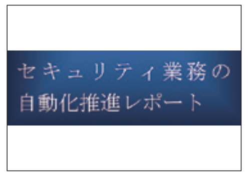
7th Core Human Resource Development Program: Web Released Final Projects

**We have web-released our final projects, other than the ones introduced in this report.
Please check them out on our website.**

Promoting the Automation of Security Operations



The team summarized strategic execution orders, considerations, and technical approaches as instrumental knowledge to automate security operations.

Visionary Security
~ Security Measures Starting from Zero ~

The team outlined security measures and created a video to enable visionary start-ups to focus more on creating new businesses that will help them penetrate the market according to the characteristics of industries.

A Summary of Risk Assessment Methodology for Vulnerability Responses (Vulnerability Response Management Project)

The team summarized the risk assessments for vulnerability response management operations. Enterprises need an appropriate risk assessment accounting for priorities to decrease the number of such operations.
This summary outlines the characteristics & functions of risk assessment indexes (CVSS and EPSS) and application examples.

Supply Chain Security for Practitioners

This project targets practitioners who will engage in in-house supply chain security and personnel who are worried about promoting supply chain security. The team organized the concepts of supply chain security and the flow of approach.

What is the True Nature of "Fuzziness" Felt about Security Rules that We Discovered after Our 448-hour Research? (by the Research Project for Intrusions and Measures)

When you hear the phrase “Information Security Rules”, do you feel you must adhere to them? You may feel “fuzzy” if someone “forces you to follow the rules” without knowing the reasons.
The team focused on this “fuzziness” and created this book to “clear” this phenomenon.

Security Awareness Content
(Incident exercises & Security Measures for IoT/ DX)

The team built two awareness content based on the defense and response perspectives as follows:
(1)A card game focusing on information collaborations for incident responses
(2)A card game to learn cyber damages and measures for IoT and DX

A Security Measure Handbook for Remote Access to Control Systems

The team examined the challenges from enterprise surveys and created a handbook based on the results. This handbook describes remote access mechanisms, risk analysis methods, security measures, and examination processes for implementing and operating remote access to the control systems.

Security-by-design
“Security Improvement for System Development”

The team produced a security education document for beginners of the system development team, targeting design and development engineers and security assurance personnel. Users will learn from this document anti-patterns that are common mistakes causing security incidents and what not to do when implementing security-by-design.

Security Action Laboratory ~ A Project for Practical Learning ~

The team created two deliverables targeting IT system-related enterprises that strive to improve employees' security awareness and knowledge: Training Content Enabling Users to Practice Exhaustively from Environment Development to Security Measures, and an Enlightenment Manga & Video Simulating a Victim of a Cyber Incident.

Communication for Cyber Resilience

To respond to cyber incidents promptly and flexibly, the team outlined procedures for communication that security personnel must be aware of and created "Communication for Cyber Resilience- A Skill Book for Communication Required for Security Personnel."

Principles of War versus Cybersecurity
~ To Comprehend the Ideas of Appropriate Security Measures Referencing to a Military Framework and Attackers' Perspective ~

The team compiled a booklet applying the military framework, "Principles of War," to cybersecurity. We recommend this booklet to anyone who desires to gain the ability to think and act independently and to deepen the understanding of cyber attackers in the increasingly complex cybersecurity environment.

A Guide for Implementing and Operating SBOM

A Guideline for Implementing and Operating SBOM
The team summarized the initiatives and know-how when practitioners implement and operate SBOM. This guideline outlines the initiative for each phase as a checklist.

Cloud Security (How to Utilize Cloud Security)

クラウドセキュリティ
IPA 産業サイバーセキュリティセンター
中核人材育成プログラム 7期
クラウドセキュリティプロジェクト

The team published the portal site "How to Utilize Cloud Security" to improve cloud security. The team unified and visualized the guidelines to enable users to access guidelines promptly that fit users' particular needs.

Please visit our website for more information about the final projects.

