ISC2

AIに関するISC2試験のガイダンス

2026年4月2日

ISC2試験とAIセキュリティの概念

AIが組織の運営形態を急速に変化させる中、サイバーセキュリティの専門家はリスクとチャンスの両方に直面しています。脅威アクターはAIを活用して脆弱性を発見し、偵察を加速して高度にパーソナライズされたソーシャルエンジニアリング攻撃を仕掛けています。同時に、AIはサイバーセキュリティの専門家が反復作業を自動化し、脅威の検出を改善し、効率を高め、ヒューマンエラーの低減に役立ちます。

AIに関するISC2試験のガイダンスでは、AI関連の知識、スキル、能力が、世界的に認められたベンダーニュートラルなISC2サイバーセキュリティ認定試験のポートフォリオにどのように組み込まれているかを概説しています。このガイダンスは、50を超える主要なサイバーセキュリティ試験ドメインと200のサブタスクにおけるAI概念の出現状況を明らかにし、厳格で継続的なISC2の試験管理プロセスが、AI主導型に移行する世界で認定専門家が組織の資産を保護する準備をどのように整えているかを示します。

ISC2の認定試験は新たな動向とともに継続的に進化しています。

ジョブタスク分析(JTA)、試験ブループリントの作成、試験問題作成、レビュー、基準設定、および公開を含む3年ごとの厳格な試験改訂サイクルを通じて、ISC2から認定された専門家および専門知識を持つ現場の実務者が、試験が実務上の要件を確実に反映するよう取り組んでいます。AI機能が進化し、中核となるサイバーセキュリティ分野と交差するにつれて、これらの専門家は定期的にAIに焦点を当てたタスクとセキュリティ上の考慮事項を認定試験のブループリントに統合し、ISC2の資格が適切でタイムリーかつ厳密に保たれるようにしています。

AIセキュリティの概念は、セキュリティとリスクマネジメント、資産セキュリティ、セキュリティアーキテクチャとエンジニアリング、通信とネットワークセキュリティ、セキュリティ評価とテスト、セキュリティ運用とソフトウェア開発セキュリティなど、ISC2の中核となるサイバーセキュリティドメイン全体に継続的に統合されています。

AIセキュリティを組み込んだISC2認定試験のドメイン

ISC2のポートフォリオに含まれる9つの認定試験すべてに対応するこの試験ガイダンスは、サイバーセキュリティの専門家とその雇用主が、すべてのISC2認定資格が今日のAIサイバーセキュリティ慣行の最先端にとどまっていることを確信できるようにします。

Table of Contents	

2026年9月1日発行のCC試験概要について

Certified in Cybersecurity (CC) 認定資格は、サイバーセキュリティ人材に参入する個人にとってグローバルなゲートウェイです。AIが企業のテクノロジーにおける標準的な構成要素となるにつれ、エントリーレベルの専門家であってもそのセキュリティ上の影響を理解することが不可欠です。CC試験概要では、5つの分野すべてにわたって基本的なAI概念を統合しました。このアプローチにより、新しく業務に従事する人でもAI資産を特定し、自動化された脅威を認識し、こうした最新技術を安全に保つためのガバナンス体制を支えることができるようになります。

ドメイン1:セキュリティの原則

CC試験概要では、AIが情報セキュリティの中核となる柱に与える影響を基礎レベルで紹介しています。機密性、完全性、可用性エントリーレベルの専門家は、AIシステムに基本的なセキュリティ原則を適用する方法を理解しており、特に「モデルポイズニング」を防ぐ上でデータの完全性がいかに重要であるかに焦点を当てています。この統合にはAIの倫理的な利用も含まれており、包括的なセキュリティ文化の一環として、自動化された意思決定における透明性と偏りのない判断の重要性が強調されています。さらに、この分野は、より広範なガバナンス、リスク、コンプライアンス（GRC）の枠組みにおけるAIの役割を明確にするものです。受験者は、AIツールも従来のソフトウェアと同様に、組織のポリシーや法的要件の対象となることを認識している必要があります。これらの大枠の原則を理解することで、AI分野に参入したばかりの専門家は、AIの導入が組織のリスク許容度や倫理基準に沿ったものとなるよう、経営陣を支援することができます。

