

製造業における CSIRT/PSIRT/FSIRTの組織形態に応じた構築手法 Starting guide of CSIRT/PSIRT/FSIRT in manufacturing industry according to organization structure 福井雄也・マネジメント分科会・情報セキュリティ大学院大学 For CSIRT/ PSIRT/FSIRT/FSIRT in the manufacturing industry, indicate whether the functions and departments are related based on the manufacturing sector

課題と成果

製造業でセキュリティ対応組織の重要性が高まっている。
既存の構築ガイド資料において、

- ・課題1 CSIRT/PSIRT/FSIRTが担う機能と組織部門の関係がわからない
そもそも、製造業で必要となるFSIRTが担う機能について述べられていない
- ・課題2 CSIRT/PSIRT/FSIRTが担う機能毎に組織部門間の時系列の流れについてわからないため、組織立上げ時、訓練などでインシデント時の動きなどが時系列で理解できない
- ・課題3 1社単独かグループ会社など複数社で形成するのか、事業所の数などの企業形態を考慮できていないため、工場などの拠点がある場合に対応できない
- ・課題4 CSIRT/PSIRT/FSIRTの役割の機能で共通化できる箇所を判断し、組織全体で効率化の図り方がわからないため、コストを抑え方がわからない

製造業でセキュリティ対応組織の新たな構築ガイド資料として提案

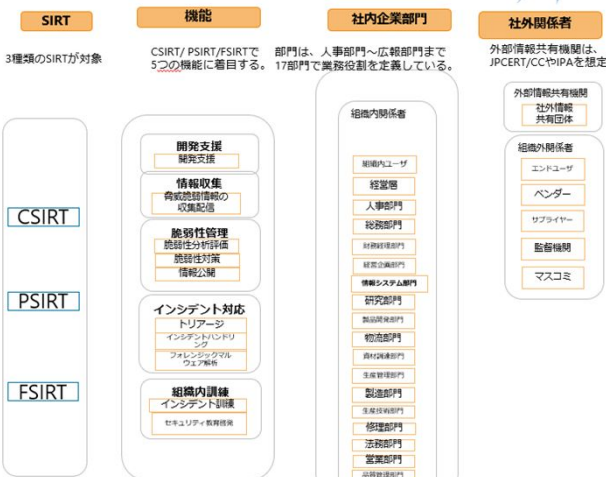
- ・CSIRT/PSIRT/FSIRTが担う機能について、製造業の組織内部で機能を主に担う部門、協力する部門の関係性を示したガイド資料
- ・CSIRT/PSIRT/FSIRTのインシデント事例に基づいて、インシデント時の部門間の動きなどが理解でき、組織立上げ時、訓練等に利用できるガイド資料

セキュリティ対応組織の概要

- CSIRT(Computer Security Incident Response Team) ITセキュリティに関わるインシデントに対処するための組織である。
- PSIRT(Product Security Incident Response Team) 自社製品に関わるインシデントに対処するための組織である。
- FSIRT(Factory Security Incident Response Team) 工場設備などの安定稼働を脅かす外的脅威への対応をする組織である。

研究で取り扱った要素

研究の要素として、CSIRT/ PSIRT/FSIRTについて、機能と製造業で一般的な社内企業部門を定め、社外関係者との要素を取り扱い研究を行った。



参考:2020年度成果報告書 戦略的イノベーション創進プログラム(SIP)第2期/10T社会に対応したサイバー・フィジカル・セキュリティ/10T社会に対応したサイバー・フィジカル・セキュリティに係るOSSの技術検証、CSIRT・PSIRT連携等に関する調査

機能と組織部門の関係の分析

製造業で想定される部門に対して、セキュリティ対応組織(CSIRT/ PSIRT/FSIRT)の機能と部門との関係の分析を行った。これらの成果を構築時の新たなガイド資料として提案

機能	CSIRT				PSIRT				FSIRT				
	関係	関係	関係	関係	関係	関係	関係	関係	関係	関係	関係	関係	関係
開発支援													
情報収集													
脆弱性管理													
インシデント対応													
組織内訓練													