The project members raised operational challenges and discussed potential countermeasures based on their respective business experiences; therefore, they shared actionable approaches for issues and solutions for OT-SOC operations. By going beyond theoretical discussions, we experientially validated scenarios in the simulated environments, making our deliverables more practical and applicable to real-world operations. By going beyond theoretical discussions, we experientially validated scenarios in the simulated environment and produced more practical and applicable deliverables to real-world operations.

Our final deliverable is a document designed to help OT-SOC implementation teams easily understand the key issues and decision-making points they may face at each stage of the lifecycle. The document is designed as a reference for guiding the implementation process, supporting project members in facilitating discussions and deliberations with internal stakeholders within their respective dispatching organizations.
In particular, the document features visually accessible tables and flowcharts, enabling practitioners to efficiently structure discussion points even under time constraints.

Interview with a graduate

Mr. TAKAHASHI Masaru

What is your utmost benefit from this project?

The most valuable outcome of this project was clarifying previously vague approaches to OT-SOC implementation and operational challenges through company interviews and validations in the simulated real plants, allowing the project members to gain practical insights to directly apply to advancing OT-SOC initiatives within their respective organizations.
In particular, having prior knowledge of critical considerations, common pitfalls, and operational best practices is anticipated to contribute to improving the overall quality of OT-SOC initiatives.
Furthermore, the project helped compile and compare multiple OT-SOC models along with their respective advantages and disadvantages, providing a helpful reference for organizations when considering the most suitable model for their environments.

Methods for utilizing project outcomes

The project deliverables are intended for use by personnel responsible for considering and implementing OT-SOCs within our dispatching organizations.
They can be used as a reference when identifying key challenges and considerations encountered at each stage of the OT-SOC lifecycle, from implementation through operation.
In particular, the materials are helpful for facilitating discussions with internal stakeholders and establishing a foundation for the implementation processes.

This is unique to the ICSCoE

The most distinctive aspects of the ICSCoE are the discussions among the project members from diverse backgrounds, hands-on learning environments, and professional guidance from instructors.
The project brought together members from various industries including both IT experts and practitioners primarily focused on OT.
This diversity enabled us to have balanced and unbiased productive discussions and outcomes by respecting both domains' priorities: confidentiality and availability in IT, safety and reliability in OT.
In addition, our instructors provided us with technical expertise in OT network monitoring, which enriched participants' understanding.
The support and introductions provided by the instructors enabled the members to conduct corporate interviews with a wide range of organizations, including OT-SOC operating companies, managed security service providers, and solution vendors, gaining direct insights from each perspective.
Alongside the scenario validations using the simulated real plants, I believe that gaining such valuable opportunities for learning and connections was one of the utmost benefits that only the ICSCoE could offer.

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Bunkyo Green Court Center Office,
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591
TEL 03-5978-7554 FAX 03-5978-7513

R60 古紙パルプ配合率60%再生紙を使用
リサイクル適性Ⓐ
この印刷物は、印刷用の紙へリサイクルできます。

IPA Better Life with IT

ICSCoE REPORT
Industrial Cyber Security Center of Excellence
10.24.2025
vol. 24

The ICSCoE Report is a public relations newsletter on ICSCoE's activities.

8th Core Human Resource Development Program Introducing Activities of Our Final Projects Part2

Perceiving Careers in the Security Field Through Games

Backgrounds and Issues

Facing the shortage of cybersecurity professionals, many enterprises face a reality where a certain number of employees have been assigned to the security department without the knowledge or experience of information technologies.
On the other hand, many tasks in security departments are highly specialized and require a solid foundation of IT knowledge, making it difficult for beginners to perceive the nature of duties.

The project team set the objective to create enjoyable content that allows users to perceive the nature of security duties without IT experience, based on the above circumstances.

Issue-solving & Outcomes

The team prepared two types of content based on steps as their outcomes: A List of Security Duty Examples to recognize duties, and Three Games to perceive the nature of duties.

Content 'to Recognize Security Duties'

Created a list of representative security duty examples

Content 'to Perceive Security Duties'

Produced 3 games to perceive the nature of security duties

Security Strategy Boad Game

Forensic Examination Board Game

Security Operations Simulation Game

— A list of Security Duties —

"A List of Security Duty Examples" identifies typical security duties and summarizes them on a single page (A3 size) in both an overview and a detailed version. The front paper provides explanations accessible to beginners without requiring specialized knowledge, while the back page clarifies more details of professional duties.

― Security Strategy Board Game: Ready to Secure? ―

This board game aims to provide players with the experience of developing security strategies. It is a cooperative game for three to five players, in which participants discuss and formulate strategies to maximize profit. If players solely focus on profit, incidents might occur that significantly reduce acquired assets, and in the worst case, might result in bankruptcy. In this game, therefore, players choose their actions b y balancing profit-seeking and security while considering the risk profiles of their enterprises.