ドメイン2:事業継続(BC: Business Continuity)、災害復旧(DR: Disaster Recovery)、インシデント対応(IR: Incident Response)の概念

このドメインでは、CC試験の試験範囲にAIが組織のレジリエンスを複雑化させると同時に強化する仕組みが盛り込まれています。対応の観点から、受験者は、AIを活用したツールがセキュリティインシデントの早期発見にどのように役立つかについて、その基礎を理解している必要があります。CC試験概要では、初級実務者が、自動化された脅威に対応できるよう改訂された既定の手順に従うことの重要性が強調されており、侵害の疑いがある場合の初期対応において、実務者が的確な支援を提供できるよう確保することが求められています。

復旧と事業継続の観点から、この統合では、従来のデータだけでなく、AIサービスを支える特定の構成やデータセットのバックアップの必要性に重点が置かれています。

CC試験概要では、AIの性能低下が重要な業務に影響を及ぼす可能性があるとして、「モデルのドリフト」が事業継続上の潜在的なリスクの一つとして挙げられています。これらの概念を活用することで、CC保有者は、障害発生時および発生後も、インテリジェントシステムの可用性を維持するための支援を行う準備が整います。

ドメイン3:アクセス制御の概念

アクセス制御は防御の最前線です。受験者は、人間のユーザーと同様に、AI「ボット」や自動化されたサービスアカウントも、プロビジョニングからデプロビジョニングに至るまで、正式なライフサイクルを通じて管理されなければならないことを理解している必要があります。この統合により、最小権限の原則が強調され、エントリーレベルのスタッフは、自動システムが指定されたタスクを実行するために必要な権限のみを持っていることを確認できます。

さらに、CC試験概要には、行動分析を通じて認証を強化するためにAIがどのように使用されているかが記載されています。受験者は、多要素認証(MFA: Multi-Factor Authentication)の基本概念と、AIが「不自然な移動経路」や異常なログインパターンの検出にどのように役立つかを理解している必要があります。これにより、新しい実務者は、AIへのアクセスをどのように保護すべきか、またAIが企業全体においてユーザーの身元を保護する上で、いかに「影のパートナー」としての役割を果たしているかを理解できるようになります。

ドメイン4:ネットワーク セキュリティ

ネットワークセキュリティに関して、CCの試験概要には、AIがトラフィック監視や脅威の防止にどのような影響を与えるかについての基礎知識が含まれています。エントリーレベルの実務者であっても、単なる署名照合にとどまらない、AIを活用したファイアウォールや侵入検知システム(IDS: Intrusion Detection Systems)の概念を理解している必要があります。 これらのツールが機械学習を活用して異常なネットワーク動作を特定する仕組みを理解することで、受験者はダッシュボードを監視し、潜在的な異常を上級アナリストに報告する準備が整います。

この統合は、AIデータが通過する経路のセキュリティ対策も講じられています。CC試験概要では、AI開発環境を機密性の高い本番データから分離するためのネットワークセグメンテーションの重要性について説明しています。この基礎知識により、CCとして認定された専門家はゼロトラスト原則の実装をサポートし、ネットワークが価値の高いAIトレーニングデータを送信するための安全な環境であり続けることを保証できます。

ドメイン5:セキュリティの運用

最後のドメインでは、CC試験概要はAIと連携するセキュリティ専門家の日常業務に焦点を当てています。これには、セキュリティ情報イベント管理(SIEM: Security Information and Event Management)ツールがAIを活用してデータを相関分析し、「アラート疲労」を軽減する仕組みに関する基礎的な理解が含まれます。 受験者は、これらの自動化システムの出力を適切に処理する方法を理解しており、通常の自動化された処理と、人間の介入を必要とする優先度の高い事象とを確実に区別できます。

また、オフィス環境におけるWebベースのAIツールとLLMの安全な使用に焦点を当てた「AIワークスペースのセキュリティ」についても紹介します。受験者は、従業員が一般公開されているAIサービスを利用する際に生じるデータ漏洩のリスクを特定できるようになります。この領域に含まれるサブタスクは、自動化が進む現代において、受験者が効果的な「ヒューマンファイアウォール」として機能し、組織のデータの完全性を守れることを保証するものです。

