

# ISCN Newsletter

(ISCN ニュースレター)

## No.0349

## January, 2026

Integrated Support Center for Nuclear Nonproliferation, Security and  
Human Resource Development (ISCN)

原子力人材育成・核不拡散・核セキュリティ総合支援センター

Japan Atomic Energy Agency (JAEA)

国立研究開発法人日本原子力研究開発機構



---

## 目次

1. お知らせ	4
1-1 新年のご挨拶	4
1-2 「原子力平和利用と核不拡散・核セキュリティに係る国際フォーラム 2025」を開催	5
1-3 令和 7 年度「原子力人材育成ネットワーク」シンポジウム開催	7
1-4 ISCN-WINS 共催ワークショップ「核セキュリティに係るサプライチェーン・リスク」開催のお知らせ	8
2. 核不拡散・核セキュリティに関する動向(解説・分析)	9
2-1 民生用原子力分野での AI の活用に係る 2 つの VCDNP 文書の概要紹介	9
2-1-1 「人工知能(AI)と核セキュリティガバナンス:フロンティア AI リスクへの対応」の概要紹介	10
核セキュリティ分野における人工知能(AI)の影響を体系的に整理し、政策、技術及び倫理的観点からの議論の必要性を促した「AI と核セキュリティガバナンス:フロンティア AI リスクへの対応」と題する報告書の概要を紹介する。	
2-1-2 「過去、現在、そして未来における原子力分野での AI の活用」の概要紹介	15
原子力安全、核セキュリティ及び政策決定支援等、多岐に亘る分野における AI の導入状況と将来展望を体系的に整理し、その活用可能性とその課題等を明らかにした「過去、現在、そして未来における原子力分野での AI の活用」と題する論文の概要を紹介する。	
3. 活動報告	25
3-1 日本核物質管理学会第 46 回年次大会参加報告	25
2025 年 12 月 2 日～3 日に開催された日本核物質管理学会(INMMJ)第 46 回年次大会において、ISCN から 7 件の発表を行ったので、それぞれの概要を報告する。	
3-2 第 93 回及び第 94 回原子炉工学特別講座報告 上期・下期	29
第 93 回及び第 94 回原子炉工学特別講座報告 上期・下期について報告する。	
3-3 欧州委員会共同研究センター(EC-JRC)との運営委員会開催報告	30
欧州委員会共同研究センター(EC-JRC)との運営委員会開催結果を報告する。	
3-4 IAEA 研修「Integrated Workshop on Radiological Crime Scene Management and Nuclear Forensics」参加報告	31
IAEA が主催する「Integrated Workshop on Radiological Crime Scene Management and Nuclear Forensics」の参加報告をする。	
3-5 ASEAN Energy Cooperation Week 2025 参加報告	33
ASEAN Energy Cooperation Week 2025 について報告する。	

---

### 3-6 技術報告 - Report from 2025 IEEE Nuclear Science Symposium, Medical Imaging Conference, and Room Temperature Semiconductor Detectors Symposium (IEEE NSS MIC RTSD) in Yokohama!----- 34

横浜で開催された国際会議(2025 IEEE NSS MIC RTSD)に技術開発推進室の核検知チーム3名が参加し、文部科学省の核セキュリティ強化プロジェクトにおける最新成果を発表した。ここではその概要について述べる。

## 4. コラム ----- 36

### 4-1 フランス便り ～関根 恵～ ----- 36

フランスでフルリモートワークを行っている、編集委員の関根よりフランスの雰囲気を紹介する。

---

## Contents

<b>1. Announcements</b>	<b>4</b>
1-1 New Year's Greetings	4
1-2 “2025 International Forum on Peaceful Uses of Nuclear Energy, Nuclear Non-Proliferation and Nuclear Security” Held	5
1-3 Notice: FY2025 Japanese Human Resource Development Network Symposium	7
1-4 Notice: ISCN-WINS Joint Workshop: “Supply Chain Risks Related to Nuclear Security”	8
<b>2. Nuclear Non-proliferation and Nuclear Security Trends and Analysis</b>	<b>9</b>
2-1 Introduction to two VCDNP (Vienna Center for Disarmament and Non-Proliferation) Reports on the Application of AI in the Civilian Nuclear Sector	9
2-1-1 Summary of VCDNP Report: “Artificial Intelligence and Nuclear Security Governance: Addressing the Risk of Frontier AI”	10
2-1-2 Summary of VCDNP Report: “Past, Present, and Future Applications of AI in the Nuclear Sector”	15
<p>This article presents the key points of VCDNP report entitled "Past, Present and Future Applications of AI in the Nuclear Sector," which systematically summarizes the current state and future prospects for the application of AI in the nuclear sector and clarifies a wide range of potential applications and challenges, including nuclear safety, nuclear security and policy-making support.</p>	
<b>3. ISCN's Activities Reports</b>	<b>25</b>
3-1 Summary of Presentations by ISCN members at the 46th Annual Meeting of Institute of Nuclear Materials Management(INMM) Japan Chapter	25
<p>This article presents summaries of each of the seven presentations given by ISCN at the 46th Annual Meeting of the Institute of Nuclear Materials Management of Japan (INMMJ) held on December 2-3, 2025.</p>	
3-2 Report on the 93rd and 94th Special Lectures on Reactor Engineering	29
3-3 Report on steering committee of European Commission-Joint Research Center (EC-JRC)	30
3-4 Report on Integrated Workshop on Radiological Crime Scene Management and Nuclear Forensics by IAEA	31
3-5 Reporting on the ASEAN Energy Cooperation Week 2025	33
3-6 技術報告 - Report from 2025 IEEE Nuclear Science Symposium, Medical Imaging Conference, and Room Temperature Semiconductor Detectors Symposium (IEEE NSS MIC RTSD) in Yokohama!	34
<p>Three members of our team presented at the 2025 IEEE Nuclear Science Symposium, Medical Imaging Conference, and Room Temperature Semiconductor Detectors Symposium (IEEE NSS MIC RTSD) the latest results from MEXT's Nuclear Security Enhancement Project. This article provides an overview of the results.</p>	

---

---

#### **4. Column ----- 36**

##### **4-1 Letters from France ~Ms. Megumi Sekine~ ----- 36**

From Sekine, an editorial committee member working fully remotely in France, shares impressions of the local atmosphere.

---

## 1. お知らせ

### 1-1 新年のご挨拶

新年あけましておめでとうございます。

いつも ISCN Newsletter をご愛読いただき、誠にありがとうございます。昨年は旧原子力人材育成センターとの統合を経て、皆さまの多大なご支援のもと、新 ISCN として再出発し、滞りなく業務を進めることができましたこと、心より御礼申し上げます。

世界は脱炭素化、エネルギー安全保障、AI データセンター等の新たな電力需要を背景に原子力リサージェンス(復興)に向かって力強く動き始めました。国際政治的にも長引くウクライナ紛争、これまでになく複雑化した中東情勢、東アジア情勢を背景とする核不拡散・核セキュリティ・核軍縮分野も複雑化し目を離せません。国内では昨年、閣議決定された第 7 次エネルギー基本計画に基づいた動きが活性化してきています。

2026 年は丙午の年、「丙(ひのえ)」は火を意味し、情熱的でエネルギッシュ、「午(うま)」は躍動・成功を象徴し、「事業発展や努力が実を結ぶ年」とのこと、ISCN では今後も核不拡散の一層の強化、核セキュリティの一層の向上に加え、原子力科学技術の健全な発展に 3S 人材育成支援×2S 技術開発を通じて貢献できるよう前向きにエネルギッシュに努めてまいります。

本 Newsletter もこれらの動きを注視しながら動向を皆さまにお伝えし、広くご活用いただけるよう、尽力してまいります。

2026 年も皆さまにとって実り多い一年となりますよう、心からお祈り申し上げます。本年もどうぞよろしくお願いいたします。

【報告:ISCN センター長 井上 尚子】

---

## 1-2 「原子力平和利用と核不拡散・核セキュリティに係る国際フォーラム 2025」を開催

JAEA/ISCN は、2025 年 12 月 11 日、「原子力平和利用と核不拡散・核セキュリティに係る国際フォーラム 2025」を、対面及びオンラインのハイブリッド形式で開催し、約 350 名の方々にご参加いただきました。



### 【開会挨拶】

国立研究開発法人日本原子力研究開発機構 理事長 小口 正範



### 【来賓挨拶】

文部科学省 研究開発局 局長 坂本 修一氏



### 【基調講演 I】

「核・放射線脅威に対する世界的備えの強化: グローバルな核セキュリティ強化戦略と核鑑識への期待」

国際原子力機関(IAEA) 核セキュリティ部 部長

エレナ ブグロバ氏(オンライン)



### 【基調講演 II】

「科学と安全保障の視点 核鑑識 R&D と人材育成 - 規制機関の使命と展望、研究機関への期待」

タイ原子力庁(OAP) 安全規制技術支援局 セキュリティ・保障措置技術支援課 課長 ハリネート ムンパヤバン氏



### 【JAEA/ISCN の事業報告】

ISCN センター長 井上 尚子

講演後は、ISCN 副センター長 山口知輝がモデレーターを務め、以下のパネリストの方々でパネルディスカッションを行いました。

➤ タイ原子力庁(OAP) 安全規制技術支援局 セキュリティ・保障措置技術支援課

課長 ハリネート ムンパヤバン氏

- インドネシア国家研究イノベーション庁(BRIN) 原子力エネルギー機構 核セキュリティ上級アナリスト アリフ サソニコ アディ氏
- 英国国立原子力研究所(UKNNL) 核鑑識技術責任者 ピーター ヒラー 氏
- 警察庁 科学警察研究所 物理研究室 主任研究官 田辺 鴻典 氏
- 国立大学法人 東京科学大学 総合研究院ゼロカーボンエネルギー研究所 助教 木村 祥紀 氏
- 学校法人 中部大学 工学部 電気電子システム工学科(「ISCN 夏の学校 2025」代表学生) 川口 煌 氏



パネルディスカッションの様子

左からヒラー氏、川口氏、木村氏、アディ氏、田辺氏、ムンパヤバン氏、山口

パネルディスカッションでは、「知と行動をつなぐ:核鑑識、国際・地域協力、人材育成による未来への備え」と題し各パネリストからの発表後に議論を行いました。

なお、本フォーラムの詳細報告は近々ニューズレター特別号にて掲載予定です。また、基調講演者及びパネリスト等の略歴並びに発表資料等は ISCN ホームページ (<https://www.jaea.go.jp/04/iscn/activity/2025-12-11/index.html>)でも掲載しております。



基調講演者やパネリスト等の集合写真



---

### 1-3 令和 7 年度「原子力人材育成ネットワーク」シンポジウム開催

原子力人材育成ネットワーク<sup>1</sup>は、2 月 10 日にシンポジウムを開催します。今年度は、中高校生に対する原子力教育に関する講演をはじめ、人材育成に資するデータ収集および分析に関する報告が行われます。

