OTセキュリティ実装のリアル
― 技術・組織・文化の交差点で起きたこと

日本精工株式会社　加澤　靖

2026年4月24日

自己紹介

自己紹介

名前	加澤　靖（Kazawa Yasushi）
所属/役割	日本精工株式会社　デジタル変革本部　デジタルトラスト・セキュリティ部　部長
資格	CISSP,　CISA,CISM,情報処理安全確保支援士, システム監査技術者, 情報セキュリティ監査人補,ITストラテジスト

NSKでの経歴

- 2007年 中途入社。海外のサプライチェーン/生産システム導入を担当。要件定義・設計・インフラ設計、プログラム開発等。
- 2014年 デジタル化推進/スマートファクトリー化推進組織にて、企画、PoC、ガバナンス、セキュリティ対応
- 2019年 セキュリティ推進組織に異動。CSIRT（インシデント対応体制）を立ち上げ、各種セキュリティ強化の企画、実行、デジタル化推進を担当

近影

活動方針

サプライチェーン、DX、セキュリティのスペシャリストとして、ビジネスと社会の変革を支え、貢献する。

中国工場立ち上げ時

中国工場(現在)

新華社. “中国のイノベーションに融合　日本精工が合肥で歩む共創の道”
https://jp.news.cn/20250817/0ecac3fcd8f24d5ca441cb70331007da/c.html

会社紹介

会社概要

■会社名	日本精工株式会社(NSK Ltd.)	
■証券コード	6471 東京証券取引所プライム市場	
■創立	1916年(大正5年)11月8日	
■資本金	672億円	(2025年3月末)
■売上高	7,967億円	(2025年3月期)
■営業利益	285億円	(2025年3月期)
■子会社数	77社	(2025年3月末)
■従業員数	24,057名	(2025年3月末)

本社ビル
（品川区大崎）

代表執行役社長･CEO　市井 明俊

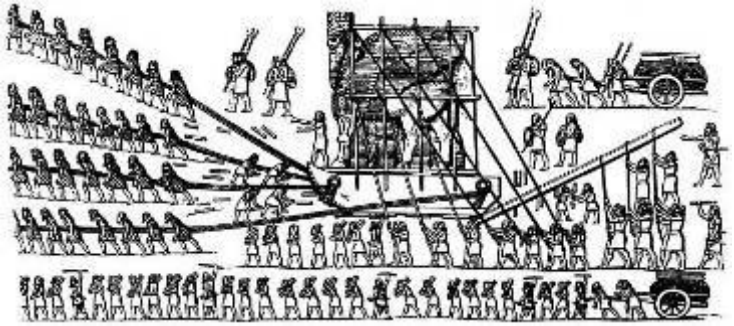
＜企業理念＞
NSKは、MOTION ＆ CONTROL™を通じ、
円滑で安全な社会に貢献し、
地球環境の保全をめざすとともに、
グローバルな活動によって、
国を超えた人と人の結びつきを強めます。

日本最初の軸受（ベアリング）メーカー / 軸受シェア 日本第１位　世界第３位

軸受とは – 軸受の種類と構造 -

ベアリング（軸受）とは、

- **回転部分の摩擦を軽減・コントロール**し、スムーズな動きを支える機械要素部品
- 原理は、紀元前7世紀アッシリアの**巨大な石像の運搬用丸太**
- 15世紀に**レオナルド・ダ・ヴィンチ**が現在の軸受に近い基本構造を考案



■種類

・転がり

ボールベアリング

ローラーベアリング

■構成部品

ボールベアリング（完成品）

外輪

転動体（ボール）

保持器

内輪

軸受とは –軸受の用途 -

軸受は私たちの身のまわりで幅広く使われ、人々の暮らしを支えています

自動車

鉄道車両

写真提供：東海旅客鉄道株式会社

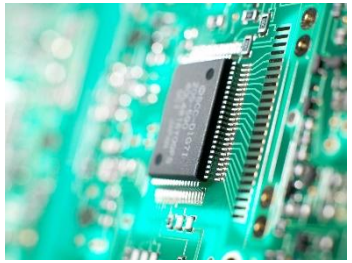
鉄鋼設備

風力発電機

掃除機

洗濯機

半導体製造装置



航空機

ドローン

データセンター

人工衛星

工作機械

ロボット

会社概要 – グローバルに広がる生産拠点 -

グローバルに生産拠点85拠点、200以上の事業拠点を展開

（2025年3月末日時点）

※拠点数には持分法適用会社含む

アイスブレイク
-歴史から学ぶ工場セキュリティの重要性-

本日お話する内容

1. セキュリティ組織紹介
2. 工場セキュリティ組織（FSIRT）の具体的な活動紹介
3. 今後の課題
4. まとめ

１．セキュリティ組織紹介

情報セキュリティマネジメントの取り組み（公開版）

情報セキュリティマネジメント | 日本精工 (NSK)