2024年9月15日発行のSSCP試験概要について

Systems Security Certified Practitioner (SSCP) は、実践的なセキュリティ管理者にとって最高の認定資格であることに変わりはありません。AIツールが実験的なものから運用的なものへと移行するにつれて、SSCP試験概要は、実務担当者がこれらの技術を安全に実装、監視、管理できるように進化してきました。7つのSSCPドメインにAIトピックを組み込むことで、受験者は、自動アクセス制御の保護からリアルタイムのインシデント対応のための機械学習の活用まで、AIの技術的現実を管理できるかどうかがテストされます。

ドメイン1:セキュリティの運用と管理

SSCPの基礎領域において、AIの統合は、自動化システムに対して情報セキュリティの柱を適用する方法における根本的な転換に焦点を当てています。セキュリティ管理者は「アルゴリズムの完全性」によってAIの 出力が信頼性を保ち、改ざん防止がどのように保証されるかを理解する必要があります。自動化プロセスにおける倫理的ガイドラインと透明性の重要性を重視してAIを導入し、システムがより自律的になっても、確立されたセキュリティポリシーと組織基準に対する説明責任が維持されるように対応します。

さらに、このドメインはAI対応のセキュリティコントロールのライフサイクル管理にも取り組んでいます。実務担当者には、機械学習モデル特有の更新サイクルを考慮した変更管理プロセスをサポートする任務があります。この統合により、セキュリティ専門家は単なる受動的な観察者ではなく、AI主導のビジネスツールの機能的なセキュリティ体制の維持に積極的に参加できるようになります。

ドメイン2:アクセス制御

AI時代のアクセス制御では、新たな種類の「知能を持つ」非人間的な実体を管理することが求められます。このドメインでは、自動化されたタスクを実行するAIエージェントとサービスアカウントのID管理ライフサイクルに焦点を当てています。

この統合により、これらのエージェントに対して最小権限の原則が適用され、特定の業務範囲やトレーニング要件の範囲外にある機密データ層へのアクセスが防止されます。

さらに、AIが従来のアクセス制御メカニズムをどのように強化するかについても説明します。SSCPは、適応型認証および行動バイオメトリクスの導入を支援することで、AIを活用し、ユーザーのアクセスパターンにおける異常をリアルタイムで検知することができます。この双方向の統合により、AIによるシステムへのアクセスを保護すると同時に、AIを活用してアクセス制御アーキテクチャ全体の耐障害性と柔軟性を高めることが可能になります。

ドメイン3:リスク特定、モニタリング、分析

このドメインでは、実務担当者の焦点がAI固有のリスクの可視性と報告へと向けられます。組織は、「モデルドリフト」や疑わしいクエリパターンなど、ML環境に固有の侵害、危殆化指標(IoC: identify Indicators of Compromise)を特定するように管理者をトレーニングすることでAIを統合できます。受験者は、AIエンドポイントの脆弱性を評価するセキュリティアセスメントに関する知識を有しており、これらのシステムが組織全体のリスクレジスターおよび脆弱性管理ライフサイクルに確実に組み込まれることを確実にします。

モニタリングも、AIによる分析を取り入れることで大きな飛躍を遂げました。SSCPは、機械学習を使用してノイズを減らし、真のセキュリティイベントを特定する相関エンジンの結果を分析する任務を負っています。これらの自動化された視覚化および傾向分析ツールを組み込むことで、実務担当者は調査結果をより効果的に伝え、侵害が発生する前に重大なリスクを上層部にエスカレーションできます。

ドメイン4:インシデントレスポンスとリカバリ

セキュリティインシデントが発生した場合、スピードが最も重要な要素です。ドメイン4では、初期対応段階で自動プレイブックの使用とAI支援によるトリアージに重点を置いてAIを統合します。セキュリティ専門家は、AIが標的、もしくは加害者となった可能性に関するフォレンジック調査を支援し、モデルログの証拠の取り扱い(証拠の連鎖 (チェーン・オブ・カスティディ) など)が、法的および倫理的原則に従って行われることを確実にします。

復旧作業では、AI駆動型システムの復旧に伴う特有の要件に対応しています。これには、MLモデルとそれに関連するトレーニングデータのバックアップとリカバリの手順がしっかりしていることを確認することも含まれます。インシデント対応にAIを統合することで、現代のセキュリティ管理者は、脅威と防御策が機械並みのスピードで変化する環境においても、ビジネスの継続性を確保できるようになります。

