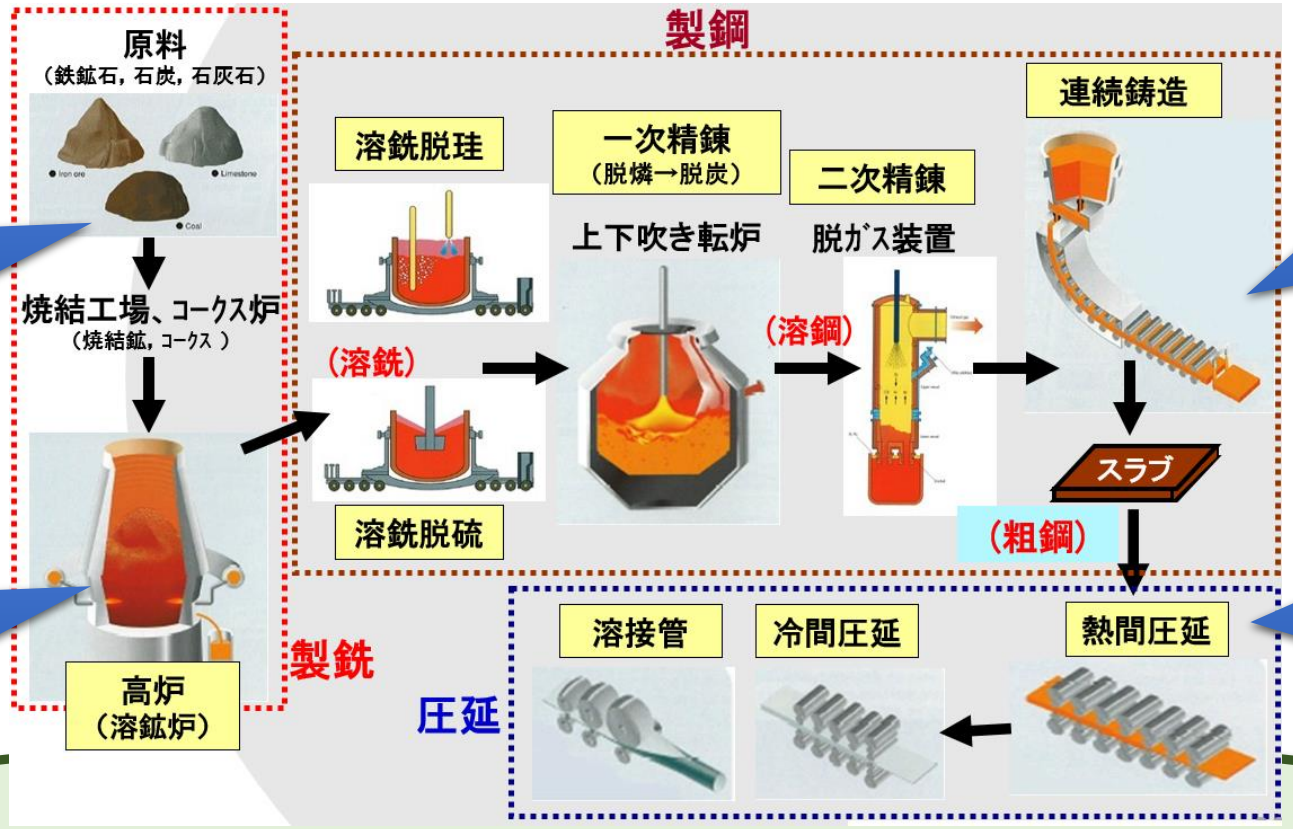
会社紹介：製鉄プロセスの概要

サス鉄ナブル!

鉄鋼の生産現場は大型でダイナミックかつ繊細な製造プロセスを有しています。
これらを実現するのが鉄鋼制御システム≒OTシステムです。

原料溶解
1500℃超

銑鉄量
6,000m³



成分調整精度
ppm
1ppm = 0.0001%

鋼板寸法精度
μm
1μm = 0.001 mm

IoT機器　ローダ/EWS　プロコン　PLC/DCS　センサー　測定機

目次

目次

JFEグループ：サイバーセキュリティガバナンス体制

サス鉄ナブル!

