報道関係者各位
プレスリリース

2026年3月19日

グローバルセキュリティエキスパート株式会社

GSX、AIセキュリティ人材育成を「SecuriST®」「EC Council」で本格化
初級～上級をカバーする講座群でAIセキュリティ人材向けラーニングパスを提供

グローバルセキュリティエキスパート株式会社（本社：東京都港区、代表取締役社長：青柳 史郎、証券コード：4417、以下「GSX」）は、AI利活用が本格化する中、企業が安心してAIを推進し、活用するために必要な知識と実践力を身につける認定資格講座の提供を開始します。

本講座は、GSXオリジナルブランド「SecuriST®」および日本総代理店を務める「EC Council」の両ブランドで展開し、初級者から上級者までを対象に、AIセキュリティ人材を段階的に育成するラーニングパスを提示します。

生成AIの業務利用やAI搭載サービスの開発が広がる一方で、リテラシー不足や不適切な利用に起因する情報漏えい、品質・安全性に関わるリスクへの対処は、まだ十分とはいえません。加えて、AIそのものを標的とした攻撃や、AIを悪用した攻撃など、AIの利活用拡大に伴い対応すべきリスクも多様化しています。

GSXはサイバーセキュリティ教育カンパニーとして、本講座を通じて、こうしたAIリスクに対応し、AIを安全に活用できる実務人材の育成を支援して参ります。また、AIの普及はGSXにとってはビジネス拡大の機会であり、講座提供を皮切りにAI普及を多面的に活用したビジネス展開を行うことで、事業拡大を実現して参ります。

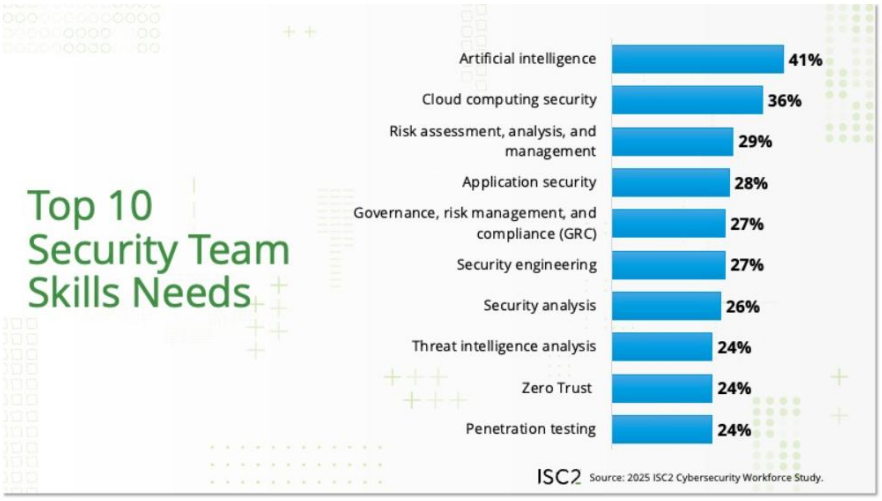
■　AIセキュリティ講座立ち上げの背景

エンジニアがプログラミングの生産性向上にAIを活用したり、AIでセキュリティ運用を効率化したり、AIを組み込んだサービスを開発するなどAIの活用が進んでいます。AIの利用が普及するにつれ、AIを安全に使えるようにする「Security for AI」、AIでセキュリティを強くする「AI for Security」という概念が浸透し始めています。

一方で、その使い方を一歩間違えると、情報漏洩につながる情報セキュリティ面の考慮を欠かすことができません。また、AI活用には「品質・安全リスク」という、重大なリスクにも直結します。さらには、AIを悪用して攻撃や不正が行われる点も見過ごせません。また、サイバー攻撃を行うハッカーもAIを活用して攻撃を仕掛けてくる点にも配慮が必要です。

しかしながら、エンジニアがAI利用に関するリスクを十分に認識せずに開発や運用に臨んでいたり、マネジメント側も十分な知識を持って事業運営ができていない実態があります。

そのため、エンジニアやマネジメントがAIに関する知識を十分に持ち、開発や事業運営を行っていくスキルを獲得することが急務です。ISC2の調査では、調査対象の41%が「セキュリティチームにAI人材が必要」と回答するなど、AIセキュリティ人材の育成には大きな需要が見込まれます。その対象は開発を行うエンジニアだけにとどまらず、マネジメントを行う事業責任者や経営陣にも及び、正しい知識を持ち、正しく実行していくことが求められます。