ドメイン5:暗号

暗号技術のドメインでは、AIの基盤となるデータセットを保護する上で、暗号が果たす極めて重要な役割に焦点を当てています。この分野における統合では、トレーニングおよび推論の各フェーズにおいて「使用中のデータ」のセキュリティ確保に重点を置き、最新の暗号プロトコルを活用してデータ漏洩を防止します。また、量子コンピューティングや高度な暗号解読技術がAI資産の長期的なセキュリティに及ぼす影響を検証し、実務担当者がAI関連の機密情報に対して強靭な鍵管理を実装できるよう支援します。

さらに、AIによる意思決定の否認防止策として、ブロックチェーンやその他の分散型台帳技術の使用についても取り上げています。SSCPは、AIモデルの出力に暗号署名を適用することで、自動化された意思決定の出所が検証可能であり、データが転送中に変更されていないことを保証し、自律運用に必要な信頼を維持するのに役立たせることができます。

ドメイン6:ネットワークと通信のセキュリティ

AIワークロードが拡大すると、ネットワークアーキテクチャには特有の要求が課せられます。このドメインは、AIトラフィックを監視するネットワークベースのセキュリティデバイスの安全な配置と構成に焦点を当てることによりAIを統合します。実務担当者は、AIトレーニングクラスターを隔離するためのマイクロセグメンテーションを実装する知識を有しており、これにより、侵害されたAIインターフェースを足がかりとして攻撃者が組織ネットワーク内でのラテラルムーブメントを防ぐことができます。

また、ネットワーク境界の防御におけるAIの役割についても説明します。これには、高度な「低速攻撃」を検出してブロックできるAI搭載ファイアウォールと侵入防止システム(IPS: intrusion prevention systems)の管理が含まれます。SSCPは、AIを利用するIoT(Internet of Things)デバイスとモバイルエンドポイントの通信経路を保護することにより、ネットワークがインテリジェントアプリケーションにとって堅牢な環境であり続けることを保証します。

ドメイン7:システムとアプリケーションセキュリティ

最後のドメインでは、SSCP試験概要はAIアプリケーションをホストするシステムの日常的な運用管理に焦点を当てます。統合には、機械学習ライブラリのソフトウェア・サプライチェーンを管理し、アプリケーションのセキュリティテストにおいてAI特有の論理的欠陥が正しく考慮されるようにすることが含まれます。実務担当者は、これらのシステムの安全な導入とパッチ適用を監督し、「モデルハイジャック」または推論攻撃がアプリケーション層で確実に対策されるようにする任務を負っています。

多くのAIサービスはこれらのプラットフォームを介して提供されるため、モバイルとクラウドのセキュリティも大きな役割を果たします。SSCPは、コンテナ化されたAI環境の運用に関する知識を持ち、これらのアプリケーションと企業内の他のシステムをつなぐAPIのセキュリティを管理します。これにより、サーバーからエンドポイントに至るまで、アプリケーションスタック全体が、従来の脆弱性だけでなく、AIを活用した最新の脅威に対しても強靭な耐性を備えることが保証されます。

2024年4月15日発行のCISSP試験概要について

AIや機械学習が現代のビジネス運営の基盤となるにつれ、CISSP認定資格も進化を遂げ、サイバーセキュリティの専門家がこうした高度なシステムを管理、設計、防御できるよう支援しています。ISC2は、AIを独立したトピックとして扱うのではなく、CISSP試験要綱の全8つのドメインにわたって、AI特有のセキュリティタスクおよびサブタスクを継続的に組み込んでいます。これにより、防御の自動化にAIを活用しながら、アルゴリズムバイアス、データポイズニング、敵対的攻撃などの固有のリスクに対処する包括的なセキュリティアプローチが保証されます。

ドメイン1:セキュリティとリスクマネジメント

現在、セキュリティリーダーは、AI資産が組織のリスク態勢をどのように変えるかを深く理解する必要があります。このドメインにおいて、CISSP 試験概要では、MLモデルとLLMを既存のリスク管理フレームワークに統合することを強調しています。これには、AI倫理のガバナンスの確立とアルゴリズムバイアスの低減、自動化された意思決定プロセスが法律、規制、プライバシーの要件に沿ったものになるようにすることが含まれます。