- 日 時：2026 年 2 月 10 日(火) 9:30～16:00
- 参 加 費：無料
- 開催方法：開催方法:対面(日比谷国際ビルコンファレンススクエア 8 階 8D) 及び Web 方式(ZOOM)
- 申込締切：対面希望者：2026 年 1 月 30 日(金) 18:00 まで  
web 方式参加希望者：2026 年 2 月 9 日(月) 12:00 まで

申込みは、下記 URL より登録ください。

<<https://zoom.us/meeting/register/cmdVYII7SJW7VlS7Di0R6g#/>>

申し込みができない場合は nuhrdec-nw@ml.jaea.go.jp 宛に、氏名、メールアドレス、所属及び希望参加形式(対面または Web 参加)をお知らせください。

また、過去の「原子力人材育成ネットワーク」シンポジウムの情報は下記 HP より閲覧可能です。

<<https://jn-hrd-n.jaea.go.jp/backno03.php#o>>

---

<sup>1</sup> 原子力人材育成ネットワークは ISCN が共同事務局の一部を担っています。

## 1-4 ISCN-WINS 共催ワークショップ「核セキュリティに係るサプライチェーン・リスク」開催のお知らせ

今年度の『ISCN-世界核セキュリティ協会(WINS)共催ワークショップ』につきましては、下記のとおり開催いたします。

➤ テーマ:「核セキュリティに係るサプライチェーン・リスク」

➤ 日 時: 2026年2月16日(月) 13:30～17:00

2026年2月17日(火) 9:30～13:00

➤ 参加費 : 無料

➤ 場 所: 東京都墨田区横綱 1-6-1 国際ファッションセンタービル 3 階  
KFC Hall (最寄駅: 両国駅)

➤ 申込締切: 2026年2月12日(木)

申込みは、QRコードまたは URL より登録ください。

<https://forms.office.com/r/apSmMzqNXg>



ISCN-WINS共催ワークショップ  
核セキュリティに係る  
サプライチェーン・リスク  
2026 **2.16**月 **17**火  
13:30 - 17:00 受付開始13:00  
9:30 - 13:00 受付開始9:00

**プログラム**  
【1日目 (2月16日)】  
基調講演 I  
原子力規制庁 安全管理規制管理官 吉川元浩  
「核物質防護における最近の課題」  
演劇動画とディスカッション AKTプロダクション  
基調講演 II  
Urenco UK セキュリティマネジャー Carol Higson  
「サプライチェーンセキュリティ管理の実践と教訓」  
(日英同時通訳あり)  
【2日目 (2月17日)】  
演劇動画とディスカッション AKTプロダクション

**対象** 国内の原子力事業者、政府機関、  
大学・研究機関等  
**会場** 東京都墨田区横綱1-6-1  
国際ファッションセンタービル  
JR総武線 両国駅 (東口・西口) 徒歩約7分  
都営地下鉄大江戸線両国駅 (A1出口) 徒歩約9分  
**問合せ先** 内川貞之、浅野佐知子  
iscn-event@jaea.go.jp

**申込方法** ▶ QRコードから事前登録してください (参加無料)  
**申込期限** ▶ 2月12日(木)  
演劇は2日間で完結するシナリオとなっていますが、両日のご参加が難しい場合は、  
いずれか1日のみでもご参加いただけます

**【ワークショップの進め方】**  
本ワークショップは、WINSが開発した  
演劇型セッションを取り入れています。  
会場では、実際の演劇を収めた動画を  
使用し、参加者の皆様に課題を抽出して  
いただきます。発言者・出席者を特定する  
情報は伏せる形 (チャタムハウス・ル  
ール) を適用し、議論を行います。議論  
がスムーズに進むよう、ファシリテーター  
がサポートしますが、活発な議論を  
お願いいたします。

**ワークショップ風景例**

**申込QRコード**

**AKT**

主催 | 国立研究開発法人日本原子力研究開発機構 原子力人材育成・核不拡散・核セキュリティ総合支援センター  
本ワークショップは文部科学省核セキュリティ強化等推進事業の一環として開催しています。

## 2. 核不拡散・核セキュリティに関する動向（解説・分析）

### 2-1 民生用原子力分野での AI の活用に係る 2 つの VCDNP 文書の概要紹介

2025 年 1 月 23 日、米国トランプ大統領は、「人工知能(AI)における米国のリーダーシップへの障壁を取り除く」と題する大統領令(Executive Order 14179)<sup>2</sup>を発した。同年 7 月、「競争に勝利する米国 AI 行動計画」<sup>3</sup>を発表し、AI 分野における国家戦略を打ち出した。続く 11 月には、米国エネルギー省(DOE)が主導する「ジェネシス・ミッション」の開始を命じる新たな大統領令(Executive Order 14363)<sup>4</sup>を発した。このミッションは、前述の大統領令及び行動計画に基づき、AI の活用を通じた国家戦略の推進を目的としており<sup>5</sup>、原子力分野では AI を活用した先進原子炉・核融合・送電網の近代化の加速や、国家安全保障ミッションに資する先進 AI 技術の開発並びに米国の核兵器備蓄の安全性と信頼性を確保するためのシステムの導入等が含まれている。

また 12 月 3～4 日、IAEA では「人工知能と原子力に関する国際シンポジウム」が開催され<sup>6</sup>、AI の急速な進展と原子力分野との融合に焦点を当て、AI データセンターの電力需要増加に対する原子力の貢献や、原子力発電所のプロジェクト管理における AI の応用と将来展望等について、包括的な議論が行われている。

12 月 23 日、日本政府も「人工知能(AI)基本計画」<sup>7</sup>を閣議決定した。これを受けて今後日本でも、民生用原子力分野における更なる AI 活用の可能性について議論が進展すると見込まれる。

本稿では、こうした議論に資することを目的として、2025 年にウィーン軍縮・不拡散センター(Vienna Center for Disarmament and Non-Proliferation: VCDNP)<sup>8</sup>が発表した原子力分野における AI 活用に関する以下の 2 件の文書の概要を紹介する。

• Sarah Case Lackner and Zaheed Kara, 「人工知能(AI)と核セキュリティガバナンス:

<sup>2</sup> US GovInfo, “DCPD-202500170 - Executive Order 14179—Removing Barriers to American Leadership in Artificial Intelligence”, 23 January 2025, <https://www.govinfo.gov/app/details/DCPD-202500170>

<sup>3</sup> White House, “Winning the Race: America’s AI Action Plan”, July 2025, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

<sup>4</sup> US Federal Register, “Executive Order 14363 of November 24, 2025: Launching the Genesis Mission”, <https://www.govinfo.gov/content/pkg/FR-2025-11-28/pdf/2025-21665.pdf>

<sup>5</sup> DOE, “Energy Department Launches ‘Genesis Mission’ to Transform American Science and Innovation Through the AI Computing Revolution”, 24 November 2025, <https://www.energy.gov/articles/energy-department-launches-genesis-mission-transform-american-science-and-innovation>

<sup>6</sup> IAEA, “International Symposium on Artificial Intelligence and Nuclear Energy – Programme”, 3-4 December 2025, <https://www.iaea.org/events/ai-symposium-2025/programme>

<sup>7</sup> 内閣府, 「人工知能基本計画～「信頼できる AI」による「日本再起」～」, 令和 7 年 12 月 23 日, [https://www8.cao.go.jp/cstp/ai/ai\\_plan/aiplan\\_20251223.pdf](https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_20251223.pdf)

<sup>8</sup> VCDNP (Vienna Center for Disarmament and Non-Proliferation) は、2010 年にオーストリア共和国欧州・国際関係省と、米国ミドルベリー国際大学院モントレー校ジェームズ・マーティン不拡散研究センターが設立した非政府組織。核不拡散及び核軍縮に関する研究の実施、対話の促進及び能力構築を通じた国際平和とセキュリティの促進等の活動を実施している。VCDNP, <https://vcdnp.org/about-us/>

---

フロンティア AI リスクへの対応 (Artificial Intelligence and Nuclear Security Governance: Addressing the Risks of Frontier AI)」<sup>9</sup>

- Donald Dudenhoeffer, 「過去、現在、そして未来における原子力分野での AI の活用 (Past, Present, and Future Applications of AI in the Nuclear Sector)」<sup>10</sup>

## 2-1-1 「人工知能(AI)と核セキュリティガバナンス: フロンティア AI リスクへの対応」の概要紹介

### 【概要】

VCDNP の Sarah Case Lackner 主任研究員と、人工知能(AI)の安全性に関する研究者である Zaheed Kara 氏は、VCDNP とフロンティアモデルフォーラム(FMF)<sup>11</sup>が 2025 年後半に共催し、核セキュリティ及びフロンティア AI<sup>12</sup>の専門家を招聘して行った会議での議論をもとに、報告書「人工知能と核セキュリティガバナンス: フロンティア AI リスクへの対応」を 12 月に VCDNP から発表した。

同報告書は、フロンティア AI が世界各地の原子力施設のセキュリティに及ぼし得るリスクに対応するため、核セキュリティの専門家に向けて有益な知見、初期的な分析並びに提言を提供することを目的としている。報告書では、核セキュリティ分野におけるフロンティア AI モデルの影響を体系的に整理し、政策的、技術的及び倫理的観点を含む包括的な議論の必要性を提起するとともに、両分野の関係者間における継続的かつ非公式なコミュニケーション・チャンネルの確立の重要性を強調している。

本稿では、同報告書の構成に沿い、「背景」、「核セキュリティにおけるフロンティア AI の脅威」、「結論」、及び「提言」の各セッションに分けて、その概要を紹介する。

### 【背景】

AI モデルは、情報を迅速かつ自律的に収集・処理し、有用なパターンを特定し、新たなコンテンツを生成する能力を急速に高めており、敵対者にとって強力な手段となり

---

<sup>9</sup> Sarah Case Lackner and Zaheed Kara, “Artificial Intelligence and Nuclear Security Governance: Addressing the Risks of Frontier AI”, VCDNP, December 2025, [https://vcdnp.org/wp-content/uploads/2025/12/VCDNP\\_AI-and-Nuclear-Security-Governance\\_web.pdf](https://vcdnp.org/wp-content/uploads/2025/12/VCDNP_AI-and-Nuclear-Security-Governance_web.pdf)

<sup>10</sup> Donald Dudenhoeffer, “Past, Present, and Future Applications of AI in the Nuclear Sector”, VCDNP, 29 April 2025, [https://vcdnp.org/wp-content/uploads/2025/04/VCDNP-AIT\\_Past-Present-and-Future-Applications-of-AI-in-the-Nuclear-Sector\\_web.pdf](https://vcdnp.org/wp-content/uploads/2025/04/VCDNP-AIT_Past-Present-and-Future-Applications-of-AI-in-the-Nuclear-Sector_web.pdf)