中核人材育成プログラム 卒業プロジェクト 検索

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

IPA Better Life with IT

ICSCoE REPORT vol. 21
Industrial Cyber Security Center of Excellence
3.28.2025

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

7th Core Human Resource Development Program – Introducing Our Final Projects

A Project of Developing Guidelines for Implementing and Operating Cyber Threat Intelligence

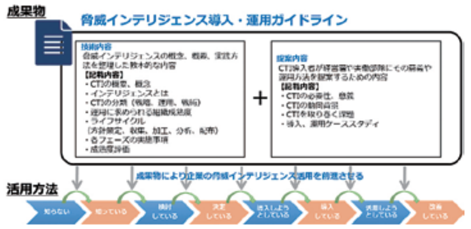
Backgrounds and Issues

Due to the increasing complexity of recent threats and the systematization of industry activities, cyber threat intelligence (CTI)*, which implements threat-based security measures, has become a hot phrase. Many enterprises do not yet understand the actual picture of cyber threat intelligence; however, promoting the utilization of cyber threat intelligence is a considerable challenge for critical infrastructure companies in Japan.
The team created a deliverable called "A Guideline for Implementing and Operating Cyber Threat Intelligence," outlining the existing state and application/ utilization procedures of CTI through this project,

* Cyber Threat Intelligence (CTI) - A decision-making lifecycle of organizational security mechanism based on intelligence obtained through collecting, processing, and analyzing threat information on cyber security.

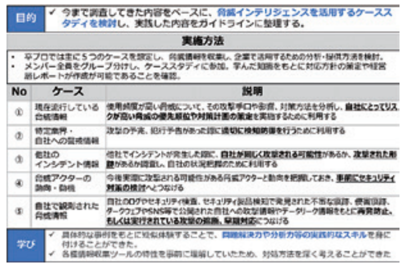
Issue-Solving and Outcomes

The project members comprehended the emerging trends of cyber threat intelligence through literature surveys and reading meetings to create this guideline. To make this guideline more practical, they also interviewed enterprises and understood a picture of the implementation status of cyber threat intelligence and the challenges facing enterprises. The guideline includes two contents: techniques (concepts and practical skills) and proposals, in which cyber threat intelligence operators precisely indicate effects, purposes, and implementation methods to managers and operational units. This guideline aims to resolve the issues enterprises face and progress in utilizing cyber threat intelligence to the next stage(refer to the upper-right figure).


成果物
脅威インテリジェンス導入・運用ガイドライン
技術内容
脅威インテリジェンスの概念、戦略、実践方法を整理した教科的な内容
【記載内容】
・CTIの概要、概念
・インテリジェンスとは
・CTIの分類（戦略、運用、戦術）
・運用に求められる組織成熟度
・ライフサイクル（方針策定、収集、加工、分析、配布）
・各フェーズの実施事項
・成熟度評価
+
提案内容
CTI導入者が経営層や実働部隊にその価値や運用方法を提案するための内容
【記載内容】
・CTIの必要性、意義
・CTIの動向背景
・CTIを取り巻く課題
・導入、運用ケーススタディ
成果物により企業の脅威インテリジェンス活用を前進させる
活用方法
知らない
知っている
検討している
決定している
導入しようとしている
導入している
活用しようとしている
改善している

Guideline Structure

The team reviewed the case studies, leveraging cyber threat intelligence, and compiled a guideline based on their research. The members assume five cases, but they could produce concrete flows for practices. We encourage our audience to utilize this guideline, enabling them to identify challenges and image systems and operations precisely when implementing cyber threat intelligence into the tasks of enterprises.