さらに、AIの統合はサードパーティのリスク管理にも影響します。組織が外部のAIサービスプロバイダーへの依存度を高めているため、CISSPはAIサプライチェーンのセキュリティを評価するための準備を整える必要があります。これには、データ収集の透明性や、プロバイダー主導型モデルの新たな脅威に対する耐性を評価し、AIの導入によって企業のセキュリティ戦略に管理の行き届かない死角が生じないよう確保することが含まれます。

ドメイン2:資産のセキュリティ

資産セキュリティのドメインでは、データがAIの生命線であり、その保護が最も重要です。この分野は現在、トレーニングデータセット、事前トレーニング済みモデル、モデルウェイトなど、AI固有の資産の分類と取り扱いを対象としています。私たちは、これらのシステムを「学習」させるために使用される情報が悪意のある攻撃者によって改ざんされたり、汚染されたりしていないことを確認するために、AIライフサイクル全体を通じてデータの完全性を維持することに重点を置いています。

特にAIシステムが個人識別情報(PII: Personally Identifiable Information)を処理する方法に関しては、依然としてプライバシーがこのドメインの基礎になります。統合向けた取り組みは、AI環境内における差分プライバシーやデータマスキングといった技術的対策に重点が置かれています。MLモデルを価値の高い知的財産として扱うことで、セキュリティとプライバシーの両方の要件を満たす方法でデータの収集、保存、および最終的な破棄を管理するためのロードマップを提供します。

ドメイン3:セキュリティアーキテクチャとエンジニアリング

アーキテクチャとエンジニアリングのドメインでは、AIを安全にホストし、運用するために必要な構造的な防御策に取り組みます。これには、高性能AIコンピューティングのための安全なエンクレーブの設計や、プロンプトインジェクションや敵対的攻撃から身を守るための堅牢な入力検証メカニズムの実装が含まれます。CISSP試験概要では、クラウドベースのAIサービスに内在する責任分担モデルを検討することで

AIを取り入れ、基盤となるインフラストラクチャがニューラルネットワーク特有の計算負荷に対して耐性を備えていることを保証しています。

このドメインには、物理的および論理的なホスティング以外にも、セキュリティ要件として「説明可能なAI」のエンジニアリングが含まれています。特定のアウトプットに到達した過程を可視化するシステムを構築することで、セキュリティエンジニアはAIの挙動をより適切に監査できるようになります。この統合により、セキュリティアーキテクチャは単なるシステムの境界線にとどまらず、AIを活用したセキュリティ制御の検証と妥当性確認を支える透明性の高いフレームワークとなります。

ドメイン4:通信とネットワークのセキュリティ

AIワークロードがネットワーク上を移動する状況において、この分野では、膨大なデータセットの転送および分散型AIノード間の通信のセキュリティ確保に重点を置いています。統合には、AIトレーニング環境を企業ネットワークの他の部分から隔離するために、専用のマイクロセグメンテーションとゼロトラストアーキテクチャ(ZTA: Zero Trust Architecture)を導入することが含まれます。これにより、AIインターフェースが危険にさらされた場合でもラテラルムーブメントを防ぐことができます。

さらに、ネットワーク防御におけるAIの役割についても取り上げています。CISSPは、AIを活用したネットワーク検知・対応(NDR: Network Detection and Response)ツールが、従来のシグネチャベースのシステムでは見逃してしまう可能性のある異常なトラフィックパターンをどのように特定するのかを理解することが求められています。「エッジでの推論」に使用される通信経路を保護することで、AIを支える通信経路の機密性と可用性を確保します。

ドメイン5:アイデンティティおよびアクセス管理 (IAM: Identity and Access Management)

AI駆動型の世界では、アイデンティティは依然として主要な境界となります。ドメイン5において、CISSP試験概要では、人間以外のエンティティ、具体的にはAIエージェントや自動化されたサービスアカウントのID管理に焦点を当てています。この統合により、AIシステムが「最小権限の原則」に基づいて動作することが保証され、学習段階や実行段階においてAIが機密データリポジトリへの不正アクセスを取得してしまうような「権限の昇格」が防止されます。

