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	2027年3月23日(火) 10:00-17:00会場
JUAS研修分類	セキュリティ(サイバーセキュリティ)
カテゴリー	共通業務（契約管理、BCP、コンプライアンス、人的資産管理、人材育成、資産管理）・セキュリティ・システム監査
講師	安田良明 氏 （株式会社ラック 次世代サイバー技術開発本部　サイバー安全保障統括部 ） 1996年情報通信メーカーへ入社。システムズエンジニアとして、ナショナルセキュリティ分野に関する情報システム構築、セキュリティオペレーションセンター構築に従事する傍ら、2005年から2007年に掛けて、米国の情報保証技術の調査研究を行う。2009年株式会社ラックに入社。サイバーリスク総合研究所の研究員として、研究成果の製品化、特定用途システムへの転用提案や情報セキュリティ教育、人財育成などを担当。2010年ナショナルセキュリティセンターを設立し、初代センター長として就任。社会システムが期待する情報保証技術の調査研究を行うと共に、国家の安全保障を担うシステムに対し、自社の研究成果を提供し、社会セキュリティの確保に貢献する活動を行う。2011年内閣官房情報セキュリティセンターセンター員として、情報セキュリティ対策の推進に関する専門的、技術的な事項についての支援業務を行う。2013年S&J株式会社へ入社。組織の業務とITの状況を可視化し、トップダウンのガバナンスコンサルタントを行う。インシデントが発生したお客様に対して、インシデントレスポンスやデジタルフォレンジックを行い、ボトムアップからの支援も担当。2019年株式会社ラックに入社。SDGs 達成に必要となる社会環境を予測し、産業システム全般に必要となるセキュリティソリューションの企画開発を行う。
参加費	JUAS会員企業/ITC：35,200円 一般：45,100円（１名様あたり　消費税込み、テキスト込み）【受講権利枚数1枚】
会場	一般社団法人日本情報システム・ユーザー協会（NBF東銀座スクエア２F）
対象	AIの導入・運用に関わる情報システム、セキュリティ、リスク管理、AI推進部門の担当者・管理者
開催形式	講義、グループ演習
定員	25名
取得ポイント	※ITC実践力ポイント対象のセミナーです。（2時間1ポイント）
特記	◆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。
ITCA認定時間	6

主な内容

■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します。
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。