目的	✓ 今まで調査してきた内容をベースに、脅威インテリジェンスを活用するケーススタディを検討し、実践した内容をガイドラインに整理する。

実施方法
・卒プロでは主に5つのケースを設定し、脅威情報を収集し、企業で活用するための分析・提供方法を検討。 ・メンバー全員をグループ分けし、ケーススタディに参加。学んだ知識をもとに対応方針の策定や経営層レポートが作成が可能であることを確認。

No	ケース	説明
①	現在流行している脅威情報	使用頻度が高い脅威について、その攻撃手口や影響、対策方法を分析し、自社にとってリスクが高い脅威の優先順位や対策計画の策定を実施するために利用する
②	特定業界・自社への警戒情報	攻撃の予兆、犯行予告があった際に適切に検知防御を行うために利用する
③	他社のインシデント情報	他社でインシデントが発生した際に、自社が同じく攻撃される可能性があるか、攻撃された形跡があるか調査し、自社の状況把握のために利用する
④	脅威アクターの動向・目的	今後実際に攻撃される可能性がある脅威アクターと動向を把握しておき、事前にセキュリティ対策の検討へとつなげる
⑤	自社で観測された脅威情報	自社のログやセキュリティ検査、セキュリティ製品検知で発見された不審な通信、侵害痕跡、ダークウェブやSNS等で公開された自社への攻撃情報やデータリーク情報をもとに再発防止、もしくは実行されている攻撃の排除、早期対応につなげる

学び	✓ 具体的な事例をもとに疑似体験することで、問題解決力や分析力等の実践的なスキルを身に付けることができた。 ✓ 各種情報収集ツールの特性を事前に理解していたため、対処方法を深く考えることができた

Outlines of case studies

Interview with a graduate

Mr. NIHONMATSU Tatsuro
Kansai Electric Power Co., Inc.

What is your utmost benefit from this project?

The utmost benefit of this project is our experience in creating a new guideline. We have recently not found many guidelines generally applied in Japan; therefore, developing this guideline was quite challenging, as we had to decide how to incorporate the information and experience, but we could fulfill our final project. The members and I enriched our knowledge through the research and interviews. I hope that implementing cyber threat intelligence will progress within enterprises and industries.

Methods for utilizing project outcomes

After returning to my company, I would like to apply cyber threat intelligence and utilize it for operations. On the one hand, when securing human resources and establishing organizational frameworks to apply in my enterprises effectively, cyber threat intelligence faces many challenges, and its level is quite high. Therefore, I would like to proceed with this project in collaboration with more parties.

This is unique to the ICSCoE!

Extensive personal connections are unique to the ICSCoE.
In the early stage of our project, when studying the adaptation of cyber threat intelligence to enterprises, It was challenging for us to perceive the reality through literature surveys and consulted my mentor; he introduced me to the enterprise personnel implementing cyber threat intelligence and the prominent professor writing the references in this area. I could obtain great opportunities to exchange views regarding guideline development, and they reviewed the project outcomes. I might not be able to realize such relationship-building through in-house operations.

Cybersecurity Reinforce Unit for the Railway Industry
~ Good to be Aware and Protect! ~

Backgrounds and Issues

In recent years, the damages from cyber attacks have been increasing steadily, and these attacks are now targeting control systems previously considered secure. Cyber attacks against railway systems have also frequently occurred overseas. Therefore, there is a possibility that Japan's railway systems may face cyber attacks in the future. However, we have not yet prepared adequate investigation mechanisms, such as systems and analytic environments. In this project, the team focused on intolerant events from these circumstances and produced two outcomes: "A Cybersecurity Enhancement Textbook" is a guidebook demonstrating examination techniques from risk analysis to security measures, and "Recommendation of Exploiting Logs to Prepare for Cyber Attacks" is also a guidebook identifying technical and organizational challenges necessary for detection, response, and recovery when cyber attacks occur.

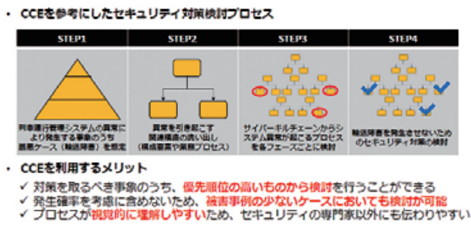
Issue-solving and Outcomes

○ **A Cybersecurity Enhancement Textbook**

The railway industry has prepared guidelines outlining comprehensive management policies for its cybersecurity measures; however, in some cases, we have not undertaken the necessary measures, considering the priorities. In this textbook, the team examined the procedures from risk identification to security measure preparation for the train operation management system*1 based on a risk-based approach called CCE*2 to raise the security level of the railway sector.

