生成AI時代のクラウドセキュリティ入門_2026年11月1日～2027年1月31日開催【動画】(4326127)

パブリッククラウド上で生成AIシステムの企画・設計・運用に携わる方を対象に、「生成AI特有のセキュリティリスク」と、企業において活用ユースケースの多い「クラウド上でのRAG(検索拡張生成：Retrieval-Augmented Generation)システムにおけるセキュリティ」を中心に解説します。

開催日時	2026年11月1日(日) 動画配信開始 2027年1月31日(日) 動画配信終了
JUAS研修分類	セキュリティ(情報セキュリティ)、データ・AI活用・技術動向(AI・新技術　検証)
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 専門スキル
DXリテラシー	How(データ・技術の活用)：留意点
講師	小林弘典 氏 （NRIセキュアテクノロジーズ株式会社　研究開発センター　インテリジェンス統括部 エキスパート・セキュリティリサーチャー ） グローバルSIerやコンサルティングファームで、サイバーセキュリティやシステムリスク関連のサービスに従事。 直近では、サイバーセキュリティ関するリサーチ活動やAIを活用したシステム開発・サービス開発に携わっている。
参加費	JUAS会員企業/ITC：23,650円 一般：30,250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	オンライン配信（指定会場はありません）
対象	・「生成AIのセキュリティを理解しておきたい」、セキュリティ・情報システム部門担当者 ・自社サービスや社内業務に生成AIを組み込もうとしている開発者・企画担当者 ・クラウド上でシステム開発・運用に携わる開発者 ※クラウドやWebアプリの基礎がわかる方向けの内容です。 初級
開催形式	講義
定員	無制限
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	＊本録画は、2026年10月22日に開催したアーカイブ動画です。 ＊キャンセル規定について、動画開始日を開催日といたします。
ITCA認定時間	4

主な内容

■受講形態
録画視聴のみ　【録画視聴のご注意】
録画配信期間　：2026年11月1日～2027年1月31日
視聴時間めやす：約４時間
■テキスト
配信日当日よりマイページ掲載
■配信日までの課題事項
特になし

※本録画は、2026年10月22日に開催したセミナーのアーカイブ動画です※

クラウド上で生成AIを本格活用する企業が急増する一方で、
LLM（大規模言語モデル）特有の脅威やクラウドネイティブ基盤の複雑化により、セキュリティとガバナンスの再設計が喫緊の課題になって

います。
本セミナーは、パブリッククラウド上で生成AIシステムの企画・設計・運用に携わる方を対象に、「生成AI特有のセキュリティリスク」と、企業において活用ユースケースの多い「クラウド上でのRAG(検索拡張生成：Retrieval-Augmented Generation)システムにおけるセキュリティ」を中心に解説します。

「生成AIをもっと使いたいが、セキュリティ面が心配でブレーキを踏んでいる」
「専門用語だらけの資料は読んだが、自分のプロジェクトにどう落とし込めばよいか分からない」
といった方を対象に、基本知識と実装例を交えて解説します。

■ アジェンダ
1. 生成AIにおけるセキュリティリスク
生成AIを業務利用する際に直面するリスクと課題
攻撃メカニズムと攻撃実例の紹介（情報漏洩、誤回答、攻撃者の悪用等）

2. LLMを守るための基本的な考え方（ガードレール入門）
LLMにおける多層防御アプローチの紹介
主要クラウドサービスにおけるガードレールの例

3. RAG（社内ナレッジ検索＋生成AI）におけるセキュリティ
RAGアーキテクチャと脅威の理解
セキュアなナレッジベース構築の方法論
セキュリティ対策ポイントの解説

4. エンタープライズにおけるAIガバナンス
AIを業務利用するうえで意識したい「ガバナンス・リスク・コンプライアンス」

＜キャンセル規定＞
録画配信日を開催日といたします。あらかじめご了承ください。
・土日祝を含む開催７日前から前々日まで…参加費用の50%
・土日祝を含む開催日前日および開催当日（欠席）…参加費の全額
※受講権利チケット利用にてお申し込みの場合
・土日祝を含む開催７日前から開催当日…参加費の全額（必要枚数）
※動画視聴前であってもキャンセル料が発生しますので、ご注意ください。