NSK 製品情報 カタログ 技術情報・支援ツール 産業別情報 企業情報 採用情報 お問い合わせ 日本

ホーム > 企業情報 > サステナビリティ情報 > リスクマネジメント > 情報セキュリティマネジメント

情報セキュリティマネジメント

基本的な考え方 体制 目標と実績 取り組み

インシデント対応力の向上

情報機器やネットワーク通信などにおける不審な動きや、セキュリティの脅威を把握する技術的施策の推進、検知したインシデント情報を分析し対策を講じるセキュリティオペレーションセンター※1による対応など、迅速なインシデント対応を可能にする仕組みを構築しています。加えて、セキュリティレーティングサービス※2やアタックサーフェスマネジメント（ASM）※3を運用し、NSKグループ全体に影響を及ぼす脆弱性のモニタリングを実施しています。
また、近年のセキュリティインシデントによるサプライチェーンへの大きな影響を鑑み、取引先への情報セキュリティ点検を実施し、セキュリティレベルの向上に向けて取り組んでいます。
自社においても、工場のインシデント対応体制を強化し、ITだけでなく、OT領域※4のインシデントにも対応できるよう取り組みを進めています。

※1 セキュリティオペレーションセンター：サイバー攻撃の検知や分析を行い、対策を講じる専門組織
※2 セキュリティレーティングサービス：企業のセキュリティ対策状況を数値化し、外部や内部でのリスク評価や対策に役立てることができるサービス
※3 アタックサーフェスマネジメント：組織の外部（インターネット）からアクセス可能なIT資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスのこと
※4 OT（オペレーショナルテクノロジー）：工場等の制御システムのこと。ITは情報を取り扱うのに対し、OTは物理環境と相互作用する点が特徴的とされる

自社においても、工場のインシデント対応体制を強化し、ITだけでなく、OT領域のインシデントにも対応できるよう取り組みを進めています。

FSIRT体制

FSIRT発足当初は、各工場の生産技術部門・品質保証部門・工場IT部門をメンバーを選出したが、工場のFSIRT活動状況に併せて総務部門や製造部門もメンバーに追加されている。また、事務局と各工場のFSIRTメンバーで定期的にミーティングを実施し、コミュニケーションを取っている。

3．FSIRTの具体的な活動紹介

FSIRT活動概要サマリー

FSIRT発足当初に比べ、工場セキュリティは強化されてきてはいるが、まだ道半ばといった状況。

2021年～

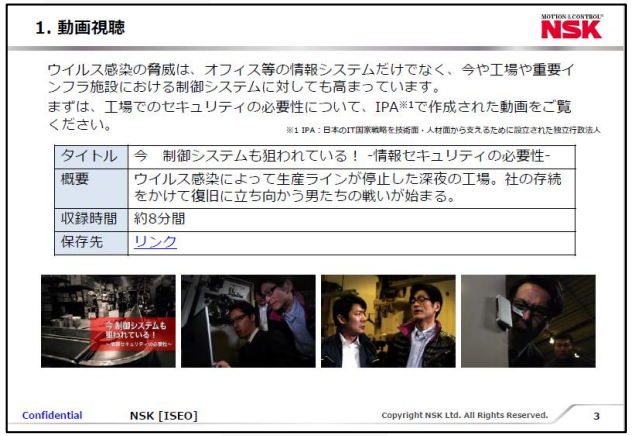
要素	FSIRT発足当初の状況	これまでの活動	成果(現状)	課題
人 (People)	工場作業者や工場担当者がセキュリティ強化方法を分からない。	・連絡体制整備 ・FSIRTミーティング ・セキュリティ教育	平常時のセキュリティ強化やインシデント発生時の対応体制が構築されている。一部の工場作業者や工場担当者に定期的に教育している。	・工場作業者や工場担当者の自分事化が出来ていない ・工場全体へのセキュリティ知識の強化不足
プロセス (Process)	インシデントが起きてから対応する。	・リスクアセスメント ・インシデント対応訓練 ・PC/USBメモリ接続対策 ・脆弱性対応	情報セキュリティ部門からの指示により、簡単な対処や予防対応を実施できる。	・役割分担・運用フローの明確化が不十分 ・工場で自主運用するレベルに至らず
技術 (Technology)	工場資産が把握出来ていない。不審な通信や動きを把握していない。	・資産管理 ・バックアップ対応 ・EDR導入	工場資産やリスクを把握している。 不審な通信や動きが検知できる。	・古い資産への監視が不十分 ・工場の新たな技術活用にセキュリティリスク対応が追従せず