「サイバーセキュリティ経営宣言」のもと、深刻化・巧妙化するサイバー脅威に対し、JFE-SIRTを中心とした経営主導によるサイバーセキュリティ対策強化を推進。

【サイバーセキュリティ経営宣言】

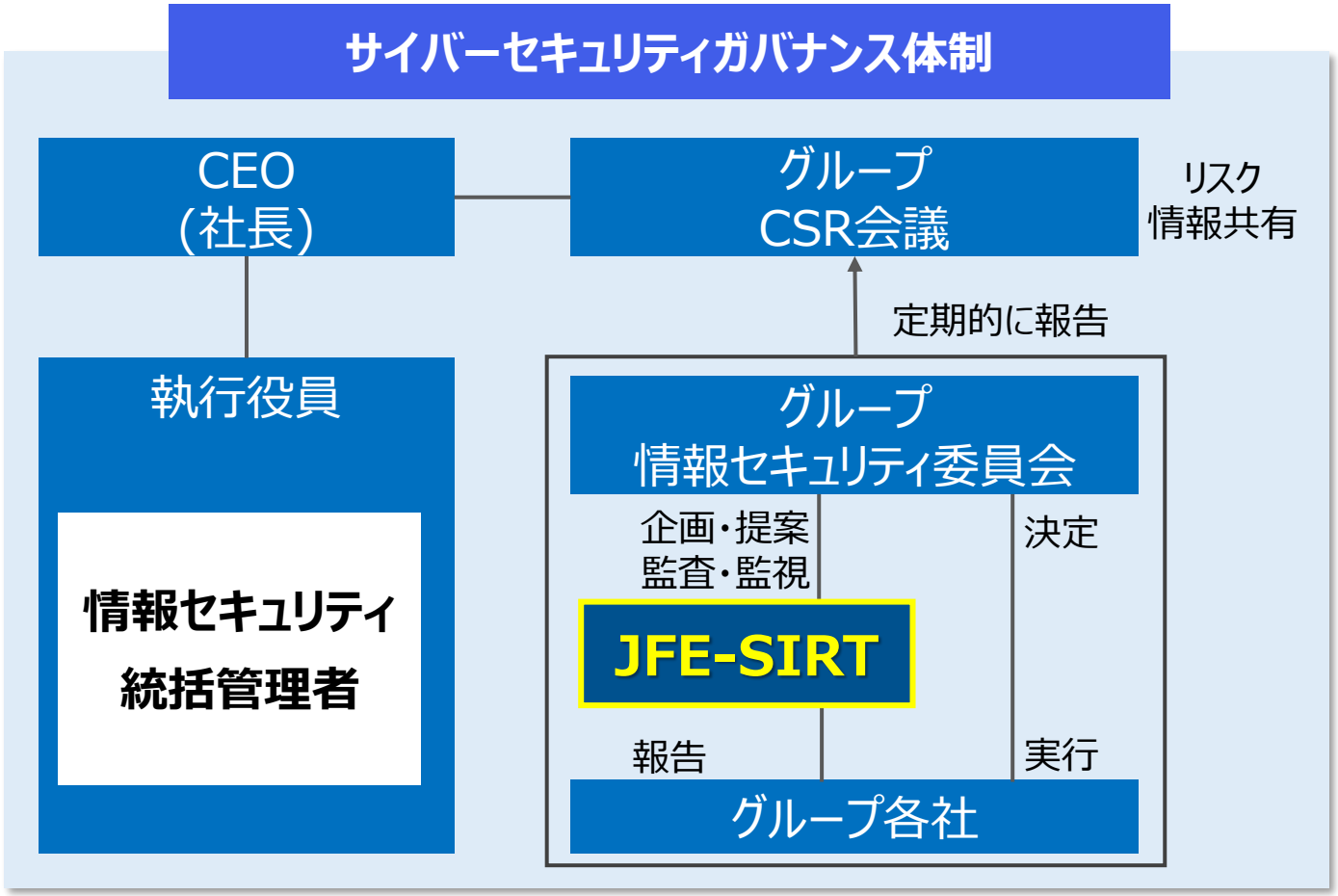
1．経営課題としての認識

2．経営方針の策定と意思表明

3．社内外体制の構築・対策の実施

