

【GSX主催ウェビナー】

AIエージェントを“安全に開発し、安全に使う”には？
～SecuriST セキュアAIエージェント実装講座～参加費
無料

2026年8月5日 水 14:00～15:00(13:45 開場)

定員 50名

※ 事前登録制につき定員になり次第、受付を終了させていただきます。
※ タイムスケジュール、講演内容、講演者等は、予告なく変更される場合がございます。ご了承ください。

ウェビナー概要

生成AIの活用が急速に進む中、AIエージェントは業務効率化や自動化を実現する新たな手段として注目されています。一方で、外部ツールやAPI、社内データと連携し、自律的に判断・実行する特性から、従来のシステムにはなかった新たなセキュリティリスクへの対応が求められています。そのため、AIエージェントを取り扱うエンジニアやセキュリティ担当者には「攻撃を受ける前提で安全なAIエージェントを設計・実装・運用する視点」が必要不可欠となってきます。

GSXのご提供する『SecuriST セキュアAIエージェント実装講座』は、そんな「どこまで危ないのか」が判断できない」や「業務で使えるAIエージェントを作りたいが、セキュアな開発方法が分からない」といった課題を解決するための、実践型講座です。

本講座では、

- ✓ AIエージェントの仕組みや代表的な脅威を理解し、攻撃者視点でリスクを捉えられるようになる
- ✓ 安全な設計・実装・検証手法を、実践演習を通じて体系的に学ぶ

ことで、「安全にAIエージェントを構築・活用できる人材」を目指します。

本ウェビナーでは、講座監修者である上野宣氏をお招きし、AIエージェント特有のセキュリティリスクや、安全なAIエージェント構築についての考え方について解説していただきます。また、『SecuriST セキュアAIエージェント実装講座』講座で習得できる知識・スキルや実践演習の内容についてご紹介いたします。

さらに今回は、「AIエージェントへのハッキングデモ」を実演いたします。対策が不十分なAIエージェントがどのように悪用されるのかを実際の挙動を通じて確認し、安全な設計・実装の必要性を体感できる貴重な機会となっております。

こんな方にご参加をおすすめします

情報システム部門・セキュリティ担当者 / 社内開発エンジニア / DX推進・研修担当者 / AI活用ツールやサービスの安全性に責任を持つ方

皆さまのご参加を心よりお待ちしております。

※類似サービスを提供しているお客様の場合は、ご参加をお断りすることがございます。

セッション1

AIエージェントのリスクを体感する ～ハッキングデモ&セキュアAIエージェント実装講座紹介～

14:05-14:45
(40分)

株式会社トライコーダ代表取締役
OWASP Japan 代表
グローバルセキュリティエキスパート株式会社 社外取締役

上野 宣

AIエージェントへのハッキングデモを通じてセキュリティリスクを体感いただくとともに、それらへの対策を実践的に学べる「セキュアAIエージェント実装」講座の内容をご紹介します。

セッション2

受講形式・申込方法のご案内

14:45-14:55
(10分)

教育事業本部 事業企画部

『SecuriST セキュアAIエージェント実装講座』の受講形式・申込方法についてご紹介します。

Q&A

14:55-15:00
(5分)

オンラインでQ&Aを実施します。
講演中に「Q&A」へ登録されたご質問に対して講演後にご回答させていただきます。

■Webからのお申込み及び詳細について

https://www.gsx.co.jp/seminar/webinar_260805.html



【個人情報のお取扱いについて】

グローバルセキュリティエキスパート株式会社（以下「当社」といいます）はプライバシーポリシーに基づき、お客様の個人情報の取扱いに細心の注意を払っております。当社における個人情報の取扱いについての考え方を以下に記載します。

■個人情報の収集について

当社では次のような場合にお客様の個人情報をお聞きします。

1. 会員制サービスにご登録いただく場合
2. 各種セミナー等にお申し込みいただく場合
3. アンケートにお答えいただく場合

お客様はご自身の個人情報を明らかにすることなく当社のホームページをご利用いただけますが、一部のページへのアクセスおよび一部のサービスのご利用ができない場合がございますのでご了承下さい。

■個人情報の利用について

当社にご提供いただいたお客様の個人情報は、次のような目的の達成に必要な範囲内においてのみ利用いたします。

1. 申し込まれたサービスの提供のため
2. 申し込まれたサービス関連情報の提供のため
3. お問い合わせに対する対応のため
4. サービスの企画・向上のため
5. お客様に有用な情報を提供するため

■個人情報の管理について

当社は、お客様の個人情報の紛失、破壊、改ざん、漏えいなどが起こらないよう適切な安全管理策を実施し、厳重に管理します。

■個人情報の第三者への提供について

当社は、個人情報をお客様の承諾なしに第三者に提供することはありません。

なお、以下の場合を除きます。

1. 個人情報の取扱い業務の一部を社外に委託する場合
2. 裁判所など法令の定める事務を遂行することに対して協力する場合

■個人情報の問い合わせについて

お客様は当社に対し、当社が管理しているお客様の個人情報を問い合わせることができます。

個人情報の開示、訂正、削除を要求される場合またはその他お客様の個人情報に関するお問い合わせは、下記のお客様情報相談窓口までご連絡下さい。