CISSP 試験概要には、行動バイオメトリクスと適応型認証を通じてIDおよびアクセス管理を強化するためのAIの使用も組み込まれています。AIを活用してユーザーのログインパターンを分析し、異常をリアルタイムで検出することで、CISSPはより動的なアクセス制御を実装できます。この二重の焦点により、AIアイデンティティを保護すると同時に、AIを使用して組織全体のアイデンティティインフラストラクチャのレジリエンスを高めることができます。

ドメイン6:セキュリティの評価とテスト

セキュリティテストは、AIシステム向けの「レッドチーミング」を取り入れるよう進化させることが求められています。このドメインにおいてCISSP 試験概要には、回避攻撃や抽出攻撃に対するモデルの堅牢性をテストするための方法論が組み込まれています。専門家は、ソフトウェアのバグだけでなく、攻撃者に悪用される可能性のあるモデルの出力の「論理上の欠陥」 がないか、AIシステムを監査します。

さらに、AIを使用して脆弱性管理ライフサイクルを自動化することにも取り組んでいます。AIを活用したスキャンツールを統合することで、組織はリアルタイムの脅威情報に基づいて修復作業の優先順位を付けることができます。これにより、セキュリティ評価が特定の時点に限定されずに継続的に行われるようになり、従来のコードと複雑な機械学習アーキテクチャの両方における脆弱性を迅速に特定することが可能になります。

ドメイン7:セキュリティの運用

セキュリティオペレーションセンター(SOC)では、AIは戦力を倍増させる役割を果たします。この分野では、AIおよび機械学習(ML)をセキュリティオーケストレーション、自動化、および対応(SOAR: Security Orchestration, Automation and Response)プラットフォームに統合することに重点を置いています。CISSP試験概要では、AIを活用してばらばらなイベントを関連付け、セキュリティアナリストに詳細なコンテキストを提供することで「アラート疲れ」に対処し、インシデント対応の迅速化を図る方法について説明しています。

運用面では、本番フェーズでの「AIのセキュリティ」についても取り上げています。これには、時間の経過とともにAIのパフォーマンスが低下する「モデルドリフト」の監視や、実際の敵対的攻撃への対応が含まれます。CISSPは、従来のインシデント対応とAI固有の監視を組み合わせることで、組織のオペレーションの回復力が、自動化された脅威のスピードに遅れないようにします。

ドメイン8:ソフトウェア開発セキュリティ

AIがコードの記述方法を変革するにつれて、ドメイン8はモダンな開発ライフサイクルを保護するために進化してきました。CISSP試験の試験範囲には、AI支援型コーディングツールの使用が含まれており、LLMによって生成された「幻覚」的な脆弱性や、セキュリティ上の問題があるコードスニペットが誤って組み込まれるリスクに重点が置かれています。自動化されたAIセキュリティテストをCI/CDパイプラインに組み込み、これらの欠陥が本番環境に到達する前に検出することに重点が置かれています。

さらに、このドメインはMLライブラリとフレームワークに関連するソフトウェアサプライチェーンのセキュリティにも対応しています。専門家には、ソフトウェア層を標的とする「モデルハイジャック」や「推論攻撃」を特定して対応する任務があります。ソフトウェア開発ライフサイクル(SDLC: Software Development Life Cycle)にAIの要素を組み込むことで、最終製品の品質を損なうことなく、開発者がAIの効率性を最大限に活用できるようにします。

2026年8月1日より施行されるCCSP試験概要について

LLMやMLパイプラインのホスティングやトレーニングにおける主要なインフラとしてクラウド環境が定着する中、Certified Cloud Security Professional(CCSP)は、こうした課題に対応できるよう進化を遂げてきました。CCSP試験概要では、6つのドメインすべてにわたってAIセキュリティを明確に統合しています。これにより、クラウドアーキテクトとエンジニアは、データ主権やアーキテクチャの完全性を損なうことなく、AI駆動型のサービスを設計、展開、管理できるようになります。

ドメイン1:クラウドの概念、アーキテクチャ、設計

クラウドアーキテクチャのドメインにおいて、AIの統合は、特殊なAIワークロードをホストするためのクラウドサービスプロバイダー(CSP)の機能評価から始まります。アーキテクトは、サービスとしてのAI：AI-as-a-Service(AIaaS)に適用される責任分担モデルを理解し、特に、モデルインフラストラクチャに関するプロバイダーの責任がどこで終わり、モデルの構成やデータに関する顧客の責任がどこから始まるのかを明確に把握する必要があります。 これには、論理的な分離を維持しつつ、AIトレーニングに必要な膨大なスループットを処理できる高性能コンピューティング・エンクレーブの設計が含まれます。