<sup>11</sup> FMF (Frontier Model Forum) は、Google、Microsoft、OpenAI、Anthropic 等、AI 関連のサービスを提供している各社が 2023 年 7 月に、「AI の安全性のベストプラクティスを特定し、社会的課題への AI 技術の利用を促進する」ことを目的として設立した国際的な非営利組織。CAPA、「Google などの AI 関連企業が集結し設立させた『Frontier Model Forum』とは」、<https://www.capa.co.jp/archives/43592>、及び FMF, <https://www.frontiermodelforum.org/about-us/>

<sup>12</sup> 英国政府は「フロンティア AI」を、「多様なタスクを遂行可能で、現在の最先端 AI モデル(most advanced AI models) に匹敵する、あるいはそれを上回る能力を有する高度な汎用 AI モデル」と定義している、UK Government, “AI Safety Summit: introduction (HTML)”, Updated 31 October 2023, <https://www.gov.uk/government/publications/ai-safety-summit-introduction/ai-safety-summit-introduction-html>

つつある。近年では、特にフロンティア AI モデルが、大量破壊兵器(WMD)開発を企図する悪意ある主体に悪用されるリスクが注目され、その対策を巡る議論が活発化している。一方で、フロンティア AI モデルと核兵器の開発・製造との関連については、核兵器に関する専門知識や機密情報へのアクセスの困難さから、議論は限定的な範囲にとどまっている。しかし、フロンティア AI モデルによる核兵器の開発支援を防ぐためには、必ずしも技術的詳細に踏み込む必要性はなく、核物質や関連施設のセキュリティに焦点を当てた実効的な対策を講じることが可能である。

## 【核セキュリティにおけるフロンティア AI の脅威】

核物質や関連施設に対する敵対者の攻撃は、「標的の選定」、「攻撃計画と技能習得」、及び「攻撃の実施」の 3 つのフェーズに大別される。各フェーズにおけるフロンティア AI モデルがもたらし得るリスクは、以下の表 1 のとおりである。

表 1 3 つのフェーズとフロンティア AI モデルがもたらし得るリスク

敵対者の攻撃に関する 3 つのフェーズ	フロンティア AI モデルがもたらし得るリスク
<b>1. 標的の選定</b> 敵対者が、核物質の種類や量、施設内の安全及びセキュリティシステム等の情報を基に、攻撃対象を選定する段階	<b>&lt;施設の配置及び核セキュリティの妨害&gt;</b> ・施設の公開情報、規制当局への申請書類、衛星画像等の情報の組み合わせによる機密情報の推定
	<b>&lt;システムの特特定&gt;</b> ・施設の安全対策、セキュリティ体制及び運用システムの種類、モデル及び製造元の特特定 ・潜在的な脆弱性の識別とその悪用手段の推定
	<b>&lt;分析上の欠陥の特特定&gt;</b> ・施設の安全及びセキュリティ分析の検証と、論理的な欠陥、未検証の前提及び見落とされた故障モードの特特定 ・潜在的な脆弱性とその悪用手段の推定
<b>2. 攻撃計画と技能習得</b> 敵対者が詳細な攻撃計画を策定し、攻撃実施に必要な技能を習得する段階	<b>&lt;過去の攻撃の分析&gt;</b> ・過去の物理的・サイバー攻撃情報の活用によるセキュリティ上の脆弱性及び攻撃手法の特特定
	<b>&lt;物理的セキュリティの無効化&gt;</b> ・メーカーの仕様書や既知の脆弱性に基づく物理的セキュリティシステムの無効化または回避計画の策定
	<b>&lt;システム上の脆弱性の意図的な悪用&gt;</b> ・安全上重要なシステムを妨害する信憑性あるシナリオの構築 ・共通原因故障 <sup>13</sup> の可能性の特特定・評価

<sup>13</sup> 「一般に原子力発電所では、安全上重要な系統・機器は多重化などにより冗長性をもたせた設計となっており、異常事象発生時の安全炉停止操作に高い信頼性を確保するようになっている。このような冗長化された系統・機器が同一の原因で同時に機能喪失することを共通原因故障(common cause failure, CCF)と呼ぶ」。吉田智朗、「国内原子力発電所 PRA のための共通原因故障分析」、保全学 Vol.14, No.1 (2015)、p.77.



	<p>&lt;サプライチェーンにおける脆弱性の可視化&gt;</p> <ul style="list-style-type: none"> <li>原子力施設の重要構成要素のデジタル及び/または物理的サプライチェーンの可視化</li> <li>サプライチェーン内の脆弱な標的の特定・分析</li> </ul>
	<p>&lt;ソーシャルエンジニアリング<sup>14</sup>&gt;</p> <ul style="list-style-type: none"> <li>機密性の高い運転情報の取得、施設内の重要職にある職員に対する内部協力の働きかけ、極めて現実的かつ説得力のあるカスタマイズ型フィッシングメール<sup>15</sup>やソーシャルメディアを通じた情報操作キャンペーンの構築</li> </ul>
3. 攻撃の実施 攻撃が実行に移される段階	<p>&lt;サイバー攻撃能力の強化&gt;</p> <ul style="list-style-type: none"> <li>既知の脆弱性に対して機能するエクスプロイトコード<sup>16</sup>(攻撃コード)の作成</li> </ul>
	<p>&lt;データの改ざんまたは操作&gt;</p> <ul style="list-style-type: none"> <li>職員を欺く行為、違法行為の隠蔽、施設の運転手順やプロセスの意図的改変</li> </ul>

## 【結論】

報告書は、表 1 に記載したフロンティア AI がもたらし得るリスク分析に基づき、3 つの結論を導出しており、その概要は表 2 のとおりである。

表 2 フロンティア AI がもたらし得るリスク分析に基づいた 3 つの結論

結論
<p>1. フロンティア AI の開発者と核セキュリティの専門家が連携し、現実的なリスク・シナリオとその緩和策の検討の必要性</p> <ul style="list-style-type: none"> <li>核セキュリティの実施者(事業者)や規制当局は、施設に対するリスクの一部を評価できるが、急速に進化するフロンティア AI の能力を把握するには、フロンティア AI 関係者の知見が不可欠。特に核セキュリティの専門家は、フロンティア AI の現状能力を把握・理解する必要がある。</li> <li>核セキュリティの専門家は、フロンティア AI の開発者が原子力分野における高リスク領域を正確に理解し、その悪用を防止する効果的な方策の策定を支援できる。</li> </ul>
<p>2. フロンティア AI の開発者と核セキュリティの専門家の間でのリスク低減に関する責任共有体制の構築の必要性</p> <ul style="list-style-type: none"> <li>フロンティア AI の開発者は、自らが開発したモデルの安全性とセキュリティに対して一定の責任を負うよう動機付けられているが、原子力施設への攻撃を助長し得るあらゆる悪用の可能性を完全に排除する対策の設計は現実的ではない。このため、原子力施設特有のリ</li> </ul>

<sup>14</sup> 例えば IBM は、ソーシャルエンジニアリングを、「人々を巧みに操ることで、情報の共有、ソフトウェアのダウンロード、ウェブサイトへの訪問、犯罪者への送金、個人または組織のセキュリティを危険にさらすミス犯させる攻撃のこと」と定義している。IBM、「ソーシャルエンジニアリングとは」、<https://www.ibm.com/jp-ja/think/topics/social-engineering>

<sup>15</sup> 特定の個人や組織を標的とし、受信者が不審を抱かないように内容が巧妙に調整されたフィッシングメール

<sup>16</sup> ソフトウェアまたはハードウェアのシステム上の欠陥や弱点を悪用し、システムに侵入して攻撃を開始するコード。SentinelOne、「サイバーセキュリティにおけるエクスプロイトとは?」、<https://www.sentinelone.com/ja/cybersecurity-101/threat-intelligence/what-is-an-exploit/>

スクを低減するためには、核セキュリティ関係者も責任を分担し、協調的に対応する必要がある。

- 例えば、フロンティア AI の開発者は、原子力施設のレイアウトや脆弱性につながる故障モード等、機密性の高い情報を AI モデルが再構築しないよう、適切な防護方策を講じるべきである。一方、核セキュリティの規制当局や施設運転者は、フロンティア AI モデルの高度な情報収集・処理能力を踏まえた上で、適切なセキュリティ対策を講じる責任を負う。

### 3. フロンティア AI の進化に伴い、攻撃リスクの低減・対応責任が核セキュリティ関係者に過度に集中することになる

- フロンティア AI モデルが特定の原子力施設への攻撃に悪用される可能性を分析することは、核セキュリティ上、極めて重要である。その際には、安全、セキュリティ、運転システムに対するリスクを統合的に捉える「システムアプローチ」<sup>17</sup>の採用が求められる。特に各国は、サイバーと物理的セキュリティの適切なバランスの確保、攻撃発生時の運転レジリエンスの強化、原子力施設に関する情報の一般公開を通じた透明性の確保、といった課題について、早急に議論を開始する必要がある。
- オープンソース及びオープンウェイト型のフロンティア AI モデル<sup>18</sup>は、敵対者による防護措置の無効化が容易であり、構造的に高い脆弱性を有する。またフロンティア AI の開発者の中には、利便性の優先、リスク認識の欠如、あるいは悪意により十分なセキュリティ対策を実装しない事例も想定される。

## 【提言】

報告書は、表 2 に記載した結論に基づき、2 つの提言を行っており、その概要は表 3 のとおりである。

表 3 結論に基づいた 2 つの提言

提言
<b>1. フロンティア AI の開発者と核セキュリティ関係者の間における、継続的かつ非公式なコミュニケーション・チャンネルの確立</b> <ul style="list-style-type: none"><li>• 現時点では、核セキュリティとフロンティア AI モデルの双方に高度な専門性を有する人材は極めて限られている。両分野における技術的理解を相互に深めるためには、両者間で継続的な対話の枠組みを確立することが不可欠である。</li><li>• 核セキュリティの規制当局や政策立案者は、フロンティア AI の開発者との非公式かつ常設的なコミュニケーション・チャンネルを通じて、AI モデルの能力に対する理解を深めることができる。このようなチャンネルは、関係者間の連携強化や、両分野に精通した専門家の育成支援、情報共有の促進に資するのみならず、フロンティア AI モデルが核物質及び関連施設の安全性向上に貢献し得る可能性について議論する場としても機能し得る。</li></ul>
<b>2. フロンティア AI モデルがもたらす核セキュリティ上のリスクの動的(dynamic)かつ体系的、そして変化する性質を踏まえた核セキュリティ体制と対策の構築</b> <ul style="list-style-type: none"><li>• 将来の核セキュリティ対策においては、フロンティア AI モデルを含む新たな、かつ動的なリスクへの対応が不可欠である。しかし、こうしたリスクへの対応の必要性や対応能力は国毎</li></ul>