― Forensic Examination Board Game: Become a Forensist! ―

This board game aims to provide players with the experience of examining security forensics. It is a cooperative game for three to five players, in which participants explore the full extent of incidents accurately and promptly. In this game, players analyze simplified logs to detect suspicious activities and verify consistency with information gathered from interviews with relevant parties, aiming to elucidate entire incidents.

― Security Operations Simulation Game: Singularity ―

This simulation game aims to provide players with the experience of security operations through on-the-job training (OJT). This game allows users to play individually on a PC, progressing by choosing appropriate duties in quizzes presented throughout the game. This game features the duties of normal operations and incident occurrence, allowing users to grasp the big picture of duties while playing.

Interview with a graduate

Mr. WATANABE Kodai
2nd from the right in the front row

What is your utmost benefit from this project?

The ultimate benefit from our final project is to organize and model security operations. When identifying security duties, we re-acknowledged that security is a broad and highly specialized field.

In gamifying these duties, we distinguished between 'tasks' and 'values,' with the intention of modeling not merely the performance of tasks but the experience of actions generating values. Therefore, I believe the members gained a wide-ranging understanding of the critical elements of security operations.

Methods for utilizing project outcomes

Users will effectively utilize our outcomes to recognize the security duties involved. Enterprises can apply them to workshops for student internships and new employees or as a tool for non-security staff to understand security-related tasks.

Our project outcomes are enjoyable security-learning games; thus, enterprises can utilize them to foster communication and interactions within security departments.

This is unique to the ICSCoE!

I believe that this project enabled us to tackle shared challenges across industries. By exchanging ideas with colleagues from various sectors, including automotive, energy, defense, and financial services, we produced exploitable outcomes that are not specific to any industry.

Additionally, the project team held game experience sessions for the general public and exhibited and introduced our outcomes at the IPA booth during the Interop, providing me with a distinctive ICSCoE experience.

Beyond the project activities, the most significant benefit is the rich and meaningful year I spent with instructors, experts, and colleagues, whom I would not have met otherwise.

I would like to fully leverage the lessons learned and the connections I have built to contribute to enhancing the security capabilities of my enterprise.

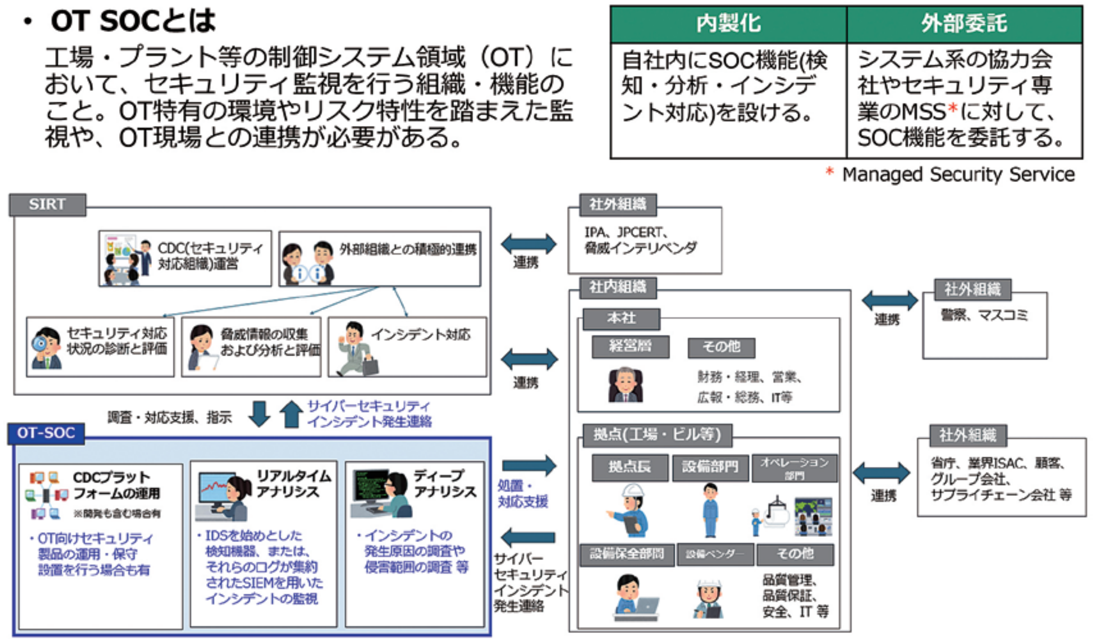
Guidelines for Establishing and Operating Cyber Attack Monitoring in OT Environments (OT-SOC)

Backgrounds and Issues

In recent years, the risks of cyberattacks targeting the Operational Technology (OT) domain has been increasing. Traditionally, control systems in factories and plants were once isolated from external networks. However, with the advancement of digital transformation (DX) and the growing use of remote maintenance, these systems are now increasingly connected to IT networks and cloud environments. As a result, new attack vectors and risks not previously considered under traditional IT security frameworks have emerged.