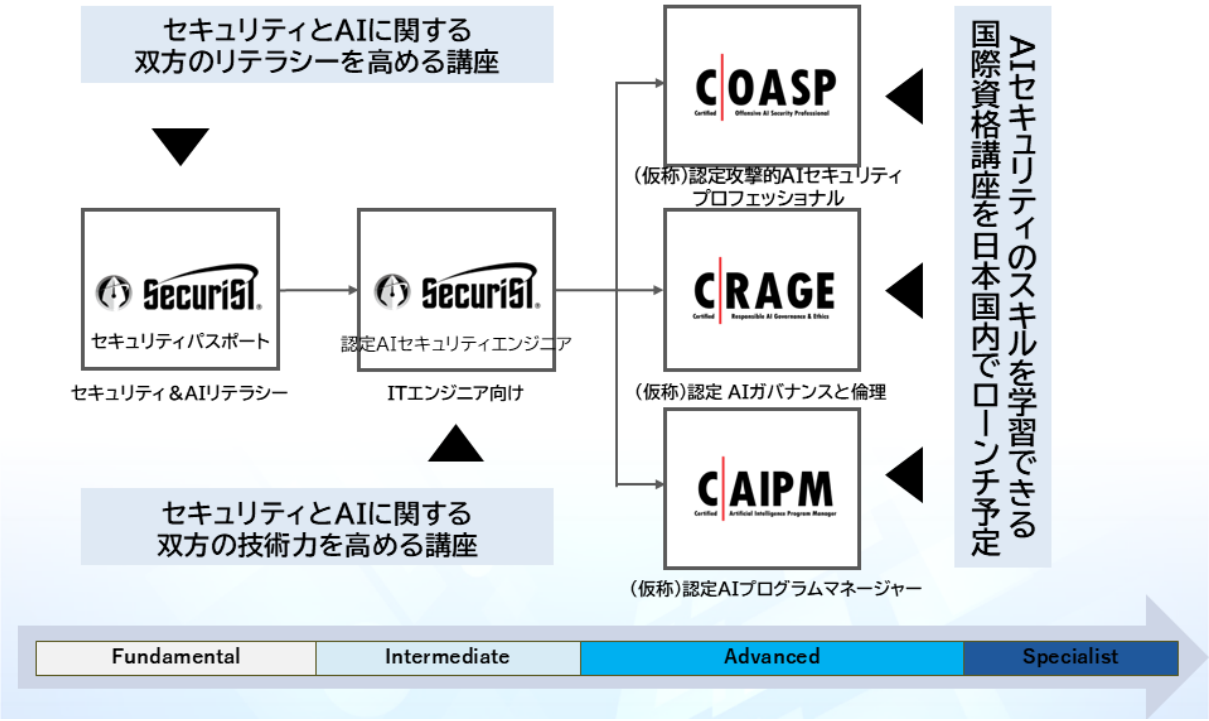


ISC2　Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities
https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

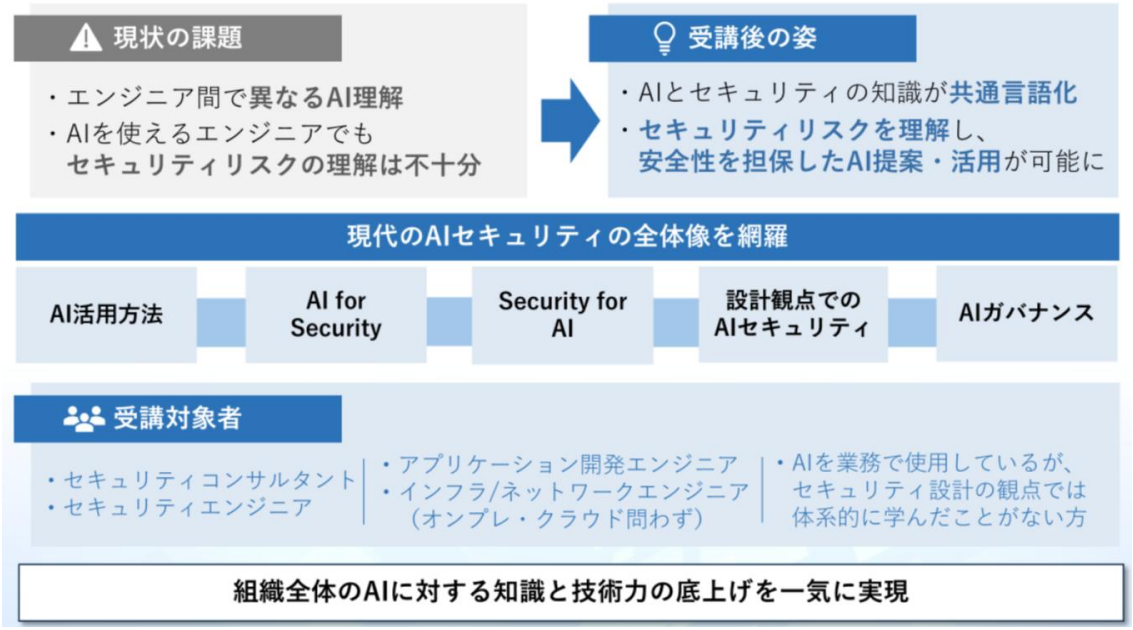
上記の背景を受けて、GSXはサイバーセキュリティ教育カンパニーとして、セキュリティに配慮してAIを利活用するためのスキルを身につけるエンジニア向け認定資格講座を、GSXオリジナルブランドである「SecuriST®」および、日本総代理店を務める「EC Council」の両ブランドで提供することといたしました。

