



【実務者向け短期プログラム】  
令和8年度（2026年10月開催）

# 重要インフラ分野における AIセキュリティトレーニング ご案内資料

2026年8月

独立行政法人  
情報処理推進機構  
産業サイバーセキュリティセンター



## 重要インフラ分野におけるAIセキュリティトレーニング ～ 産業制御システムの現場でAIを安全に使うために ～

### 対象者

主に重要インフラ分野の企業において

- AI導入に際して利活用の推進及びセキュリティ対策を企画・判断する方
- OT保全・制御技術部門、CSIRTの担当者

#### ◆ 推奨する前提知識

- 企業ITに関する基礎知識（ネットワーク、認証、ログなど）
- AIに関する基礎知識（プロンプト、LLM、学習データなど）

※ 専門的な知識（機械学習・制御システム）や開発経験（プログラミング経験）は必要ありません。

### 日程／会場

- 日程： 2026年10月26日(月)、27日(火) 各日10時～17時（予定）
- 会場： 独立行政法人情報処理推進機構  
東京都文京区本駒込2-28-8 文京グリーンコートセンターオフィス 8階  
<https://www.ipa.go.jp/about/location.html>

### 受講料／定員

- 受講料： 20万円（税込） ※ 受講料には、交通費・食事代は含みません。
- 定 員： 25名 ※ 定員に到達し次第、募集を締め切らせていただきます。

## 概要

- 主に重要インフラ分野の企業を対象に、AIを導入・活用する際に直面する課題やリスクを理解し、実践的な対応策を学びます。
- 1日目は、AIをセキュリティ業務に活用する「AI for Security」を中心に、フロンティアAIが脆弱性対応やセキュリティ運用に与える影響、AI活用を支えるデジタル基盤について扱います。2日目は、AIシステムを安全に構築・運用する「Security for AI」を中心に、LLMシステムへの攻撃、脅威モデリング、業務・産業分野へのAI導入に伴うリスクと対策を学びます。
- 講義、ハンズオン演習、グループディスカッションを通じて、AIセキュリティの基礎を体系的かつ幅広く学びます。実践的な攻撃・防御を体験するとともに、自組織におけるAI活用の課題や必要な対策を検討するための知識と材料を得ることができます。

※ 特定のAI製品に関する使用方法、攻撃コードの作成・侵入テスト（ペネトレーションテスト）については扱いません

## スケジュール（予定）

| 1日目 10時00分～17時00分 ※適時休憩あり                                          | 2日目 10時00分～17時00分 ※適時休憩あり                                      |
|--------------------------------------------------------------------|----------------------------------------------------------------|
| ・ AIセーフティ・インスティテュート（AISI）の専門家による講演                                 | ・ プロンプトインジェクション攻撃の体験と対策<br>疑似的なLLMシステムへの攻撃を通じて、弱点と基本的な対策を理解する  |
| ・ フロンティアAIと脆弱性対応の変化<br>AIの高度化が、攻撃・防御・脆弱性管理に与える影響を理解する              | ・ 脅威モデリング:MITRE ATLAS、STRIDE+AI<br>LLMシステムの構成を題材に、主な脅威と対策を整理する |
| ・ AI活用を支えるセキュリティ基盤<br>資産管理、SBOM、CI/CD、検査スキル(skill.mdによる検査の自動化)等を学ぶ | ・ AIの業務・産業利用に伴うリスク<br>RAG、アクセス管理、Physical AIを題材に、安全な運用を考える     |
| ・ AIを用いた脆弱性対応の実践演習<br>AIによる情報収集、リスク分析、優先順位付けを体験する                  | ・ AIセキュリティの実践課題を議論<br>AIに任せる範囲、人が判断する範囲、必要な対策などを議論する           |

## 特徴

AIをセキュリティ業務に活用する視点と、AIシステムを安全に利用する視点の両面から、AIセキュリティの基礎を学びます。重要インフラやOT(Operational Technology)で重視される安全性・可用性にも触れ、米国CISAなどの公開資料やIPA産業サイバーセキュリティセンター(ICSCoE)での知見を参照しながら、講義・ハンズオン演習・議論（グループディスカッション）を行います。

### 01

#### AIの活用と保護を両面から学ぶ

1日目は、AIをセキュリティ業務に活用する「AI for Security」、2日目は、AIシステムを安全に利用するための「Security for AI」を扱います。フロンティアAIの動向、脆弱性対応、プロンプトインジェクション、脅威モデリングなど、AIセキュリティの基本的なテーマを概観します。