At the same time, security measures for the OT domain remain under development, and compared to IT security, comprehensive knowledge and practical case studies for OT cybersecurity have still been insufficient. Among these, designing and operating Security Operation Centers (SOCs), tailored to the systems and operational characteristics unique to OT, is a subject that many organizations have begun to consider.

Against this backdrop, our project aimed to gain practical insights into the implementation and operation of OT-SOCs, laying a foundation for future security enhancements across participating companies.



- **OT SOCとは**

工場・プラント等の制御システム領域（OT）において、セキュリティ監視を行う組織・機能のこと。OT特有の環境やリスク特性を踏まえた監視や、OT現場との連携が必要がある。

内製化	外部委託
自社内にSOC機能(検知・分析・インシデント対応)を設ける。	システム系の協力会社やセキュリティ専業のMSS*に対して、SOC機能を委託する。

* Managed Security Service

SIRT
CDC(セキュリティ対応組織)運営
外部組織との積極的連携
セキュリティ対応状況の診断と評価
脅威情報の収集および分析と評価
インシデント対応
調査・対応支援、指示
サイバーセキュリティインシデント発生連絡
OT-SOC
CDCプラットフォームの運用
※開発も含む場合有
・OT向けセキュリティ製品の運用・保守設置を行う場合も有
リアルタイムアナリシス
・IDSを始めとした検知機器、または、それらのログが集約されたSIEMを用いたインシデントの監視
ディープアナリシス
・インシデントの発生原因の調査や侵害範囲の調査 等
連携
連携
処置・対応支援
サイバーセキュリティインシデント発生連絡
社外組織
IPA、JPCERT、脅威インテリベンダ
社内組織
本社
経営層
その他
財務・経理、営業、広報・総務、IT等
拠点(工場・ビル等)
拠点長
設備部門
オペレーション部門
設備保全部門
設備ベンダー
その他
品質管理、品質保証、安全、IT 等
連携
社外組織
警察、マスコミ
連携
社外組織
省庁、業界ISAC、顧客、グループ会社、サプライチェーン会社 等

Conceptual Diagram of OT-SOCs

Issue-solving & Outcomes

The primary objective of this project was for each member to gain insights into OT-SOCs and apply those to their dispatching organizations to strengthen the future security postures.

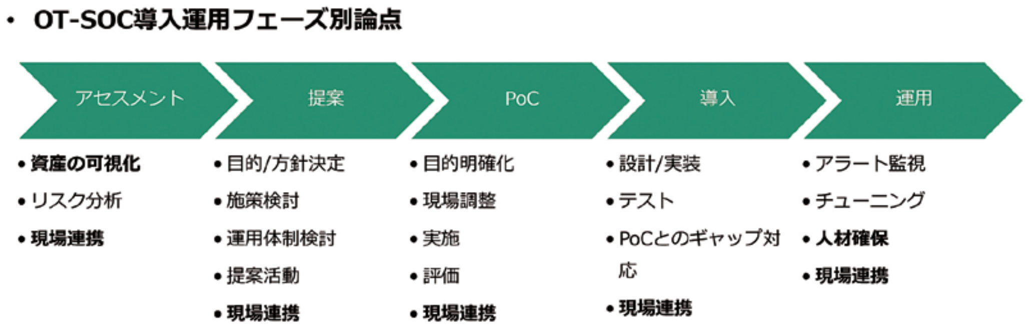
To achieve this goal, the project team centered on two main activities.

The first activity involved conducting interviews with more than ten organizations representing various perspectives on OT-SOC operations . In addition to user companies operating OT-SOCs, we received valuable input from Managed Security Service (MSS) providers and OT monitoring and visualization solution vendors, through which we collected extensive information on challenges and approaches from practitioners.

The collected insights were then mapped to the OT-SOC lifecycle—from assessment and proposal to PoC, implementation, and operation—to identify common challenges and discussion points at each stage.

Our OT-SOC lifecycle aimed to create a practical guide that helps SOC planners and implementers objectively assess their organization's current status and determine the next steps to realize OT-SOCs.

The second activity focused on operational validation using a simulated plant environment.



- **OT-SOC導入運用フェーズ別論点**

アセスメント	提案	PoC	導入	運用
• **資産の可視化**	• 目的/方針決定	• 目的明確化	• 設計/実装	• アラート監視
• リスク分析	• 施策検討	• 現場調整	• テスト	• チューニング
• **現場連携**	• 運用体制検討	• 実施	• PoCとのギャップ対応	• **人材確保**
	• 提案活動	• 評価	• **現場連携**	• **現場連携**
	• **現場連携**	• **現場連携**		

OT-SOC Lifecycle and Key Considerations at Each Phase