4．対策を講じた製品・システムやサービスの社会への普及

5．安心・安全なエコシステムの構築への貢献

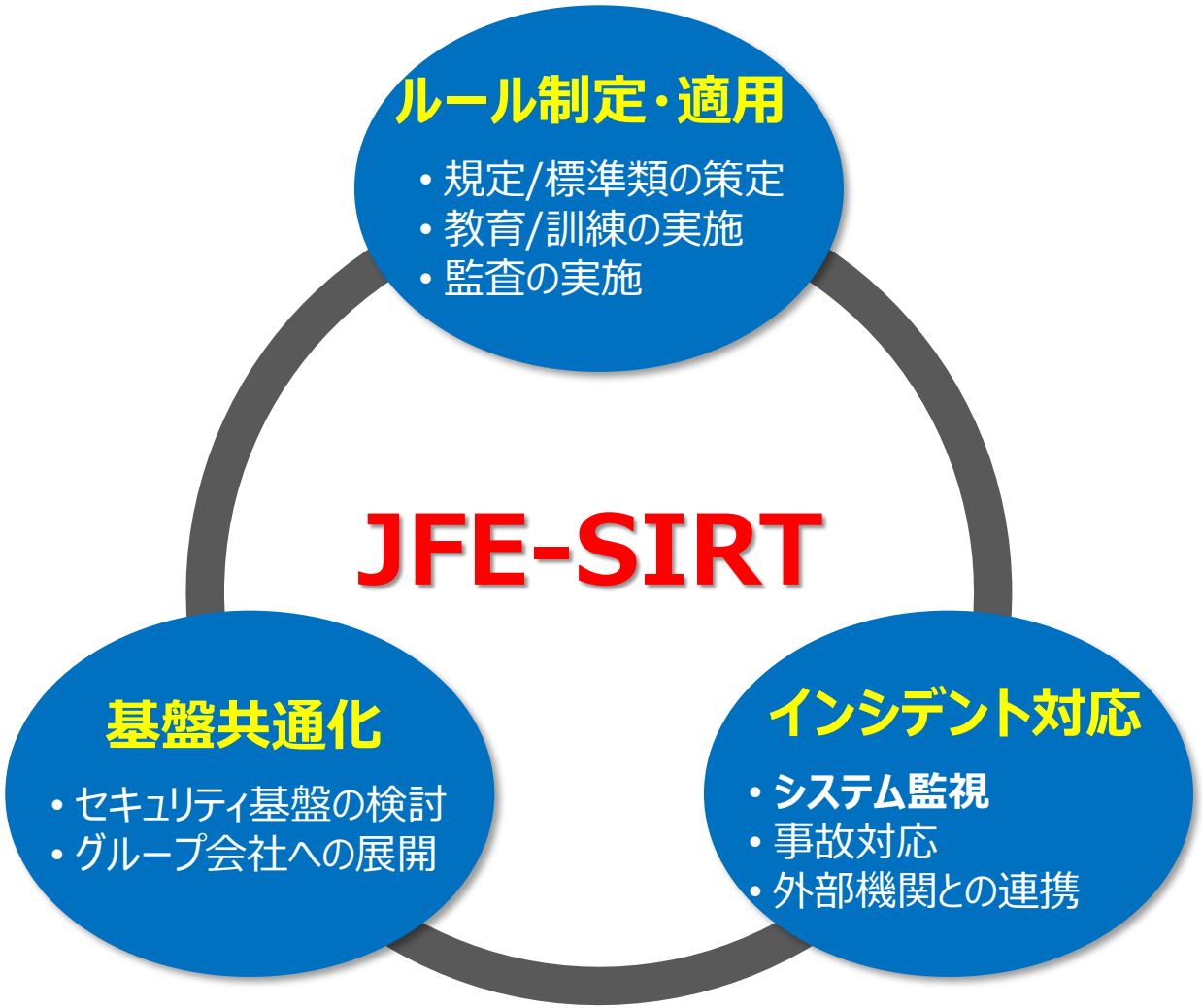


出典：JFEグループ DX戦略説明会 資料

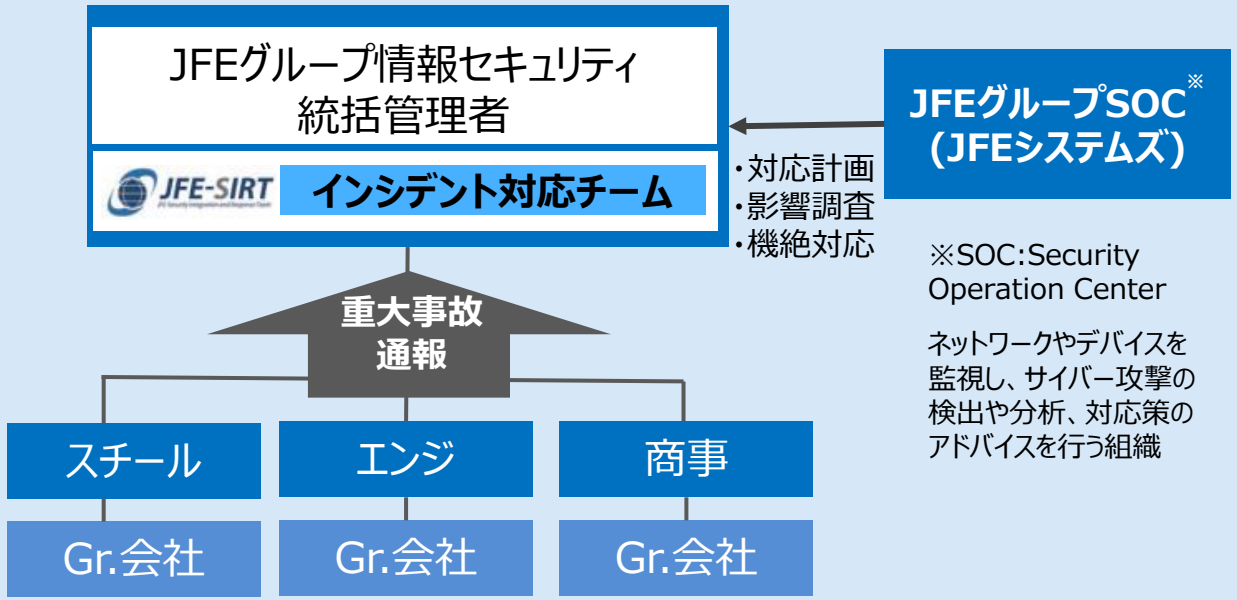
JFEグループ：サイバーセキュリティ管理組織（JFE-SIRT）

サス鉄ナブル!