セキュリティ教育

工場設備に関わる人を中心に、定期的にセキュリティ教育を実施

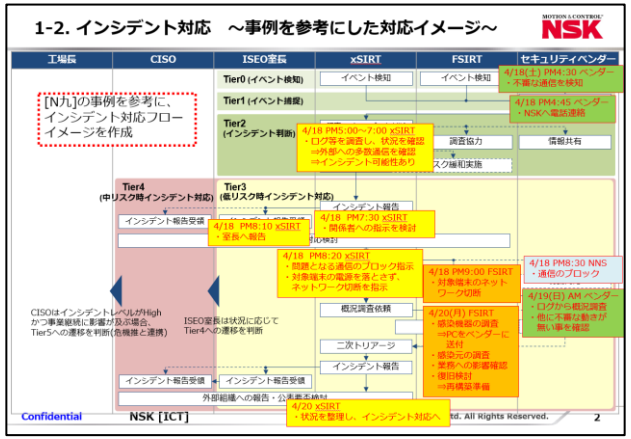
	一般向け教育	担当者向け教育
目的	・工場セキュリティの脅威の理解 ・今後のセキュリティ強化活動の理解	・インシデント対応フローの理解 ・インシデント事例対応の共有
時期	定期的(年1回)に実施	FSIRTミーティングの中で随時説明
対象者	生産技術、品証保障を中心	FSIRTメンバー
形式	資料配布、動画視聴、アンケート	説明、Q&A
内容例	・インシデント事例紹介 ・今後の活動予定紹介 ・動画視聴	・インシデント発生時の対応フローの説明 ・インシデント事例対応紹介

一般向け教育(動画視聴)



一般向け教育(事例紹介)

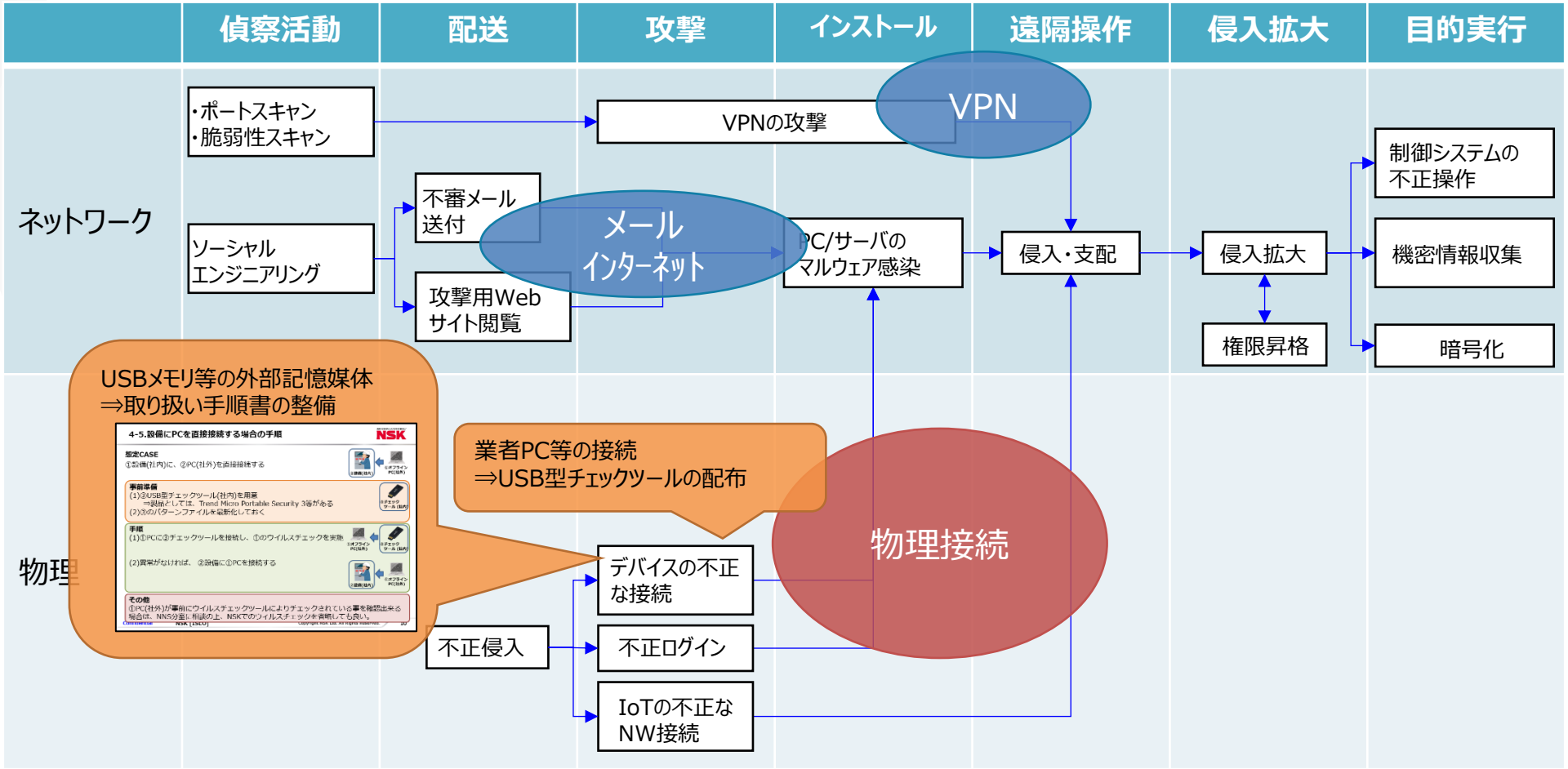
担当者向け教育(対応フロー説明)