<sup>17</sup> 物事を全体として捉え、構成要素の関係性や相互作用を重視する考え方

<sup>18</sup> モデルのコードや設計、学習方法等が公開され、誰でも自由に閲覧、使用、改良が可能な AI モデル

に異なるため、段階的かつ柔軟なアプローチを考慮することが重要である。規制当局、政策立案者、事業者がこれらのリスクに対処する新たな戦略を策定するに当たり、国家レベルでの検討の出発点となり得る 5 つの要素は以下のとおりである。

- ✓ **データセキュリティ及び管理方針の最優先化:**  
フロンティア AI モデルの高度なデータ処理能力を踏まえ、データのセキュリティ確保及び管理方針の策定・実施を優先課題とし、戦略的に取り組む必要がある。
- ✓ **核セキュリティの体系的・包括的アプローチの導入:**  
フロンティア AI モデルが、複数のシステム間における共通原因故障の特定や、情報の偽造・改ざんを可能にする点を踏まえると、物理的防護とサイバーセキュリティの双方を統合したリスク評価手法の導入が不可欠である。
- ✓ **サイバーセキュリティ対策の強化と柔軟な適用:** エクスプロイトコードの自動生成や、自律的な目標達成能力を備えた AI 強化型敵対者の出現を見据え、状況に応じて柔軟に適用可能なサイバーセキュリティ対策を強化する必要がある。特に、デジタル・トランスフォーメーション(DX)の進展に伴い、原子力分野におけるサイバーリスク対策の重要性は今後一層高まると予想される。
- ✓ **サプライチェーンのセキュリティの強化:** フロンティア AI モデルが、敵対者による信頼性の高いサプライヤーの偽装を支援する可能性を踏まえ、原子力サプライチェーンにおけるデジタル及び物理的なセキュリティ対策の強化が求められる。
- ✓ **高度化するソーシャルエンジニアリング攻撃への対応戦略:** スピアフィッシング<sup>19</sup>や AI を活用した内部脅威者の採用といった新たな攻撃に対応するため、AI 強化型のフィッシングメール検知技術の導入や AI 搭載チャットボット<sup>20</sup>の悪用リスクを含む内部脅威対策訓練の強化が不可欠である。

<sup>19</sup> 特定の企業や個人を狙い、個人情報や機密情報の盗取を目的としたフィッシング詐欺

<sup>20</sup> 人間との対話を、AI 技術を活用して自動化するプログラム



## 2-1-2 「過去、現在、そして未来における原子力分野での AI の活用」の概要紹介

### 【概要】

核セキュリティ及びコンピューターセキュリティの専門家である Donald Dudenhoeffer 氏<sup>21</sup>が執筆し、VCDNP から発行された「過去、現在、そして未来における原子力分野での AI の活用」と題する論文の概要を紹介する。

本論文は、原子力分野における AI の導入状況と将来展望を体系的に整理し、原子力安全、核セキュリティ(物理的セキュリティとサイバーセキュリティ)、政策決定支援等、多様な活用可能性と課題を明示したものである。本論文は、「AI の概要」、「原子力分野における AI の導入状況」、「原子力産業界の見解(原子力産業界の実態調査)」、「AI 導入の課題」、「AI ガバナンスの概要」、「結論」の各章で構成されており、本稿では「AI の概要」を除いた各章の要点を紹介する。

### 【原子力分野における AI の導入状況】

これまで原子力分野では、性能監視や保守支援等、限定的な分野で予測 AI(predictive AI)が活用されてきた。近年では、Copilot や Gemini、ChatGPT 等に代表される大規模言語モデル(Large Language Model: LLM)を用いた生成 AI(generative AI)への関心も高まっている。しかし、LLM の実用化には、高品質かつ膨大なデータ、十分な計算資源、堅牢なネットワークインフラ整備が不可欠である。以下では、原子力分野における予測 AI 及び生成 AI の活用事例を潜在的な可能性も含めて紹介する。

### <原子力施設における AI の活用>

原子力施設における AI の導入は 1980 年代後半に始まり、当初はシステムの安全性や信頼性の向上、正常運転の確保が主な目的であった。近年は、デジタルトランスフォーメーションの進展により、施設の運転効率の向上、システムの可視化、安全の強化といったニーズが AI の導入を加速させている。以下の表 1 は、原子力施設の運転における AI の活用事例である。

表 1 原子力施設の運転における AI の活用事例

分野	活用事例
設計、エンジニアリング	炉心設計、熱流動シミュレーション・解析、放射線遮蔽設計
製造/サプライチェーン	燃料ペレット・集合体の欠陥の検出、偽造品・不正品(CFSI)の識別
運転・保守	状況監視、異常や故障の検知・検出、予知保全、ロボットや無人航空機(UAV)による点検、データやログの収集、作業計画/スケジュールの最適化、報告書の自動生成

<sup>21</sup> Dudenhoeffer 氏は、現在、アラブ首長国連邦(UAE)バカラ原子力発電所のエクゼクティブ・コンサルタント及びオーストリア技術研究所(AIT)非常勤研究員。米国海軍大学院(NPS)で理学修士を取得、国際原子力機関(IAEA)核セキュリティ部の上級情報技術担当官(Senior Information Technology Officer)を務めた経験もある。本論文は、氏が VCDNP 及びカナダ外務省の支援を受けて執筆し、VCDNP から発行されたもの。

廃止措置	ロボットによる解体、危険区域の調査
災害・事象対応	ロボットによる消火、遠隔監視、大気サンプリング、捜索・救助

## <デジタルツイン>

近年、原子力分野では、デジタルツイン<sup>22</sup>への関心が高まっており、米国では原子力規制委員会(NRC)がアイダホ国立研究所(INL)及びオークリッジ国立研究所(ORNL)と連携し、デジタルツインの開発と規制上の実現可能性に関する研究を進めている。デジタルツインは、システム性能の高度な評価、異常や故障の早期検知・検出、意思決定支援の高度化への寄与が期待されている。また、施設の運転者だけでなく規制機関にとっても、リアルタイムで施設の状況を把握・共有できるプラットフォームとして、規制の効率化に資する可能性がある。

## <原子力安全>

現在の原子炉には多様な自動安全機能が導入されているものの、運転と制御は依然として人間の判断に大きく依存している。統計によれば、原子力施設における事象(インシデント)の約80%は、人的要因に起因または影響を受けている。このため、ヒューマンエラーの低減を目的としたAIによる人的パフォーマンス支援への関心が高まっている。人間のパフォーマンスは、「知覚(perception)」、「認知(cognition)」、「反応・行動(response/action)」といった要素により形成されるため、それらを上手く支援するように設計されたAIは、人間のパフォーマンスを向上させる可能性がある。表2に、AIを人間の作業や意思決定の流れに統合し、上記3つの要素について、AIが人的パフォーマンスの支援を行う可能性のある領域を示す。

表2 AIによる人的パフォーマンス支援の主な領域

<ul style="list-style-type: none"> <li>・システム分析及び性能推定</li> <li>・アラーム管理と優先順位付け</li> <li>・ヒューマンエラーや異常動作の検知</li> <li>・プラント状態の評価と将来予測(状況認識支援)</li> <li>・複雑な情報の総合的処理と評価</li> <li>・インテリジェントHMI(ヒューマンマシン・インターフェース)<sup>23</sup></li> <li>・インテリジェント操作手順の提示<sup>24</sup></li> <li>・運転者のタスク遂行能力の拡張</li> <li>・異常事象の評価と対応判断の支援</li> <li>・AIを活用した個別最適化型の学習・訓練支援</li> <li>・運転経験や技術文書のレビュー及び検索支援</li> <li>・運転者の適正評価(例:タスク遂行能力の把握)</li> </ul>
--

<sup>22</sup> 物理的な対象やシステムの構造及び動作を忠実に再現するために設計された、仮想的なモデルや表現のこと

<sup>23</sup> 人間と機械の間のやりとりを、より直感的で効率的、かつ状況に適応したものにするためのインターフェース

<sup>24</sup> 効率的、また状況に応じて運転者をリアルタイムで支援するといった賢い操作方法や手順

## <AI への依存>

現在、原子力発電所の運転及び核セキュリティに関連する業務は依然として人間の操作に依拠しているが、AI 及び自律機能の導入は、業務の効率化や安全性の向上に資するものとして期待されている。AI は、状況評価や直観的分析、批判的思考、創造的な問題解決といった重要な機能を委ねられる可能性もある。一方で、AI へのこうした依存の高まりに伴い、人間中心の能力やスキルをいかに維持するか、また AI 機能が利用できない状況下で人間が適切に対応できる体制の確保が重要な課題となる。

## <核セキュリティ>

核セキュリティでは、「予防(prevention)」、「検知(detection)」、「対応(response)」の各段階において、物理的、技術的及び管理的な手段が講じられている。近年、AI は悪意ある行為(不正行為)の予防、検知、被害低減といった技術的対応の支援及び自動化手段として活用されつつある。また、原子力安全分野で蓄積された人的パフォーマンス支援の知見や議論は、核セキュリティ分野にも活用可能であり、両分野に共通する基盤としての活用が期待されている。

## <物理的セキュリティ>

原子力施設の物理的セキュリティは、「抑止(deter)」、「検知(detect)」、「遅延(delay)」、「対応(respond)」、「(脅威の)無効化(eliminate)」の5つの基本的な行動原則に基づいて構築されている。AI が警備員や対応部隊を代替することは想定されていないが、AI システムは彼らの判断や行動を支援する補完的な役割を担うことができる。例えば、AI は物理的防護システムの支援、初期侵入の防止強化、検知・評価時間の短縮、対応・阻止時間を削減できる。表3に、物理的セキュリティ分野におけるAIの活用事例を示す。

表3 物理的セキュリティ分野におけるAIの活用事例

分類	活用事例
アクセス管理・識別	顔認証、指紋スキャン、音声認識による個人識別・認証
監視・検知	アラームの評価・管理、内部脅威を含む不審な行動やパターンの自動検知(異常検知)、物理的侵入の検知、映像データ等の変更/改ざん検知、映像監視データの自動分析
状況認識・意思決定支援	センサー情報の統合による状況把握、予測分析による物理的防護システムの設計・対応計画の最適化、外部情報との連携によるリスクの早期把握
監視手段の高度化	ロボットやドローンによる遠隔・自律監視
脅威の特定	信頼性評価、身元調査
業務支援	ルーティーン業務の自動化

## <サイバーセキュリティ>

サプライチェーンは、セキュリティ上の脆弱性となり得る経路とされ、AI はその防護・検知手段として不可欠な存在となりつつある。AI は、ユーザー行動分析(User

Behavior Analysis: UBA)、侵入検知システム(Intrusion Detection System: IDS)、侵入防止システム(Intrusion Prevention System: IPS)、データ漏洩防止(Data Loss Prevention: DLP)等、様々なサイバーセキュリティ製品に組み込まれており、大規模データの分析や異常行動・不正行為の兆候の検知を支援している。一方で、敵対者も既に AI を悪用し始めており、攻撃の高度化に対抗するため、AI の検知・防護手段としての活用が一層重要となっている。表 4 にサイバーセキュリティ分野における AI の現行及び近未来の実用化事例を示す。