2016年に業界初のサイバーセキュリティ管理組織(CSIRT)であるJFE-SIRTを設置



システム監視の概要



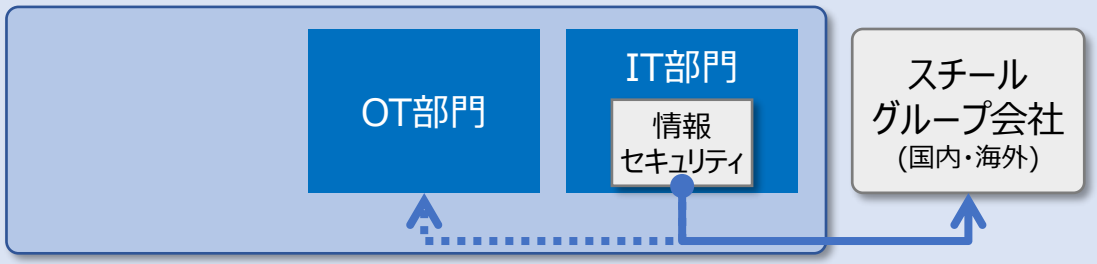
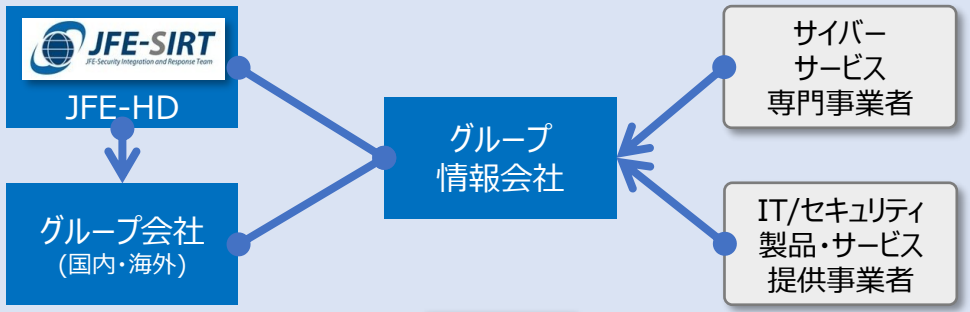
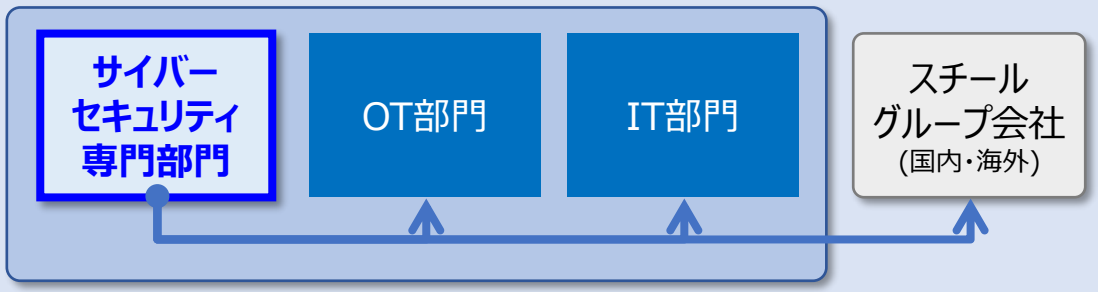
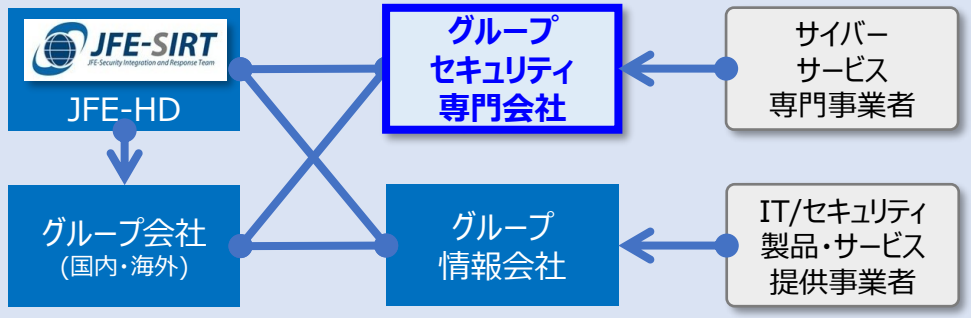
- 国内外の基幹システム・サーバ・端末など、**合計60,000ノードを24時間365日監視**
- 不審挙動や侵入兆候を検出し、**初期対応～封じ込めを実施**

出典：JFEグループ DX戦略説明会 資料

JFEグループ：サイバーセキュリティ体制の変革

サス鉄ナブル!