*1 Consequence-driven Cyber-informed Engineering: A methodology of reviewing security measures developed by Idaho National Laboratory (INL) in 2016

*2 A computer system that collectively manages and controls various systems based on the scheduled trains.



・CCEを参考にしたセキュリティ対策検討プロセス
STEP1
STEP2
STEP3
STEP4
列車運行管理システムの異常により発生する事象のうち 最悪ケース（輸送障害）を想定
異常を引き起こす 関連構造の洗い出し （構成要素や業務プロセス）
サイバーキルチェーンからシステム異常が起こるプロセスを各フェーズごとに検討
輸送障害を発生させないためのセキュリティ対策の検討
・CCEを利用するメリット
✓ 対策を取るべき事象のうち、優先順位の高いものから検討を行うことができる
✓ 発生確率を考慮に含めないため、被害事例の少ないケースにおいても検討が可能
✓ プロセスが視覚的に理解しやすいため、セキュリティの専門家以外にも伝わりやすい

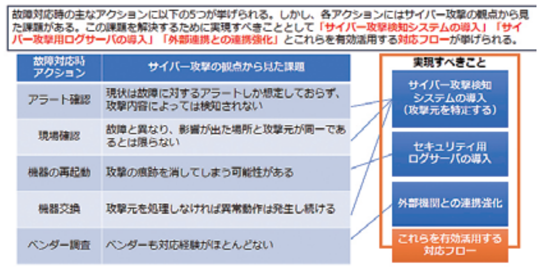
Security measures based on the risk-based approach

The team defined "transportation service disruption due to malfunction of the train operation management system" as an intolerant event and categorized steps from risk analysis to security measures.

The members scored their planned security measures based on five perspectives: costs, efforts, technical feasibility, and effects, and prioritized them to implement measures appropriate for security levels. Moreover, the team specified some security measure items described abstractly in the guidelines for users to tackle with security measures.

○**Recommendation of Exploiting Logs to Prepare for Cyber Attacks**

The existing railway control systems experience two issues when a system malfunction occurs: it is impossible to distinguish between cyber attacks and equipment failure, and response flows for control systems under cyber attacks are unclear. This guidebook outlines recommendations from both technical and organizational perspectives for determining a cyber attack and responding appropriately when railway control systems are facing an attack.



故障対応時の主なアクションに以下の5つが挙げられる。しかし、各アクションにはサイバー攻撃の観点から見た課題がある。この課題を解決するために実現すべきこととして「サイバー攻撃検知システムの導入」「サイバー攻撃用ログサーバの導入」「外部連携との連携強化」とこれらを有効活用する対応フローが挙げられる。

故障対応時アクション	サイバー攻撃の観点から見た課題
アラート確認	現状は故障に対するアラートしか想定しておらず、攻撃内容によっては検知されない
現場確認	故障と異なり、影響が出た場所と攻撃元が同一であるとは限らない
機器の再起動	攻撃の痕跡を消してしまう可能性がある
機器交換	攻撃元を処理しなければ異常動作は発生し続ける
ベンダー調査	ベンダーも対応経験がほとんどない

実現すべきこと
サイバー攻撃検知システムの導入（攻撃元を特定する）
セキュリティ用ログサーバの導入
外部機関との連携強化
これらを有効活用する対応フロー

Challenges and what we should do for failure responses from the cybersecurity perspective

In today's railway industry, field personnel and staff of the security department and maintenance vendors share information and operate in cooperation with each other. The team installed the equipment, which enables us to detect cyber attacks and collect logs, and the members developed incident response flows to tackle cyber attacks effectively during operations. Moreover, the team conducted the exercise using attack scenarios expected to happen in the railway industry in reality. The team collected feedback on the exercise to improve the flows, enabling us to handle various scenarios.