表 4 サイバーセキュリティ分野における AI の現行及び近未来の実用化事例

分類	実用化事例
検知・防護	侵入防止システム(IPS)による能動的な防護や侵入検知システム(IDS)による異常行動の検知、マルウェアやフィッシング/ソーシャル・エンジニアリング <sup>25</sup> の検出、ボットネット攻撃 <sup>26</sup> の識別、スパムメールの自動フィルタリング
脆弱性・リスク管理	コンピューターコード解析による脆弱性の可視化・検出、リスク評価と優先順位付け
事象(インシデント)対応	事象の影響分析と復旧支援、事象対応の自動化(機器やマルウェアの隔離、侵入防止)、セキュリティ情報・イベント管理(Security Information and Event Management: SIEM)アラートの分類と優先順位付け
認証・アクセス管理	ID 及びアクセス管理、ユーザー認証(多要素認証、生体認証)、ユーザー行動分析(UBA)
不正検出・情報活用	偽造または改ざんの検出、オープンソース・インテリジェンス(Open Source Intelligence: OSINT) <sup>27</sup> の活用、脅威インテリジェンス <sup>28</sup> の統合

## 【原子力産業界の見解】

AI の活用が広がる中、本論文の筆者は、原子力施設の運転者、規制機関、国際原子力機関(IAEA)、核セキュリティ協会(World Institute for Nuclear Security: WINS)、核脅威イニシアティブ(Nuclear Threat Initiative: NTI)等を含む原子力及び核セキュリティ関係の機関を対象に、原子力分野における AI 導入の現状と見解に関する調査を実施した。また、IFF リサーチ<sup>29</sup>が英国科学・イノベーション・技術省の委託により実施し

<sup>25</sup> マルウェアなどを用いずにパスワード等の情報を盗み出す手法

<sup>26</sup> 悪意のあるアクターによって制御される、インターネットに接続されたデバイスのグループによって実行されるサイバー攻撃の一種、ボットネット攻撃は、スパムの送信、機密情報の窃取、機密情報の侵害、広告詐欺の永続化、またはより危険な分散型サービス拒否や分散型サービス拒否攻撃(DDoS 攻撃、ネットワークや Web サーバーなどのリソースを標的とし、大量のリクエストを送信してオフラインにするサイバー攻撃の一種)を行うために使用される。CDNetworks, 「ボットネット攻撃とは何か、ビジネスを保護する方法」、<https://www.cdnetworks.com/ja/blog/cloud-security/botnet-attacks/>

<sup>27</sup> 一般に公開されている情報源からアクセス可能なデータを収集、分析、決定する諜報活動

<sup>28</sup> 脅威の防止や検知に利用できる情報の総称。従来のセキュリティでは見逃されていた高度なサイバー攻撃の検知、特定の業界・業種を標的とした巧妙なサイバー攻撃の防御が可能となる

<sup>29</sup> 英国を拠点とする独立系の社会及び市場調査会社。IFF, <https://www.iffresearch.com/>

た AI とサイバーセキュリティに関する調査<sup>30</sup>結果等、他産業での AI 導入に関する最新動向とも比較し、原子力分野特有の AI 導入の推進要因や潜在的な障壁を明らかにした。今次調査の主な結論を先に述べると以下のとおりである。なお、表 5 に今次調査の概要を示す。

- 原子力・核セキュリティ関係者を対象とした本調査の結果は、他産業における AI 活用の調査結果と概ね一致していた。AI 活用の動機には若干の差異が見られたものの、原子力分野では特に機密情報の保護や AI 導入に伴う課題への関心が高かった。
- 組織内で AI システムを導入し、既存業務プロセスと統合する際に考慮すべき事項が特定された(表 6 参照)

表 5 調査結果の概要

項目	内容
調査対象組織	原子力発電所の運転者(26%)、その他の原子力施設の運転者(19%)、原子力規制機関(19%)、アカデミア・研究機関(19%)、コンピューターセキュリティプロバイダー(4%)等
調査対象者の職種	約半数が管理職、残りは技術・研究職
専門分野	約 65%以上がサイバー・核セキュリティの専門家
AI に対する理解度	約 85%以上が AI を理解していると回答
AI 対応組織の有無	約半数以上の組織に AI 関連部署や内部体制が存在
ガバナンス体制	半数以上の組織で AI 関連規則・監督体制が未整備・整備中
AI 導入のインセンティブ	原子力分野では、「データ分析・研究」が主動機。一方、他産業では、「コスト削減」が最多。共通項目は、「業務の効率性」と「文書作成支援」。また、原子力産業界の回答者は人材管理と学習支援の可能性も潜在的なインセンティブとみなしていた
ロボティック・プロセス・オートメーション(RPO) <sup>31</sup> への関心	原子力産業界は他産業よりも RPO に関心を示し、原子力産業界の回答者の約 50%が RPO を導入済、または将来導入予定と回答
AI 導入状況	原子力産業界では AI の導入経験は限定的で、将来の導入にもより慎重な姿勢
主な AI 利用懸念	主な懸念は、データの喪失・漏洩、データ品質、プライバシー保護。特に原子力分野は、情報の機密性からデータ保護への関心が高い
主な AI 導入障壁	主な障壁は、機密情報の漏洩リスク、不正確な出力、意図的または偶発的な誤用。その他、AI 導入の必要性への疑念、経営層の支援不足、人間中心スキル維持への配慮など

<sup>30</sup> Department for Science, Innovation and Technology, UK Government, “Research and analysis: AI cyber security survey - main report”, 15 May 2024, <https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/ai-cyber-security-survey-main-report> 調査対象者は種々の業種(電力・ガス・空調供給業;水道業;下水道・廃棄物管理・環境修復業;運輸・倉庫業;製造業;卸売・小売業;情報通信業;金融・保険業;専門・科学・技術サービス業;医療・社会福祉業)の英国企業計 350 社

<sup>31</sup> データ入力や請求書の処理といった人がパソコンで行ってきた単純作業をソフトウェアのロボットに任せられる技術



表 6 AI システム導入の際の考慮事項

項目	考慮事項
目的と価値	導入目的と解決すべき課題の明確化、導入する価値の定義
法令・規制対応	適用される法律・規制要件の確認、コンプライアンス上の課題の把握
コスト	初期導入コスト、運用・保守コストの見積り
役割と責任	「ガバナンス」、「データ収集」、「モデル開発」、「テスト」、「運用」の各フェーズにおける役割と責任の明確化、核セキュリティ要件と責任の所在整理
人材とスキル	導入・維持・運用に必要なスキルの特定、既存人材スキルの再構築
技術・リソース	必要なハード・ソフトウェア要件の確認、内部・外部委託リソースの適切な配分設計
第三者依存とリスク管理	開発・運用・保守における外部依存の程度とリスク管理手法
倫理	AI 開発・運用に関する倫理基準・原則の明確化
データ管理	入力データの種類・収集・品質・網羅性の確認、データの保存・処理方法の設計方針、データの保存・処理方法・保管場所の明示、外部接続時の情報漏洩リスク管理 (特に OpenAI 等の公開 LLM との接続)
知的財産と出力管理	AI モデル・入力/出力データの所有権の明確化、出力形式と業務プロセスへの統合方法、出力情報の機密性・アクセス権限・制御手法 (最小権限、知る必要性の原則 <sup>32</sup> 等)
組織・人材への影響	労働力構成への影響、業務再設計、人材再配置、スキル再構築
信頼性・安全性・更新性	正確性・一貫性の検証手法と指標、誤作動・故障時の影響と対応方策、障害モードと復旧措置の設計、データセキュリティとプライバシー保護の法令準拠と監視体制、データ更新に伴うモデルの再訓練・更新手順

## 【AI 導入の課題】

原子力分野への AI 導入に当たっては、データ品質、インフラ、人材、信頼性、セキュリティ、倫理等、多岐に亘る課題への対応が求められる(表 7 参照)。

表 7 原子力施設における AI 導入の課題

項目	内容
データ	原子力施設のような複雑で特殊な環境では、施設特有のデータセット <sup>33</sup> と綿密なデータ収集戦略が不可欠。稀な事象への対応にはシミュレーションデータの活用も重要 (一般に AI モデルには、「特徴量 (features) <sup>34</sup> の 10 倍程度のデータポイント <sup>35</sup> 」が必要とされる)

<sup>32</sup> 特定の情報や資産にアクセスすることができるのは、当該情報が業務遂行に必要な不可欠な場合に限定されるというもの

<sup>33</sup> 例えば、プラントの性能、運転履歴、技術文書、運転員の経験、専門家の知見等に関するデータ

<sup>34</sup> 対象物を識別したり、評価したりするために使用される数値や記述情報。例えば、音声認識では、特定の個人や実態の声を正確に識別するために、ノイズ比、音の長さ、周波数等の特徴が必要となる場合がある。

<sup>35</sup> 統計やデータ分析において使用される、計測や調査によって得られた単一の具体的な情報、または観測値

必要とされるインフラ	グラフィックス処理ユニット(GPU) <sup>36</sup> やテンソル処理ユニット(TPU) <sup>37</sup> 等の計算基盤、クラウドやネットワーク環境、モデル開発・訓練の枠組み、デプロイ環境 <sup>38</sup> 等の整備が不可欠
人材・労働力	データサイエンティスト、AI/データエンジニア、機械学習エンジニア、に加え、核セキュリティ専門家といった専門人材の確保が不可欠。既存の職務環境の変化に伴い、スキルの再定義や継続的な研修が必要となる
透明性と説明可能性	AI の信頼性確保には、「透明性」と「説明可能性」(explainability)が不可欠。うち「透明性」には、①AI 生成コンテンツの出所と意図の明示、②AI システムの前提や動作原理の理解が含まれる。一方、「説明可能性」とは、AI の判断根拠を人間が理解・検証できることを意味し、①「予測精度」、②「追跡可能性(traceability)」、③「意思決定過程の理解可能性」の3つが重要な要素とされる
性能・監視	AI の期待通りの動作と性能要件の達成には、継続的な監視が不可欠。特に LLM では、「意図の誤解釈」、「エンティティ <sup>39</sup> 認識エラー」、「文脈処理の失敗」、及び「AI ハルシネーション」 <sup>40</sup> といった不正確な出力が課題
悪意ある使用(不正使用)のリスク	欧州連合サイバーセキュリティ機関(ENISA) <sup>41</sup> は、AI がランサムウェアやマルウェア、ソーシャルエンジニアリング等の攻撃手法を高度化・自動化する手段として悪用されていると指摘 <sup>42</sup> 。特にディープフェイク <sup>43</sup> 技術は、ソーシャルエンジニアリング、選挙操作、偽情報攻撃、身元盗用、金融詐欺等に利用されるリスクがある
攻撃手法の高度化	データポイズニング(学習データへの不正データ混入による誤学習の誘導)、回避攻撃(誤認識の誘発・検知回避のための入力操作)、推論攻撃(出力分析による機密情報の推定)、モデル抽出(多数のクエリを通じた AI モデルの特定・複製や脆弱性の特定)といった新たな脅威が出現
情報漏洩リスク	LLM を用いたコンテンツ生成において、意図せぬ機密情報の露呈リスクが存在(例: Teams 会議の議事録作成での機密情報の取り扱い、情報の断片的な蓄積による全体像の露呈等)。特に原子力分野では、個人情報、企業秘密、輸出管理関連情報に加え、保障措置及び核セキュリティ関連の機微な情報漏洩が施設の保安に悪影響を及ぼす可能性があり、多層的かつ厳格なセキュリティ対策が必要