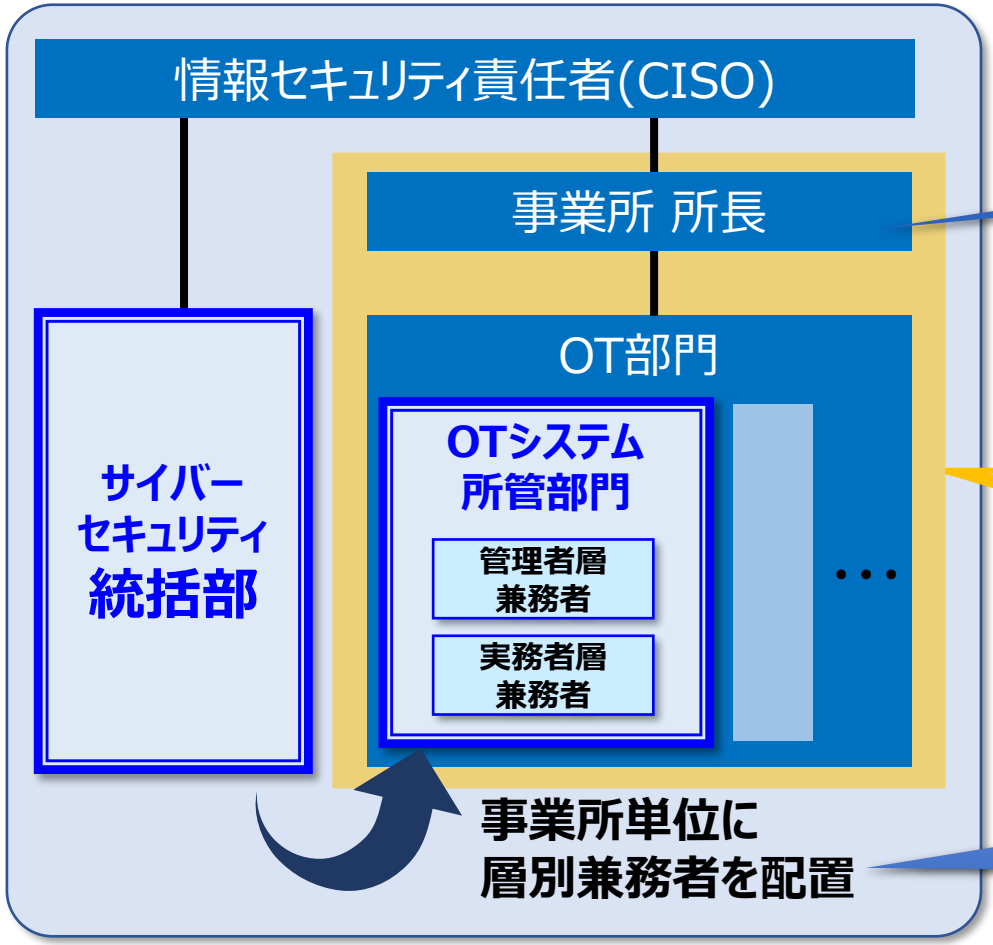
サイバーセキュリティへの対応組織の明確化、持続的な人材確保・育成を狙いとし「サイバーセキュリティ」に軸足を置いた部門・会社を新設

		ＪＦＥスチール	ＪＦＥグループ
変革点		2021年11月　サイバーセキュリティ統括部 新設	2024年4月 JFEサイバーセキュリティ&ソリューションズ 設立
イメージ	従来		
	現在		

JFEスチール：OTセキュリティ推進体制

サス鉄ナブル!