■　AIセキュリティ人材を育成するラーニングパス

AIセキュリティ人材を育成していくためには、人材のレベル感に応じた育成プログラムが求められます。GSXではAIセキュリティ人材の育成にあたり、初級者向けに「SecuriST®」ブランド、中級者・上級者向けには「EC Council」ブランドでの育成手法を提供します。2つのブランドを組み合わせることで、AIセキュリティ人材を一貫して育成することができるラーニングパスをご提示します。



■ 【2026年3月開講】中級者向け認定資格講座|SecuriST 認定AIセキュリティエンジニア（Certified AI Security Engineer）
本講座は、AI for Security・Security for AI・AIシステム設計という主要な3つの観点について、講座監修者・上野宣氏が自身のホワイトハッカーとしての知見を基に、各分野の要素の繋がりと、現代のAIセキュリティの全体像を効率的に学習できるよう体系的に整理した講座です。



▽講座内容
-Module 1｜AI基礎
LLMの仕組み・ハルシネーションの構造的理由・プロンプトエンジニアリング、確率モデルとしての理解

-Module 2｜AI活用
コード生成・障害調査でのAI活用、AI出力のリスクと責任分界点、依存しすぎない実践ルール

-Module 3｜AI攻撃（攻撃者視点）
AIフィッシング・マルウェア開発補助・Prompt Injectionの実態、攻撃のコスト構造変化と防御優先順位の整理

-Module 4｜AI防御（防御者視点）
SOC/CSIRTでのAI活用・ログ分析・人間とAIの役割分担、AI防御の限界と評価

-Module 5｜AIセキュリティ設計
OWASP Top 10 for LLM 2025に基づく設計対策、MCP・Agentic AIセキュリティ、セキュリティ設計チェックリスト

-Module 6｜AIガバナンス
社内AI利用ガイドラインの策定、説明責任、インシデント対応、ISO/IEC 42001、AI関連法規の動向

-提供方法
オンデマンド/オンラインライブ

-費用

220,000円（税込み）/人
-提供開始時期
2026年3月

-サービス紹介ページ
https://www.gsx.co.jp/services/securitylearning/securist/ai_security_engineer.html

■ 【順次開講】中級・上級者向け認定資格講座|EC Council「（仮称）認定AIプログラムマネージャー（CAIPM）」
-講座内容
人工知能の基礎
AI運用とデータ管理
AI導入リーダーシップ
インテリジェントな自動化と迅速なエンジニアリング
AIセキュリティ
AIの応用と将来の動向

-提供方法
オンデマンド/オンラインライブ

-費用
未定

-提供開始時期
2026年4月以降順次

■ 中級・上級者向け認定資格講座|EC Council「（仮称）認定 AIガバナンスと倫理（CRAGE）」
-講座内容
AI 技術エコシステムと倫理的配慮
AI 戦略とガバナンス
AI リスク管理
開発と実装のガバナンス
運用と監査ガバナンス

-提供方法
オンデマンド/オンラインライブ

-費用
未定

-提供開始時期
2026 年 4 月以降順次

■ 中級・上級者向け認定資格講座|EC Council「（仮称）認定攻撃的AIセキュリティプロフェッショナル（COASP）」
-講座内容
攻撃的な AI セキュリティの基礎

AI による偵察と脅威プロファイリング
AI システムの悪用手法
AI モデルとライフサイクル攻撃
ガバナンスと防御エンジニアリング

-提供方法
オンデマンド/オンラインライブ

-費用
未定

-提供開始時期
2026 年 4 月以降順次

◆グローバルセキュリティエキスパート株式会社

社名：グローバルセキュリティエキスパート株式会社
東京本社：〒105-0022 東京都港区海岸1-16-1 ニューピア竹芝サウスタワー10F
代表者：代表取締役社長　青柳 史郎
証券コード：4417
上場証券取引所：東京証券取引所グロース市場
資本金：546百万円（2025年12月末）
設立　：2000年4月（グローバルセキュリティエキスパートへの商号変更日を設立日として記載）
コーポレートサイトURL：https://www.gsx.co.jp/

【本リリース内容に関するお問い合わせ先】

グローバルセキュリティエキスパート株式会社　戦略統括部　マーケティング部
TEL：03-3578-9001　MAIL：mktg@gsx.co.jp