<sup>36</sup> 画像や映像の描画に必要な計算を高速で処理するための半導体チップ

<sup>37</sup> Google が機械学習や深層学習の処理を高速化するために開発した半導体チップ

<sup>38</sup> 開発した AI モデルを実際のビジネスやサービスで利用可能な状態にするためのシステム環境

<sup>39</sup> 人名、組織名、地名、日付などの固有の情報

<sup>40</sup> 事実に基づかないコンテンツ(幻覚)を生成する現象のこと

<sup>41</sup> European Union Agency for Cybersecurity、旧称は European Network and Information Security Agency: ENISA であり、旧称の略語が現在でも使用されている

<sup>42</sup> European Union Agency for Cyber Security (ENISA), “ENISA Threat Landscape 2024”, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

<sup>43</sup> AI を用いて生成された偽りの画像や映像、音声、またはそれらを生成する技術

## 【AI ガバナンスの概要】

AI の信頼性と倫理性を確保するには、組織内における明確なガバナンス体制が不可欠であり、以下の要素を包括的に整備すべきである。

- AI 関係者の役割と責任の明確化
- 責任ある AI 構築についての教育の実施
- AI 及び AI リスクの設計・管理・監視・情報共有プロセスの確立
- AI の性能と信頼性を高めるためのツールや仕組みの活用

表 8 に、マイクロソフト社 CEO のサティア・ナデラ氏が作成した AI に関する「法律(laws)」<sup>44</sup>及び米国国防総省(DoD)の AI の「倫理原則(Ethical Principles)」<sup>45</sup>を示す。

表 8 ナデラ氏の AI に関する「法律」と DoD の AI 倫理原則

マイクロソフト社のナデラ氏の AI に関する「法律(laws)」	
<ul style="list-style-type: none"><li>• 人類を支援するよう設計されるべき</li><li>• 高い透明性を備えること</li><li>• 人々の尊厳を損なうことなく効率性を追求すること</li><li>• 知的プライバシーを設計段階から組み込むこと</li><li>• アルゴリズムに説明責任を持たせ、人間が是正可能な仕組みを備えること</li><li>• バイアス(偏り)の発生を防止すること</li><li>• 人間の共感能力の維持は不可欠</li><li>• 公平な教育機会とスキル構築の促進</li><li>• 人間の創造性を豊かにする存在であること</li><li>• 最終的な責任は人間が負うこと</li></ul>	
DoD の AI 倫理原則	
AI の責任ある運用(Responsible)	最終的な責任は人間が負う
公平性(Equitable)	バイアスの最少化
追跡可能性(Traceable)	開発・運用プロセスの透明性と理解確保
信頼性(Reliable)	明確な用途定義とライフサイクル全体での検証
統治可能性(Governable)	意図しない挙動に対する人間の制御能力の確保

また、米国立標準技術研究所(National Institute of Standards and Technology: NIST)、米国電気電子学会(Institute of Electrical and Electronics Engineers: IEEE)、国際標準化機構(International Organization for Standardization: ISO)、及び国際電気標準会議(International Electrotechnical Commission: IEC) 等も、AI の開発・利用に関する基準や指針を策定している。その他、欧州連合(EU)や経済協力開発機構(OECD)も、AI に関する法令や基準(standards)、ガイダンス等を提示しており、国際的なガバナンスの枠組みが形成されつつある。

<sup>44</sup> GeekWire, “Microsoft CEO Satya Nadella lays out 10 Laws of AI (and Human Behavior)”, 28 June 2016, <https://www.geekwire.com/2016/microsoft-ceo-satya-nadella-10-laws-ai/>

<sup>45</sup> U.S. Department of War, “DOD Adopts Ethical Principles for Artificial Intelligence”, 24 February 2020, <https://www.war.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/>



## ＜原子力規制における AI の活用＞

AI の進展は、原子力規制機関に新たな課題を突き付けているが、多くの規制機関では、AI の影響を的確に評価するための専門知識や体制が未整備である。こうした状況を踏まえ、NRC は、原子力安全及び核セキュリティに対する AI の潜在的影響を評価するための能力と方法論を確立すべく、「人工知能戦略計画」<sup>46</sup>を策定した。同戦略では、以下の 5 つの目標が掲げられている。

- ・ 規制上の意思決定に向けた準備態勢の確保、
- ・ AI 関連申請の審査に対応する組織的枠組みの構築
- ・ AI に関するパートナーシップの強化・拡大、
- ・ AI に精通した人材の育成、
- ・ NRC 全体における AI の業務活用に向けた具体的検討と実証

更に NRC は、AI の自律性に応じた人間との責任分担を明確化するため、「AI 自律性のレベル分類法(a taxonomy of AI autonomy levels)」を策定した(表 9 参照)。この分類では、AI の自律性が高まるほど人間の介入は減少する一方、システム障害や誤作動が原子力安全・核セキュリティに影響が大きい場合には、より厳格な規制上の監視が求められるとされている。

表 9 AI 自律性のレベル分類(要約)

レベル	意思決定主体と AI の役割	AI の原子力安全・セキュリティへの関与
0: AI 未使用 (AI not used)	AI は使用されていない	関与なし
1: 洞察 (insight)	AI が人間の意思決定を支援	安全性・セキュリティ・制御に影響を与えない範囲で、最適化や業務支援等、非本質的領域に限定
2: 共同 (collaboration)	AI がプラントの運転に関する勧告を生成し、人間が意思決定	勧告が安全性・セキュリティ・制御に影響を及ぼす可能性があり、人間が審査・実行
3: 運用 (operation)	AI が意思決定を行い、人間の監督下で実施	AI が安全性・セキュリティ・制御に関わる操作を実行し、人間が監督
4: 完全自律 (fully autonomous)	AI が人間の介入無しに意思決定・実行	安全性・セキュリティ・制御に関わる操作を AI が単独で実行(人間の監視・介入を前提としない)。重大な影響の可能性有り

## ＜AI システムとリスク＞

原子力施設に AI やデジタル技術を導入する際には、安全性及びセキュリティへの影響を適切に評価する必要がある。NRC は、「サイバーセキュリティ規則」<sup>47</sup>において、特定の技術に限定せず、安全・セキュリティ・緊急時対応等の重要システムの保護を

<sup>46</sup> NRC, “Artificial Intelligence Strategic Plan: Fiscal Years 2023-2027 (NUREG-2261)”, 23 May, <https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr2261/index>

<sup>47</sup> NRC, “§ 73.54 Protection of digital computer and communication systems and networks.”, <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054>

---

義務付けている。一方、英国原子力規制機関(Office for Nuclear Regulations: ONR)は、AI システムはライフサイクルを通じて安全かつ堅牢に機能すべきであり、リスクは継続的に特定・評価・管理されるべきであると強調している。また、AI の判断や行動には、透明性と説明可能性(explainability、内容や仕組みを説明できること)が求められるとしている<sup>48</sup>。

NRC の「AI 戦略計画」を受けて、NRC、カナダ原子力安全委員会(Canadian Nuclear Safety Commission: CNSC)、ONR の 3 機関は、原子力施設における AI 導入に関する検討事項をまとめた共同報告書を作成した<sup>49</sup>。同報告書では、NRC が採用した AI 自律性の 4 段階モデル(表 9 参照)を用いて、AI の故障(failure)が原子力安全及び核セキュリティ機能に及ぼす影響の重大性と、各自律性レベルにおける人間の補完可能性を評価している。

同報告書では、AI の自律性が高くても、故障時の影響が限定的であれば、比較的容易に AI が導入・受容される可能性があるが、故障時の影響が重大である場合には、導入にはより強固な根拠と厳格な検証が不可欠であるとしている。

さらに AI 検証の主要な課題として、以下の 3 点を指摘している。

- AI の基準が未整備であること
- 非決定論的かつ不透明な AI モデルの挙動により、説明や再現が困難となり、検証や信頼性に問題が生じること
- 原子力施設における AI 活用の実績が限定的であること

これらの課題は、規制機関の慎重な姿勢や導入の停滞の原因となっており、原子力事業者及び規制機関の双方における AI と運用環境に対する理解の深化が求められている。

## 【結論】

原子力産業界は、運転・保守コストの削減、人的ミスの削減、人材育成能力の強化、さらには膨大な運転データやビックデータの分析ニーズといった観点から、AI システムの導入を積極的に推進すると考えられる。一方で、AI には本質的な限界があり、誤作動や失敗のリスクを内包している。したがって、原子力事業者及び規制機関は、AI の失敗がもたらし得る影響の許容範囲を慎重に評価し、AI の導入・運用に際しては明確な基準とリスク情報に基づく体系的なアプローチを確立する必要がある。これにより、安全性、信頼性及び持続可能性を確保しつつ、AI の適切な導入が可能となる。

【報告:政策調査室 田崎 真樹子】

---

<sup>48</sup> ONR, “ONR policy: ONR’s pro-innovation approach to AI regulation”, Issue No.: 1, April 2024, <https://www.onr.org.uk/media/v45dkpu2/onr-pro-innovation-approach-to-ai-regulation-paper.pdf>

<sup>49</sup> CNSC, ONR, NRC, “Considerations for developing artificial intelligence systems in nuclear applications”, September 2024, <https://www.nrc.gov/docs/ML2424/ML24241A252.pdf>

---

### 3. 活動報告

#### 3-1 日本核物質管理学会第 46 回年次大会参加報告

2025 年 12 月 2 日～3 日、東京科学大学大岡山キャンパスにおいて日本核物質管理学会(INMMJ)第 46 回年次大会が開催された。昨年度に引き続き対面とオンラインのハイブリッド開催であり、計 108 名の参加登録があった。ISCNからは、1 件の講演及び、政策調査研究、人材育成支援及び技術開発に関して計 8 件の発表を行った。