OTセキュリティ推進体制として、事業所長を制御セキュリティ責任者とし
またOTシステム所管部門へサイバーセキュリティ統括部兼務者を配置しています。



Point!
- 事業所長をセキュリティ責任者とすることで事業所単位のセキュリティを推進。

Point!
- 層別に兼務者を配置し対策を推進
- 兼務者向け定例会開催で情報周知

目次

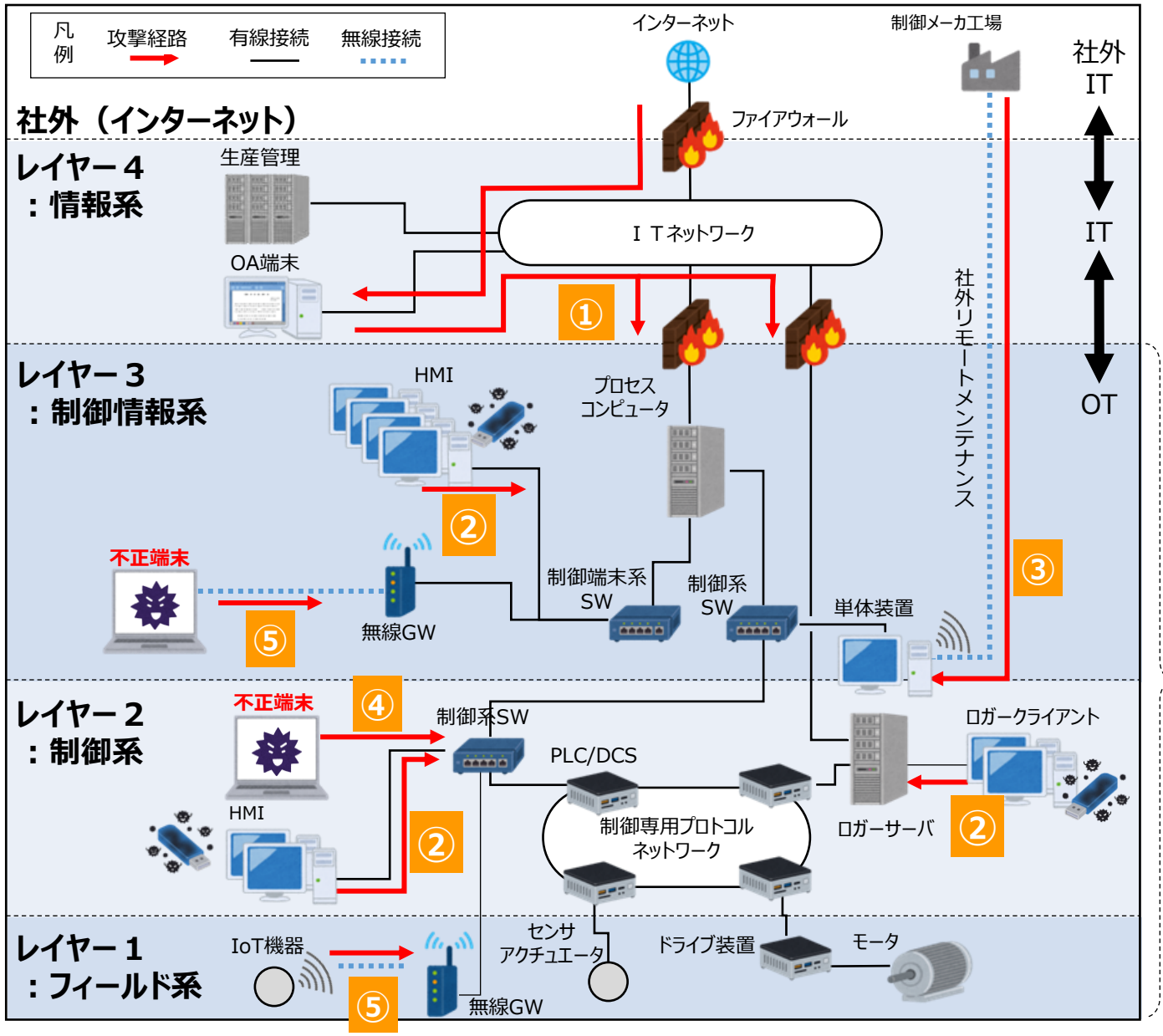
当社OTシステム構成とセキュリティ脅威

サス鉄ナブル!

当社が考えるセキュリティ脅威は大きく5つに分類されると考える。それぞれに対応した対策が必要。

OTセキュリティ脅威

No.	想定脅威
①	IT領域からの不正アクセス
②	端末NWからのウィルス感染
③	外部回線からの不正アクセス
④	物理不正侵入
⑤	無線LANからの不正アクセス



これまでに実施したOTセキュリティ施策 代表例

サス鉄ナブル!

セキュリティ脅威に対し、技術・運用・組織的対策を実施しており、
OTセキュリティIR規定整備やIR訓練についても進めてきました。

分類	項目	状況	詳細
技術的対策	OTセキュリティ強化	導入中 導入中 運用中 検討中	・OT端末対策 ・IT/OT境界へのFW(IDS)導入 ・社内リモートアクセス基盤構築 ・社外接続点に対するセキュリティ対策
	簡易フォレンジックシステム	導入済	・事業部門による簡易フォレンジック対応
	OT資産把握	導入済 検討中	・全社統一した資産管理台帳による資産把握（人力） ・資産見える化
運用・ガバナンス施策	**規程整備・運用**	施行済 運用中	・OTセキュリティインシデント対応規程策定 ・OTセキュリティガイドラインの制定
	審査	運用中 運用中	・OTクラウド利用時の審査 ・OTセキュリティ審査によるリスク抑止
	グループ会社ガバナンス	定期開催	・定期連絡会の開催
	ツール拡充	導入済	・外部記憶媒体検査ツール/USB型検査ツールの拡充
	セキュリティBCP策定	検討中	・OTセキュリティを含めたセキュリティBCP策定
	監査（部門内）	定期開催	・OTシステム所管部門と連携して開催
組織	**OTセキュリティ訓練/演習**	**定期開催**	**・事業部門独自訓練、外部教育設備を用いての演習**
	社内教育	定期開催	・OTセキュリティEラーニング

目次

OTセキュリティ文化定着のための教育

サス鉄ナブル!