### 02

#### OTへのAI導入に関する指針を紹介

CISAなどが公表した Principles for the Secure Integration of Artificial Intelligence in Operational Technology を参照し、重要インフラやOTでAI活用を検討する際の基本的な論点を紹介します。安全性・セキュリティ・可用性、人による監督、権限管理、フェイルセーフなどについて、具体例を交えて考えます。

### 03

#### 演習と議論を通じて理解を深める

講義に加えて、AIを活用した脆弱性対応やLLMシステムへの攻撃を体験するハンズオン演習を行います。グループディスカッションでは、AI導入時に生じる課題や、自組織で対応を検討するための視点を整理します。

## 東洋大学 情報連携学部 教授 満永 拓邦 氏

- JPCERT/CCにおいて、脅威情報の収集・分析やインシデント対応支援に従事。東京大学では、サイバー攻撃の実践演習環境「SiSOC TOKYOサイバーレンジ」の立ち上げと人材育成に携わった。
- 2017年からIPA産業サイバーセキュリティセンターの講師として、IT・OT双方のサイバーセキュリティ人材育成を担当。
- 現在は東洋大学情報連携学部教授。AIの安全な利活用、AIシステムに対する攻撃と防御、AIガバナンスなどを研究・教育している。FIRSTやBlack Hat Arsenalなどの国際会議においても、AIとサイバーセキュリティに関する研究成果を発表している。

## 東洋大学 情報連携学部 助教 岡田 怜士 氏

- 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」において、ITセキュリティ分野の講師を担当。
- 2019年から、インド太平洋地域の重要インフラ事業者等を対象とする「日米EU産業制御システムサイバーセキュリティ演習」にファシリテータとして参画。IT・OT双方の知見を生かし、セキュリティ人材の育成に取り組んでいる。現在は、AIを活用したシステムのリスク評価や、AIシステムに対する攻撃と防御に関する研究・教育にも取り組んでいる。

## 東洋大学 情報連携学部 特任研究員 渡會 航生 氏

- 2024年度から、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」において、ITセキュリティ分野の講師を担当。また、セキュリティ・キャンプのAIセキュリティ分野において講師を務め、若手人材の育成にも携わっている。OTセキュリティや事業継続計画（BCP）に関する研究・教育に従事するとともに、生成AIを活用したセキュリティ対策や、生成AIを安全に利用するための技術に関する研究を推進している。

## 留意事項

- ◆災害等のやむを得ない事情により、IPAの判断でトレーニングを中止することがあります。  
その場合でも、実施日の振替は行いません。中止した場合には、受講できなかった方へ受講料の返還等の措置を行います。ただし、中止に伴う受講できなかった方の不便、費用、その他の個人的損害については何ら責任を負いません。
- ◆その他詳細は、お申し込み後に受講案内等で別途ご連絡させていただきます。

## 募集期間

募集期間は**2026年10月2日(金) 17時**まで、**入金は2026年10月13日(火) 17時**までといたします。  
入金方法については、申込受付後、IPAから請求書をお送りしますので銀行振込にてお支払いください。

※ 定員に到達し次第、募集を締め切らせていただきますので、お早めにお申し込みください。

※ 同一組織から複数名の応募があった場合は、参加人数を調整させていただく可能性がございます。

## お申し込み方法

WEBフォーム上の受講申込書に必要事項をご記入いただき、お申し込みください。

※お申し込みいただきましたら、担当者よりご連絡を差し上げます。

お申し込みURL：<https://www.ipa.go.jp/jinzai/ics/short-pgm/ai-security/2026.html>

※ 原則として、納入後の受講料はキャンセルされる場合でも、返金はいたしかねますので予めご了承ください。

※ 請求書は押印省略で発行いたします。押印希望の方は、受講可否の確定後にご連絡ください。

## お問い合わせ先

電話 : 03-5978-7554 (直通)  
※受付時間：平日 9時30分-18時00分

メールアドレス：[coe-promo-ap@ipa.go.jp](mailto:coe-promo-ap@ipa.go.jp)

担当グループ : 企画部 事業推進グループ (お申し込みに関すること)  
: 事業部 人材育成グループ (演習内容に関すること)

### 【個人情報の取り扱いについて】

弊機構は、本トレーニングのお申し込みのためにご提供いただいた個人情報の適切な管理に努めております。

当該個人情報は、本トレーニングを提供するために必要な範囲（事務処理及び受講者リストの作成等）で利用させていただきます。

個人情報保護についての詳細は下記URLからご確認ください。

<https://www.ipa.go.jp/privacy/index.html>