PC/USBメモリ接続対策

工場で発生するインシデントの原因となりやすい物理接続に対し、外部記憶媒体の取扱い手順書の整備や、業者PC等のスキャンやマルウェア駆除するためのUSB型チェックツールの工場配布を実施。

工場における攻撃手段



バックアップ対応

工程管理上、ボトルネックとなるような機器を把握する為、生産への影響や、感染し易さ(OSやネットワーク)について、各機器を調査。調査結果から、対応の優先度を設定し、バックアップが取られていない機器への取り組みを進めていく。

生産への影響 (影響が高い機器ほど優先的に対応する必要あり)	**OS** (Windows系の方が感染し易い)	**ネットワーク** (範囲が広い方が感染し易い)	**対象イメージ**	**優先度**
高い	Win系	NSKネットワーク	帳票サーバ、工作機械、測定器	高
		ローカルネットワーク	測定器、検査機	高
		オフライン	測定器、検査機	高
	Win系以外	NSKネットワーク	PLC、プリンター、NW機器	高
		ローカルネットワーク		中
		オフライン		中
低い	Win系	NSKネットワーク	デジタルサイネージ	低
		ローカルネットワーク		低
		オフライン		低
	Win系以外	NSKネットワーク	電子錠、放送設備	低
		ローカルネットワーク		低
		オフライン		低

3．今後の課題

FSIRT活動から見えてきた新たな課題

数年の活動の成果もあり、十分ではないものの自分事になりつつある。意識が高まったことによる課題も出てきた。

工場側から見ると工場内のOA領域のITセキュリティと現場のOTセキュリティを区別していない

ITセキュリティとOTセキュリティは両輪で対応を進めていく必要がある

工場長が気にするのは？

訓練対象を係長やスタッフ等にも拡大したいとの要望

工場全体へ役割に応じたインシデント対応訓練や教育を実施していく必要がある

訓練は効果あり。工数は？

SCS評価制度における“製造環境等”のセキュリティ対策

SCS評価制度ではOTセキュリティはネットワークの分離などを前提とし、対象外とされている。会社としてのSCS評価制度の対応とは別に“工場セキュリティ”の取り組みを進める。