OTセキュリティ活動の必要性を広く認識してもらうために、教育活動を重点的に実施。
部門別のeラーニングの開講やインシデント対応訓練・演習等を定期実施しています。

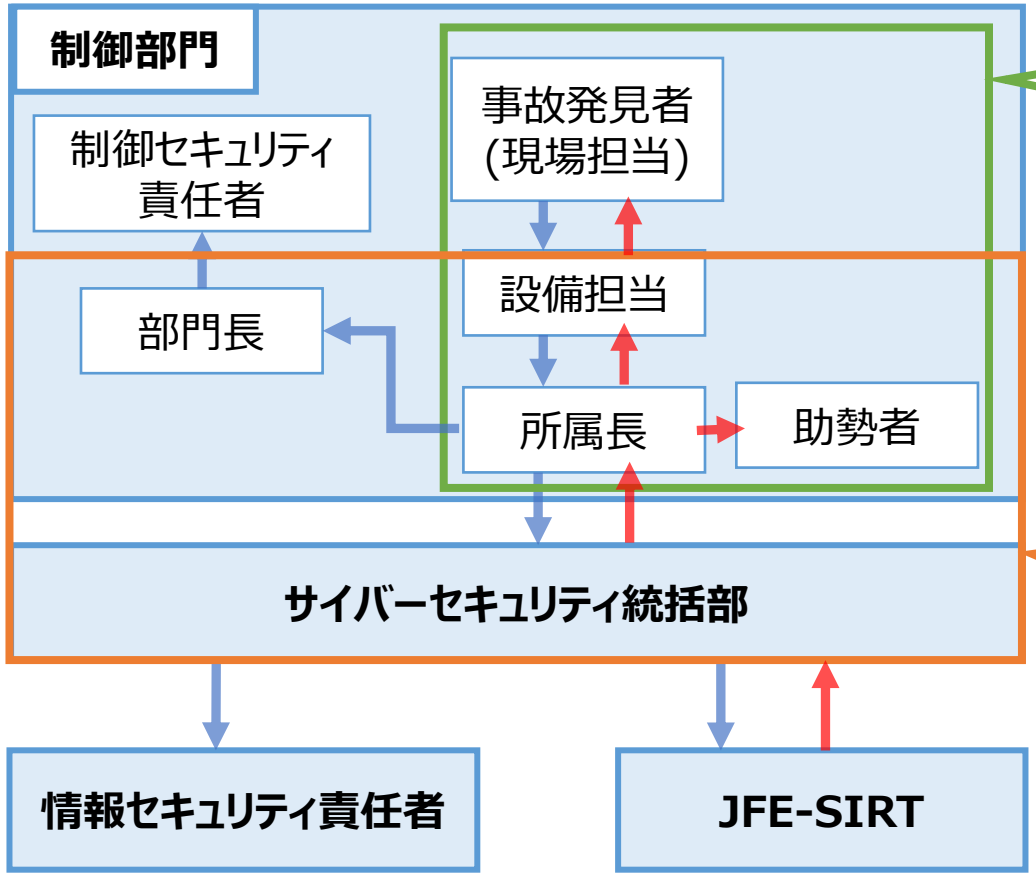
		教育							訓練・演習				
		マネジメント向け研修	経営判断訓練	高度専門研修資格	技術・管理スキル	事故調査・解析	セキュリティ基礎知識	規則ルール	経営判断訓練	部門間連携訓練	部門訓練	メール訓練	可搬型訓練／CTF
経営・管理監督層	幹部・渉外	○	○	–	–	–	–	–	○	–	–	–	–
	管理・監督	○	○	–	–	–	–	–	○	–	–	–	–
セキュリティ従事者	高度	–	–	○	○	○	–	–	–	○	–	–	–
	管理・維持	–	–	–	○	○	–	–	–	○	○	–	○
DS・DX従事者	開発・維持	–	–	–	○	–	○	–	–	○	○	–	–
	サービス外販	–	–	–	○	–	○	–	–	○	○	–	○
従業員	社員	–	–	–	–	–	○	○	–	○	○	○	○
	協力会社	–	–	–	–	–	○	○	–	○	○	○	–

OT領域のセキュリティIR訓練

サス鉄ナブル!

当社ではOT領域へのサイバー攻撃に対するインシデント対応規定を整備。
IR規定の理解促進、部門間の連携能力確認・強化を目的に訓練を実施しています。

□**想定される対応フロー**　青矢印：報告　赤矢印：作業指示



①部門訓練(IR規定理解促進)

【対象者】
・制御部門 設備管理実務者
【訓練形式】
・**机上のウォークスルー訓練**(2～3Hr)
【頻度】
・各部門毎に年1回(2022年～)

②部門間連携訓練(部門間情報連携確認)

【対象者】
・制御部門
・サイバーセキュリティ統括部
【訓練形式】
・外部訓練施設を利用した、実際の状況に近い環境での**Red＆Blueチーム訓練**(3～4Hr)
【頻度】
・年2回(2022年～)

2023年までの部門訓練の実施状況と課題

サス鉄ナブル!