Interview with a graduate

Mr. KUBO Takashi
Hankyu Hanshin Holdings, Inc.

What is your utmost benefit from this project?

The utmost benefits are utilizing the actual systems and verifying them. It was a precious opportunity to confirm behaviors that would be difficult to try on the in-house systems. Besides, it was beneficial for me to become a project leader. I had not worked in management in my enterprise. Still, it could be an incredible opportunity to apply my experience to my future work by leading the final project specific to my industry.

Methods for utilizing project outcomes

I am planning to utilize "A Cybersecurity Enhancement Textbook for my enterprise, industry, and related parties to determine cybersecurity measures.

I want to utilize the "Recommendation of Exploiting Logs to Prepare for Cyber Attacks" to conduct in-house exercises for incident responses. I intend to share both deliverables with the relevant departments and tailor them to my company to raise effectiveness.

This is unique to the ICSCoE!

I greatly benefited from the opportunity to interview professors in various fields and the extensive networking, including collaborations with enterprises and external parties. I gained excellent experience through the program because it is not easy for us to connect with managers of other companies, such as decision-makers from diverse enterprises, by simply engaging in my enterprise. It was very meaningful for me to share the latest information, other than the railway sector, with the trainees dispatched from various industries. I understood that each industry has distinct cybersecurity measures; in particular, my colleagues from the power and gas sectors shared lots of information useful for the railway industry.

Security Risks and Measures for Generative AI
~ What Guidelines Enterprises Currently Need? ~

Backgrounds and Issues

According to a survey conducted by JIPDEC, 69.5 percent of enterprises use generative AI or have been implementing it; thus, we assume that more enterprises will adopt this technology. However, Japanese companies have not yet established the rules for implementing generative AI.

Users will face various security risks when utilizing generative AI. Therefore, it is essential to understand these risks appropriately and mitigate them. From these circumstances, the project team formulated a guideline for implementing and operating text-generative AI to reduce enterprise security risks.

Issue-solving and Outcomes

This project conducted two activities: ① the validation of building secure generative AI and ② the establishment of guidelines for implementing and operating text-generative AI.

As with the security measures for generative AI, a multi-layered defense concept is critical, similar to the existing security measures.

As ① the validation of building secure generative AI; however, we examined the effects of LLM*1 security guardrail and the effectiveness of information access authority management using RAG*2 with metadata.

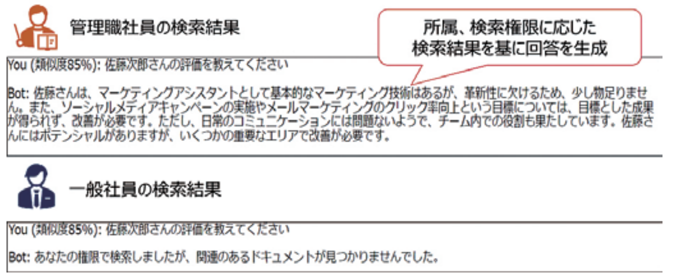
Regarding the former case, we confirmed that LLMs have some effect on adversarial prompts*3 responding to malicious questions, which LLMs cannot ordinarily answer when utilizing the guardrail.

In the latter case, we validated that RAGs with metadata enable them to change answers based on the titles of questioners, such as supervisory employees or non-supervisory employees.

*1 AI models that are capable of understanding and generating human-like natural languages by learning billions and tens of billions of text data.

*2 Passing external sources to LLMs to improve answer accuracy

*3 Prompts that allow users to guide models through conversation and generate unintentional results.



