

AIシステムセキュリティ実践～企業におけるAIのセキュアな導入・運用・ガバナンス

【会場】（4126292）

AIシステムを、データ、モデル、アプリケーション、API、クラウド、外部サービス、利用者、運用プロセスが連携する一つの業務システムとして捉えます。「AIを守る」「AIで守る」「AIを統治する」の三つの視点から、企業に求められるAIシステムセキュリティを体系的に解説します。

開催日時	2026年10月28日（火）13:00～17:00
会場	オンライン（Zoom）
定員	50名
参加費	無料
申込締切	2026年10月27日（月）18:00
申込方法	下記リンクから申し込みください。
申込リンク	こちら
主催	一般社団法人日本情報システム・ユーザー協会
協賛	（株）エヌ・ティ・エス・システム
お問い合わせ	03-XXXX-XXXX

主要内容

■受講形態

会場のみ（オンラインなし）

■テキスト

当日配布

■開催日までの課題事項

特になし

生成AIやAIエージェントの導入が急速に進むなか、「どの情報を入力してよいのか」「AIの出力をどこまで信頼できるのか」「AIにどこまで処理を任せてよいのか」「問題が起きたときに誰が責任を持つのか」といった課題が、企業の現場で顕在化しています。AIを安全に活用するためには、新しい技術だけを学ぶのではなく、既存の情報セキュリティ管理とAI固有のリスクを結び付けて考える必要があります。

本セミナーでは、AIシステムを、データ、モデル、アプリケーション、API、クラウド、外部サービス、利用者、運用プロセスが連携する一つの業務システムとして捉えます。

「AIを守る」「AIで守る」「AIを統治する」の三つの視点から、企業に求められるAIシステムセキュリティを体系的に解説します。

午前は、生成AI、RAG、AIエージェントの基本構造を確認したうえで、重要資産、データフロー、信頼境界、認証・認可、外部AIサービスの評価、多層防御について学びます。

午後は、プロンプトインジェクション、データおよびモデルのポイズニング、機密情報の漏えい、AIエージェントへの過剰な権限付与、サプライチェーンリスクなどを扱います。さらに、AIを活用したセキュリティ運用、Human in the Loop（人間による確認・承認）、AIシステムのインベントリ管理、責任分担、第三者リスク管理、継続的な監視について学びます。

講義では、社内規程や設計資料などを検索する生成AI型ナレッジ支援システムを導入しようとする架空企業A社を、終日共通のケーススタディとして取り上げます。

各セッションのワークショップを通じて、AI利用の分類、資産とデータフローの特定、攻撃シナリオと管理策の検討、自動化レベルの判断、AIセキュリティ管理策の設計まで、段階的に進めます。

特定の資格試験対策や製品・サービスの操作説明を目的としたセミナーではありません。

AIの導入を進める情報システム部門、セキュリティ部門、AI推進部門に加え、リスク管理部門など、AI利用のルールや責任体制を検討する方にもおすすめです。

自組織のAI利用に応用できる実務的な判断軸と管理策の初期案を持ち帰っていただくセミナーです。

◆受講前提

情報セキュリティの基本用語（機密性・完全性・可用性、認証・認可、ログ管理、リスク管理）を基礎的に理解していることを推奨します。演習はグループ討議を中心に実施するため、特定のAI製品のアカウントや操作経験は必須ではありません。