以下にそれぞれの発表について概要を報告する。

##### 講演

発表者: 清水 亮

タイトル: イランの核問題に関するこれまでの動向



イランの核問題について、核開発の動機から現在に至るまでの経緯を紹介するとともに、イランのウラン濃縮活動について、IAEA の報告書等の情報から、濃縮規模、遠心分離機的能力について分析した結果を紹介した。さらに、米国、イスラエルによるイランの濃縮施設への軍事攻撃を巡る混沌とした状況について、現状と見通しを紹介した。質疑においては、イランの核問題を巡る米国の動向についての質問があった。

##### 政策調査研究

政策調査研究に関しては、以下 3 件の発表を行った。

発表者: 田崎 真樹子

タイトル: 原子力施設への攻撃に関する米国の論理 ―国際人道法の観点から―



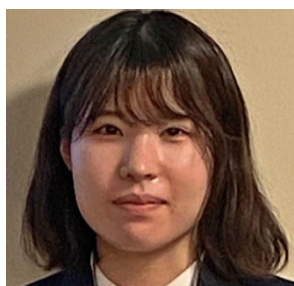
本発表では、①ジュネーブ諸条約第一追加議定書第 56 条第 1 項(ダム、堤防、原子力発電所への特別の保護)成立過程における米国の立場、②米国国務省の戦争法マニュアル、③イラク戦争や 2025 年 6 月のイラン攻撃など、米国による原子力施設攻撃の事例と、国際人道法の三原則(区別・予防・均衡)への配慮状況を分析し、原子力施設への攻撃に関する米国の論理の解明を試みた。米国は、原子力施設が軍事目標となり得るとの立場をとりつつも、実

---

際の攻撃に際しては国際人道法の三原則を踏まえ、個別に是非を判断している。今回のイラン攻撃に対し、米国は核兵器を保有する北朝鮮には有効な対応を取れていない現状を踏まえ、今後は攻撃に依存せず、国際協調に基づく持続的かつ実効的な対応策の構築が求められる。

発表者:今村 有里

タイトル:浮体式原子炉の課題と対応策の整理



本報告では、浮体式原子炉の特性に起因する核不拡散・核セキュリティ・国際法上の課題とその対応策を整理した。これらの課題に対処するためには、まず供給国・受入国間の二国間協定、さらに経由国を含む多国間協定の策定が重要となる。しかし、国際水域では、事故時の補償確保が難しいことから、合意形成は容易ではない。そのため、諸国間の合意形成に向けた制度的取り組みと、合意の前提となる浮体式原子炉技術への国際的な信頼醸成が不可欠だと本報告では結論付けた。本報告に対しては、調査を行う際、原子力船の事例は参照したかという質問を受けた。

発表者:加藤 優弥

タイトル:SMR のセキュリティ・バイ・デザイン:研究炉と実用炉の核セキュリティ規制要件の比較



本報告では、日本の研究炉と実用炉の PP 要件の主要な差異 5 点を示し、熱出力の小さい炉に期待される PP 措置の考え方を、想定されるリスクの違いから説明を試みた。その結果、区分II実用炉と比べて、区分II研究炉は妨害破壊行為のリスクが低い一方で、盗取のリスクが高いと考えられることが、両規則の PP 要件の違いを生んでいると推測された。次に、小出力の炉に期待される PP 措置の考え方から、SMR の SeBD のあり方について考察した。

---

## 能力構築支援

能力構築支援に関しては、以下の1件の発表を行った。

タイトル:2時間前通告模擬補完的アクセス教材の開発

発表者:石川 由紀



ISCN は 2024 年に IAEA と協力し、2 時間前通告の補完的アクセスビデオ教材を作成した。この教材は、ISCN が 2021 年に開発した 24 時間前通告の補完的アクセス版を元とし、2 時間前通告の補完的アクセスの流れを教材としたものである。この教材は IAEA ウェブサイトで公開し、IAEA 加盟国にも提供されている。JAEA 原子力科学研究所では、一般職向けに、2 時間前通告の補完的アクセスの重要性を説明するセミナーを開催し、本教材を活用した。セミナーは盛況のうちに終了し、参加者は円滑な IAEA 査察を進めるために、実践に活かすべき重要な点について学んだ。

## 技術開発

技術開発に関しては、以下3件の発表を行った。

発表者:ロッシ ファビアナ

タイトル:保障措置のための核分裂性物質定量に向けた中性子共鳴分析システム開発

試料中に含まれる核分裂性核物質を非破壊で定量するため、即発核分裂中性子、捕獲ガンマ線および透過中性子の共鳴解析を組み合わせた測定システムの開発について発表した。測定系として、試料周辺に配置したプラスチックシンチレータアレイと、下流側に設置した  $^6\text{Li}$  シンチレータから構成される検出系について説明した。近年の改良点として、高性能な EJ-276D プラスチックシンチレータの導入および最適化した波形弁別解析により、中性子／ガンマ線弁別性能を向上させたことを紹介した。また、京都大学の中性子飛行時間(TOF)施設において、天然ウランおよび濃縮ウラン試料を用いて実施した実験について概説した。会場からは、複数の検出器を用いていることを踏まえ、コインシデンス法の適用可能性に関する質問があった。



---

発表者:小泉 光生

タイトル:REFIT を使った中性子共鳴透過スペクトルの解析



本報告は、「REFIT を使った中性子共鳴透過スペクトル解析」のタイトルで発表を行った。中性子共鳴透過分析 (NRTA) 法は、パルス状に発生したビーム状の中性子が試料を透過して検出器に到着するまでの飛行時間 (TOF) とその量を測定する非破壊分析 (NDA) 技術である。中性子は、そのエネルギーにより試料に含まれる核種に特有な共鳴反応で減衰するので、得られる透過スペクトルから核種量 (面密度) を分析できる。発表では、京都大学のパルス中性子施設により測定したスペクトルを分析した結果について報告を行った。

発表者:高橋 時音

タイトル:大規模イベントにおける核セキュリティのための可搬型検出器を用いたリアルタイム放射線マッピングシステム

大規模イベント等において、核・放射性物質を用いたテロ等を未然に防ぐため、それらの持ち込みを迅速に検知するための技術開発を進めている。ガンマ線スペクトルと位置情報を測定する可搬型装置を持ち歩き、ネットワークを通じて測定データを一箇所に集めて、会場周辺の放射線分布をリアルタイムに可視化するシステムを開発した。実証試験では、地図上で放射線源の位置を特定し、さらにその位置で得られたガンマ線スペクトルを表示して、物質の種類を特定できることを示した。また、エネルギー分解能、検出効率を向上した新しい可搬型装置について紹介した。会場からは、今後の開発の方向性に関する質問があった。

【報告:政策調査室:清水 亮、田崎 真樹子、今村 有里、加藤 優弥  
能力構築支援室:石川 由紀  
技術開発推進室:ロッシ ファビアナ、小泉 光生、高橋 時音】

### 3-2 第 93 回及び第 94 回原子炉工学特別講座報告 上期・下期

本講座は、原子炉主任技術者資格取得のための受験対策講座として開講し、筆記試験合格のために必須となる知識を全 10 日間(上期、下期各 5 日間)で集中して学習できる内容となっている。令和 7 年度の開催形式として、上期は東京地区での対面、下期はオンライン形式で実施した。

第 93 回原子炉工学特別講座の上期は 5 月 26 日から 5 月 30 日まで、下期は 10 月 6 日から 10 月 10 日までの日程で実施した。第 94 回原子炉工学特別講座の上期は 6 月 9 日から 6 月 13 日まで、下期は 11 月 10 日から 11 月 14 日までの日程で実施した。受講者数(欠席者を除く。)は、第 93 回原子炉工学特別講座上期が 23 名、下期が 24 名、第 94 回原子炉工学特別講座上期が 26 名、下期が 25 名であった。

講義によっては理解するには難しいという意見もあったが、「今後の学習材料となる。」、「原子力以外の専攻であったが理解できた。」といった意見を頂いた。また開催方式については、対面・オンライン開催のいずれも支持する意見もあった。

なお、令和 7 年 3 月に実施した第 67 回原子炉主任技術者試験筆記試験の合格者 31 名の内、東京大学専門職大学院認定課程修了受験者を除く一般受験の合格者は 16 名で、そのうち 11 名が本講座(過去実施分を含む)の受講者であった。



対面開催の様子

【報告:人材育成推進室 仁尾 大資】

---

### 3-3 欧州委員会共同研究センター(EC-JRC)との運営委員会開催報告

2025 年 11 月 11 日、欧州委員会共同研究センター(European Commission - Joint Research Centre:EC-JRC)との運営委員会を開催した。本委員会は、1990 年に締結された「日本原子力研究開発機構と、欧州共同体委員会によって代表される欧州原子力共同体との間の核物質保障措置の研究及び開発に関する取決め」に基づき実施されるものである。

この協定は 1990 年以降継続的に更新されており、現行協定は 2021 年 5 月から 2026 年 4 月までの 5 年間。現在は、保障措置や核セキュリティに関する 4 件の協力課題が進行中である。

運営委員会は、協力課題に関する情報交換を目的として毎年 1 回開催されており、今年度は EC-JRC が事務局を務め、ベルギー・ヘール研究所を会場にオンライン併用で実施された。

会議冒頭では、EC-JRC 原子力安全・セキュリティ担当局長 Engelmann 氏より、EC-JRC の現状として原子力予算削減が続いており、原子力についてはカールスルーエ及びヘール研究所に集約されたことが報告された。また、ISCN 井上センター長からは、本年度 4 月より人材育成センターと統合し、新 ISCN がスタートしたことを紹介した。

その後、核鑑識、人材育成、非破壊測定及び標準試料に関する協力テーマ毎にその成果のレビューを行い、今後も協力を継続すること及び新たな協力として「プルトニウム核鑑識の技術協力」の開始が承認された。

共通の課題として、予算削減や、担当者の定年退職後の補充がなく人的リソースが減少していることが挙げられた。30 年以上にわたる協定で培われた技術と連携は世界に誇れる成果であり、今後さらに成果等の発信を強化していくべきとの提案があった。

また、現協定は本年 4 月で終了することから、協定を 5 年間延長することで合意し、長期的な協力体制の継続が確認された。

今回の運営委員会は、2026 年度秋に ISCN が事務局を務め、日本で開催される予定である。

【報告:原子力人材育成センター・核不拡散・核セキュリティ総合支援センター  
国分 陽子】



---

### 3-4 IAEA 研修「Integrated Workshop on Radiological Crime Scene Management and Nuclear Forensics」参加報告

本研修は、IAEA 主催の「Integrated Workshop on Radiological Crime Scene Management and Nuclear Forensics」として、放射線犯罪現場対応および核鑑識に関する知識・技能の習得を目的に開催された。研修はオーストリアの IAEA 核セキュリティ訓練・実証センターにおいて、講義と実習を組み合わせで行われた。