You (類似度85%): 佐藤次郎さんの評価を教えてください

Bot: 佐藤さんは、マーケティングアシスタントとして基本的なマーケティング技術はあるが、革新性に欠けるため、少し物足りません。また、ソーシャルメディアキャンペーンの実施やメールマーケティングのクリック率向上という目標については、目標とした成果が得られず、改善が必要です。ただし、日常のコミュニケーションには問題ないようで、チーム内での役割も果たしています。佐藤さんにはポテンシャルがありますが、いくつかの重要なエリアで改善が必要です。

You (類似度85%): 佐藤次郎さんの評価を教えてください

Bot: あなたの権限で検索しましたが、関連のあるドキュメントが見つかりませんでした。

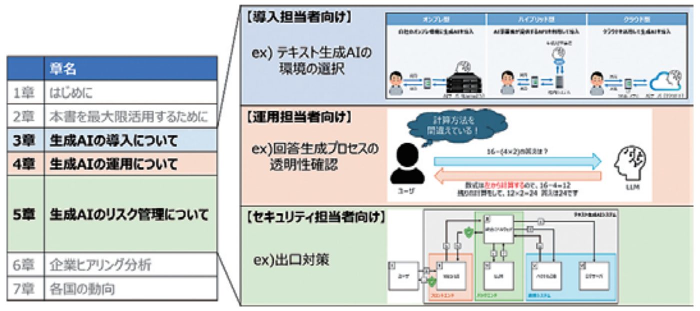
Potential Responses for the Identical Question When Using RAG with Metadata

For ② the establishment of Guidelines for Implementing and Operating Text-generative AI, the team started interviewing enterprises and municipal authorities that had already implemented generative AI and summarized risks perceived as threats and general challenges.

According to the interview results, we understood that enterprises focus on the risks caused by information leakage and hallucination and face general issues caused by a lack of users' understanding and awareness of generative AI, such as controlling for the utilization rate and expectation management; thus, we created the guidelines to resolve these concerns.

The audience for this guideline is users implementing generative AI; however, we described what personnel should consider and cooperate with other responsible individuals from three perspectives: implementation personnel, operation personnel, and security personnel.

*4 The phenomenon of generative AI models generating content that contains false or misleading information presented as facts.



	章名
1章	はじめに
2章	本書を最大限活用するために
3章	生成AIの導入について
4章	生成AIの運用について
5章	生成AIのリスク管理について
6章	企業ヒアリング分析
7章	各国の動向

Excerpts from the Guidelines

Interview with a graduate

What is your utmost benefit from this project?

I did not have the opportunity to handle AI during regular operations, and when looking at the trainees of the seventh ICSCoE program, none of my colleagues had touched AI for their businesses.

Through the final project, however, I had the chance to learn more about AI and deepen my insights; that is my utmost benefit from the project.

In particular, the trainees acquired more practical skills through hands-on training, enabling them to operate generative AI, which would be impossible for them to gain through classroom training alone.

Moreover, it was very beneficial for me to become a project leader. I had not led any project since I became a businessperson; thus, I did not know how to behave as a leader; however, I felt, "Don't worry about the failures.

I can challenge various things here!" Therefore, I nominated myself as a project leader.

The team conducted extensive interviews with numerous enterprises, municipal authorities, and colleagues from various industries to encourage more people to utilize our guidelines; I compiled the interview results with the team members' massive support. I hope the experience gained through the project will help my future activities.

Methods for utilizing project outcomes

Mr. TSUJIMURA Kai
OPTAGE Inc.

First, I expect our enterprises and related parties to utilize our guidelines. The cases of massive damage caused by generative AI services are limited now; however, potential risks are gradually becoming more recognizable. Therefore, there is no doubt that the significance of security measures will increase. I hope this document will help users to take appropriate measures at an early stage.

This is unique to the ICSCoE!

The various connections, including our mentors, lecturers, and the IPA, are unique to the ICSCoE because they enabled us to conduct extensive interviews with enterprises, municipal authorities, and related parties. In particular, when we were having trouble figuring out where to interview, the ICSCoE provided us with an opportunity to interview METI personnel; thus, we could obtain their opinions, which are different from an enterprise perspective. We reflected on the given opinions in our project. It helped us improve the quality of our outcomes. We sincerely appreciate your support.