部門訓練による実システムを題材にした机上訓練を実施することにより、
IR規定の理解向上およびセキュリティ対策活動の重要性を再認識できることを確認。
ただし、企画・運営の負荷が高く、現状ペースでは関係者全員が一巡参加するまでに16年程度の期間が必要。

□訓練概要

対象：制御部門 設備管理職場
目的：**IR規定を基に、インシデント発生時の対応事項と報告の流れを確認**
シナリオ：制御端末のランサムウェア感染、
既知のランサムウェアを題材に影響範囲特定や復旧を実施
対象システム：管理している制御システムへの感染を想定
実施時間：約2.5時間
(オープニング・訓練・振り返り)
参加人数：1回の開催で10～20名程度

□訓練後の振り返り(2022年、2023年度抜粋)

・訓練を通して、**機器管理台帳やシステム構成図、バックアップの重要性を再認識**
・有事の際に**訓練同等の行動ができるかは不安が残る**と参加者4割がアンケート回答、**繰り返し訓練の回数を重ねることが重要**と感じる
・**訓練参加職場以外は恐らく対応できない**、見学でも良いので参加者を増やすべき
・**IR規定だけ見てもイメージが湧かなかった、訓練にて対応の流れを見た方が効果的**

**訓練効果はあるが、
制御部門対象者800名強のうち、
2年間で100名と参加率が伸び悩み。
2024年度は訓練を継続実施
するとともに参加者率の向上施策を
検討する必要がある。**

目次

ICSセキュリティ担当者コミュニティ活動-工場IR訓練SWG-

サス鉄ナブル!

JPCERT/CC主催で活動しているICSセキュリティ担当者コミュニティの工場IR訓練SWGにて
日常的に取り組める「工場セキュリティIR訓練シナリオ素材」を2023年度に作成。
2024年度は作成したシナリオを活用して、現場での訓練を実施。実施結果から「課題」や「改善ポイント」の知見を得る。

シナリオNo.	シナリオ概要
1	IT部門が把握していない外部との通信経路からマルウェア感染
2	生産設備システムのFUアップデートにてNW輻輳が発生
3	不審なUSBメモリからのマルウェア感染
4	VPNリモート保守環境からの不正アクセスによる生産設備停止
5	クラウド接続点からランサムウェア感染、生産設備停止

引用：制御システムセキュリティカンファレンス2024　株式会社資生堂講演資料 「製造業10社の実務者で議論した、制御系SIRTが日常で取り組みたいインシデント対応訓練」

2024年									2025年		
4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
	SWG活動継続決定		訓練参加組織募集		各社(8組織)訓練準備・実施						
			訓練評価チェックリスト作成				各社評価回答・結果まとめ				
		オンラインMTG(1回)	オンラインMTG(2回)	オンラインMTG(2回)	オンラインMTG(2回)	オンラインMTG(2回)	オンラインMTG(2回)	オンラインMTG(3回)	オンラインMTG(1回)	制御システムセキュリティカンファレンス2025	

2024年度から ICSセキュリティ担当コミュニティの工場IR訓練SWGにJFEスチールも参加。

SWG訓練シナリオを活用した訓練の実践

サス鉄ナブル!

当社の2024年度訓練に、SWGにて作成した日常的に取り組める訓練コンテンツを採用。
全制御部門担当者向けにIR訓練を計画・実施。全事業所で合計813名の制御部門担当者が訓練参加。

QC(QualityControl)サークル活動(※)：現場の社員グループで自主的に運営を行い、品質管理や業務改善を行う小集団改善活動

□訓練概要

対象者：全事業所 制御部門 設備管理職場
QCサークル活動(※)と同じ小集団単位で訓練開催
ファシリテータは職場管理者にて実施
シナリオ：制御端末のランサムウェア感染
(シナリオ素材No.5のランサムウェア感染被害を選択)
対象システム：仮想の制御系モデルシステムを想定
実施時間：約1時間
(オープニング・訓練・振り返り)

あなたはとある工場の保全業務を担う制御部員です。
工場のオペレータから、「見慣れない赤い警告画面が表示されており画面の操作を受け付けない」との連絡を受けました。

この時点で、あなたは何を実施しますか？
（10分検討）

□訓練計画・実行スケジュール

	24/9	/10	/11	/12	25/1
訓練資料作成	■				
ファシリテータ説明会		★ 欠席者には説明会動画配信			
訓練実施		■	■		
評価アンケート		■	■	★ 全事業所の結果まとめ	

70グループ、
計813名が訓練に参加

SWG訓練シナリオを活用した当社の訓練結果

サス鉄ナブル!

所属企業向けにシナリオのカスタマイズは必要であるが、
事前のシナリオ検討や資料作成の作業負荷が大きく軽減

IR規定の理解向上＋
セキュリティ対策活動の重要性を再認識

外部機関連携について、社内で確認するきっかけとなった。
窓口は誰なのか？どのような目的・条件で外部連携するのか？

その他、参加企業の訓練評価については
JPCERT/CCによる分析結果で紹介

サス鉄ナブル!

JFE

本講演の内容につきましては、正確な記述、表現となるよう努めておりますが、その情報の正確性、完全性を保証するものではありません。本講演および資料に基づく結果について、JFEスチール株式会社および講演者は一切の責任を負いかねますのでご了承ください。