参加者は、コスタリカ、アゼルバイジャン、カザフスタン、レソト、エスワティニ、北マケドニア、韓国、日本から計 14 名で、警察、法科学機関、規制当局など多様な職種で構成された。講師は核鑑識専門家やインターポール職員など 4 名であった。

研修では、放射線犯罪現場における初動対応、証拠採取・輸送、核鑑識分析まで一連の流れを体系的に学んだ。講義では放射線・核鑑識の基礎、現場管理、安全装備、試料採取・封印、証拠品輸送などが扱われ、特に現場管理に関して新たな知見を得た。

初日から 2 日目にかけては、放射線・核鑑識の概要や証拠保全、犯罪現場での留意点を学び、「人命第一」の原則や計画・準備・訓練の重要性が強調された。模擬容疑者宅での実習では、防護服の着脱、放射性粉末の模擬調査、証拠品撮影などを体験した(写真 1)。鑑識経験のない執筆者にとって、指紋確認は特に印象的であった。3 日目には証拠採取・輸送に関する講義が行われ、インターポールによる実践的な採取技術や汚染防止の工夫を学んだ。証拠品輸送では、各国の規制の違いや欧州における国境越え輸送時の注意点が示され、計画的な採取と役割分担の重要性を再認識した。4 日目は核鑑識講義として、物理的特徴や元素・同位体分析結果を組み合わせた評価手法を学び、小型グローブボックスで証拠品開封や測定の実習を行った(写真 2)。最終日には、提示された同位体分析結果を基に報告書を作成し、チームごとに発表を行った。ウラン同位体結果の考察を通じ、証拠品間の関連性評価における不確かさの重要性を認識した。

本研修は、現場対応と核鑑識分析の両面を体系的に学べる点で非常に有意義であり、現場理解が分析結果の解釈やデータ品質向上に不可欠であることを再確認した。今後は、治安機関等の関係機関とも本研修の知見を共有していく予定である。



写真 1：模擬容疑者宅での調査の様子

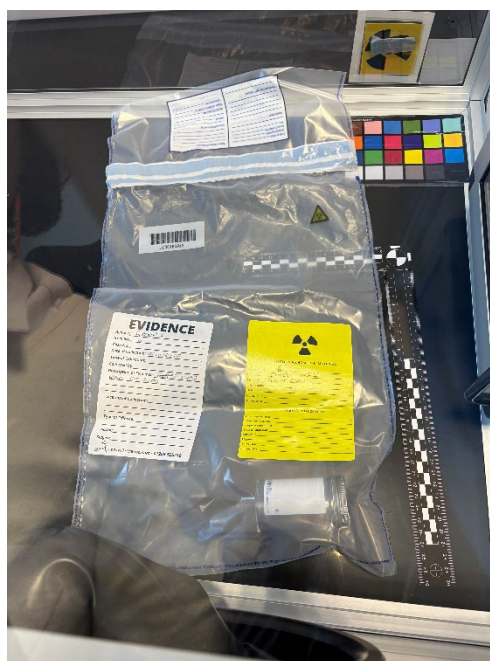


写真 2：押収した証拠品をグローブボックス内で開封する前の写真撮影

【報告:原子力人材育成・核不拡散・核セキュリティ総合支援センター  
國分 陽子】

---

### 3-5 ASEAN Energy Cooperation Week 2025 参加報告

2025 年 12 月 2 日から 3 日にかけて、インドネシア・ジャカルタにおいて「ASEAN Energy Cooperation Week 2025」が開催された。本イベントには、文部科学省核セキュリティ強化補助事業の一環として ISCN から 2 名が出席し、ASEAN 各国に対する原子力安全・核セキュリティ・保障措置(3S)分野の能力構築支援を今後も継続・拡大していく方針を発表した。

本イベントは、ASEAN Centre for Energy(ACE)が主催した。ACE は 1999 年に ASEAN 加盟国により設立された政府間機関であり、東南アジア地域のエネルギー政策を担うシンクタンクとして活動している。ISCN は ACE と覚書(MOU)を締結しており、アジア地域における核不拡散・核セキュリティ分野の人材育成支援を連携して推進している。

本イベントの主な目的は、「ASEAN エネルギー協力行動計画(ASEAN Plan of Action for Energy Cooperation: APAEC)2026～2030 年期」に関する計画案について、幅広いステークホルダーと意見交換を行うことであった。本イベントには、米国エネルギー省、仏国開発庁、豪州外務貿易省、英国外務・開発省、EU、韓国原子力協会、ASEAN 日本政府代表部等、約 30 の機関より約 80 名がステークホルダーとして参加した。

APAEC 2026～2030 年期では、エネルギー消費の効率化および再生可能エネルギーの導入拡大が主要目標として掲げられており、ASEAN 各国では原子力を低炭素電源の一つとして位置付け、今後の活用可能性について検討が進められている。

行動計画の 7 番目のテーマである「民生原子力エネルギー(Civil Nuclear Energy: CNE)」に関するセッションでは、ACE から、原子力発電は脱炭素化に貢献する手段の一つとして期待されている一方、ASEAN 各国における原子力導入や開発の進捗には大きな差があるとの説明がなされた。このため、原子力の潜在的な役割に対する理解を深めるとともに、関係機関・人材の能力向上を図ることが今後の戦略として示された。

これに対し、各ステークホルダーからは、自国で蓄積した技術やノウハウの共有に関する提案がなされた。具体的には、原子力規制、緊急時対応、放射性廃棄物管理、燃料サイクル、小型モジュール炉(SMR)に関する技術協力等について意見交換が行われた。また、加盟国間で原子力に対する関心や導入段階が異なる点への対応について質問があり、ACE は各国のニーズを丁寧に把握した上で、ケースごとに柔軟に対応していく方針を示した。

本セッションでは ISCN からも発言し、APAEC の前フェーズ(Phase II: 2021-2025)に ASEAN 諸国を対象に実施してきた各種トレーニングコースや研修生受入等の実績を紹介するとともに、ACE との協力関係を一層強化していく意思を表明した。これに対し ACE からは、特に 3S 分野および原子力規制に関する ISCN の取組に大きな期待が

---

寄せられ、今後も連携を継続していきたいとの発言があった。

本イベント終了後、ACE と打合せを行い、今後の具体的な協力について議論を継続することを確認した。APAEC Phase II に続き、2026 年以降も ASEAN との協力・連携を強化していきたい。

【報告:能力構築支援室 佐藤 優実】

### **3-6 技術報告 - Report from 2025 IEEE Nuclear Science Symposium, Medical Imaging Conference, and Room Temperature Semiconductor Detectors Symposium (IEEE NSS MIC RTSD) in Yokohama!-**

The weather was warm, the conference venue was excellent, and after several years of limited travel, it felt fantastic to be back at a fully in-person international event. We were able to meet new people, reconnect with the community, and speak with potential collaborators and vendors.

During the weekend, we attended several short courses and workshops. All three of us participated in a course on the use of AI in data analysis, a very timely topic, and we were eager to learn how these techniques can be applied to keep our research up to date. On Sunday, I also attended a workshop on the current status and future development of neutron beam facilities in Japan and abroad.

For the rest of the week, we showcased progress in three key technology-development areas:

(1) Delayed-gamma spectroscopy for active neutron analysis (Lead: Rodriguez)

We reported results from “sample-effect” experiments using the Fission Signature Assay Instrument (FSAI). This system was built to actively interrogate spent-fuel solutions to quantify uranium and plutonium. By testing surrogate metal solutions that mimic dissolved spent fuel, we compared activation rates and chemical contents with those from metal foils, gaining insight into future measurement performance.

(2) Wide-area, rapid nuclear/radiation detection for large event venues (Lead: Takahashi)

We introduced a new survey system designed to ensure that nuclear or radioactive materials are not brought into the area surrounding major public events. If something is detected, the system can quickly identify both the location and the radioactive isotope. We also presented a portable LaBr<sub>3</sub>(Ce) scintillation detector optimized for this mission.

(3) Advanced pulse-shape discrimination (PSD) using plastic and glass scintillators (Lead: Rossi)

We presented progress on sophisticated PSD techniques that cleanly separate gamma-ray and neutron signals. This boosts the reliability of measurement data and opens the door to more accurate nuclear-analysis systems. The poster drew significant attention, and

---

discussions confirmed both the importance of the technique and the potential value of our newly developed analysis code to the research community.

Overall, the conference was a great success, not only scientifically, but also as an opportunity to reconnect face-to-face with the global community. Winning the day-one photo contest was a wonderful start for me (picture below), and we returned energized, inspired, and eager to continue pushing our work forward.



(Photo by Fabiana Rossi)

【報告:技術開発推進室 Fabian Rossi】



---

## 4. コラム

### 4-1 フランス便り ～関根 恵～

みなさん、こんにちは。編集委員の関根です。私は JAEA の制度を活用してフランスからフルリモートワークをしています。今回はストラスブールのクリスマスマーケットの雰囲気をお届けします。子どもから大人まで、屋台やホットワインを楽しみながら、クリスマスに向けた飾りや雑貨、お茶やお菓子等、様々なお店を巡り楽しいひと時を過ごしていました。



クリスマスにちなんだオーナメントや人形



昼と夜、印象が変わるクリスマスツリー

---

## 編集後記

私は先日 20 歳を迎えました。

思い出にあふれた 10 代のゴールテープを切り、20 代というスタートラインに新たに立ちました。小学校や中学時代に「早くなりたい!」と考えていた「大人」にやっとなれたわけですが、特段、体に変化はありません。コーヒーが飲めるようになったわけでも、身長が大きくなったわけでも、嫌いな食べ物が食べられるようになったわけでもありません。それでも振り返ってみると 1 人で遠出をするようになったり、ゲームに費やしていた時間を別の趣味に使うようになったりなど、確かに自分に変化しているのだと感じました。

きっと、人は変化がないように見えても毎日ほんの少しずつ成長しているのだと思います。昨日よりも少しだけ考え方が広がったり、選択肢が増えたり。その積み重ねが、いつか振り返ったときに「こんなに変わったんだ」と驚くほどの大きな力になるはずです。そう信じながらこれから 20 代を歩んでいきたいと思います。

最後になりますが、以前開催された機構報告会ですが、開会挨拶前に 2025 年 10 月に 20 歳を迎えた職員が登壇していました。私も「もう少し早く生まれていれば。。。」と少し悔しさが残る瞬間でした。

(T.T)

**ISCN ニュースレターに対してご意見・ご質問等は以下アドレスにお送りください**

**E-MAIL: [iscn-news-admin@jaea.go.jp](mailto:iscn-news-admin@jaea.go.jp)**

\*\*\*\*\*

発行日: 2026 年 1 月 29 日

発行者: 国立研究開発法人日本原子力研究開発機構 (JAEA)

原子力人材育成・核不拡散・核セキュリティ総合支援センター (ISCN)