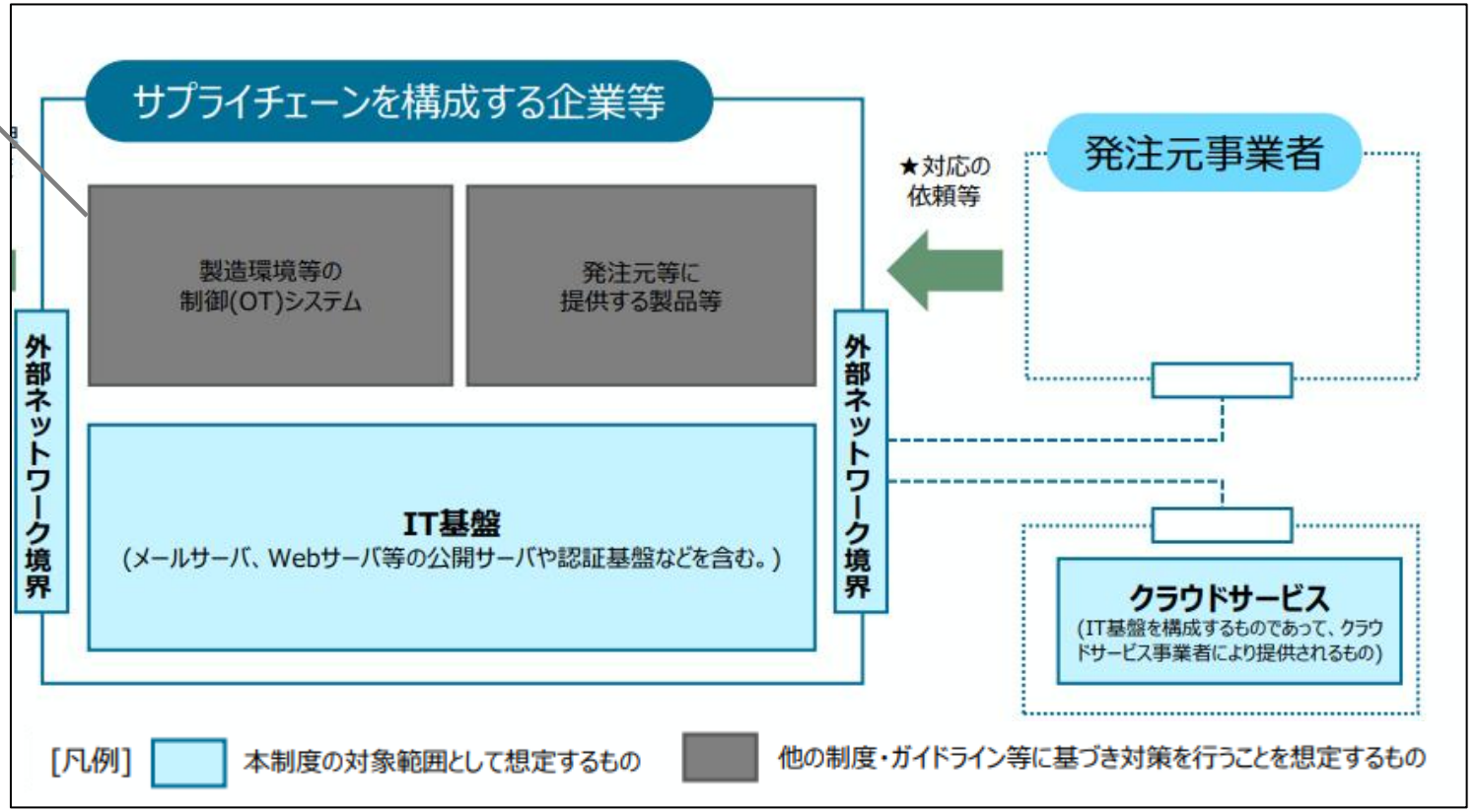
製造環境等の制御（OT）システムは対象外

- 求められる対応が基本的に異なることから直接の対象とせず、他のガイドラインを参照
- IT基盤と接続する場合、ネットワーク機器など（例：VLAN,ファイアウォール）により適用範囲内外の通信を必要最小限にすることが条件

“工場セキュリティ”はどこまで対象か？

- ネットワーク構成による
- OTの定義は自身で決めてよい

SCS評価制度の対象範囲



経産省「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」（令和８年３月）
https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf

４．まとめ

まとめ -得られた知見-

- 工場のスマート化・デジタル化
- IT組織とOT組織の連携
- 工場の立場の理解
  - 工場ごと、製品の違い

画像引用 Unsplash
https://unsplash.com/ja/%E5%86%99%E7%9C%9F/%E6%9C%A8%E8%A3%BD%E3%81%AE%E3%83%86%E3%83%BC%E3%83%96%E3%83%AB%E3%81%AE%E4%B8%8A%E3%81%A7%E6%8F%A1%E6%89%8B%E3%81%99%E3%82%8B%E4%BA%8C%E4%BA%BA-NzIV4vOBA7s?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash

MOTION & CONTROL™
NSK

NSKの企業理念

NSKは、MOTION & CONTROL™ を通じ、
円滑で安全な社会に貢献し、
地球環境の保全をめざすとともに、グローバルな活動によって、
国を越えた人と人の結びつきを強めます。