さらに、このドメインでは、クラウド設計プロセス自体へのAIの統合についても取り上げています。CCSP試験概要では、耐障害性の高いAI環境を構築するための「Infrastructure as Code(IaC)」の活用、およびモデルの逆転や抽出のリスクを低減するためのクラウドネイティブなセキュリティ設計原則の適用が重視されています。CCSPは、クラウド・AIスタックの基盤にセキュリティを組み込むことで、インテリジェントなサービスがプロビジョニングされた瞬間から、スケーラブルであり、コンプライアンスに準拠し、防御可能な状態であることを保証します。

ドメイン2:クラウドデータセキュリティ

データはクラウドAIエコシステムにおける最も重要な資産であり、ドメイン2はAIライフサイクル全体にわたるデータの保護に重点を置いています。統合の取り組みは、大規模な「データレイク」やトレーニングセットのセキュリティに重点を置いており、AIを活用して機密情報が機械学習パイプラインに入る前に特定する、高度な検出・分類ツールを導入しています。CCSP 試験概要では、AIトレーニングデータを複数のクラウドリージョンで処理する場合の、データ主権と管轄リスクという特有の課題を取り上げています。

さらに、このドメインには、推論フェーズ中のデータを保護するために、準同型暗号化や差分プライバシーなどの技術的制御が組み込まれています。実務担当者は、AIノードで使用される一時的なストレージに伴う「データ残留」のリスクを管理し、機密性の高いトレーニング残差が完全に消去されるようにします。これにより、クラウドベースのAIを使用しても、誤ってデータ漏洩や世界的なプライバシー規制の違反につながることがなくなります。

ドメイン3:クラウドプラットフォーム&インフラセキュリティ

このドメインは、クラウドでAIを安全に実行するために必要な強化されたインフラストラクチャに焦点を当てています。CCSP 試験概要では、MLモデルをホストする仮想化レイヤーとコンテナ化レイヤーのセキュリティに取り組むことでAIを統合します。CCSPは、AIトレーニングクラスターを隔離するための高度なマイクロセグメンテーションを実施し、クラウドネイティブのハードウェアセキュリティモジュール（HSM）を活用して、モデルの署名やデータの暗号化に使用される暗号鍵を保護する役割を担っています。

さらに、物理的および論理的なインフラ防衛におけるAIの役割についても検討しています。これには、機械学習を活用してAIエンドポイントを標的とした高度な「Low and Slow」攻撃を検知・遮断する、クラウドベースのDDoS対策およびWebアプリケーションファイアウォール(WAF)の管理が含まれます。基盤となるクラウドプラットフォームのセキュリティを確保することで、AIを支えるコンピューティングリソースが常に利用可能であり、悪意のある操作に対して耐性を維持できるようにします。

ドメイン4:クラウドアプリケーションセキュリティ

クラウドアプリケーションがAI API を活用する傾向が高まるにつれ、ドメイン 4 はこれらの統合に関するセキュリティに対処するようになりました。CCSP試験概要には、AI駆動型クラウドアプリケーション向けのセキュア開発ライフサイクル(SDLC: secure development lifecycle)が盛り込まれており、セキュリティ対策が不十分なAPI呼び出しによるリスクや、アプリケーション層における「推論攻撃」の可能性に重点が置かれています。実務担当者は、AIベースの機能を標的としたプロンプトインジェクションや自動的なリソース枯渇攻撃から防御するため、堅牢な入力検証とレート制限を実装することができます。

このドメインでは、ソフトウェアサプライチェーンのセキュリティ、特にサードパーティのMLライブラリと事前トレーニング済みモデルの組み込みについても取り上げています。CCSPは、AIを活用したアプリケーションに対してセキュリティテストを実施し、自動化された「ハルシネーション」や論理的欠陥によって本番環境に新たな脆弱性が持ち込まれないようにします。これにより、クラウドアプリケーションが自律性を高め、複雑化していく中でも、そのセキュリティが確保されます。

ドメイン5:クラウドオペレーション

クラウドSOCにおいて、AIはクラウドから生成される膨大な量のログを管理するための不可欠なツールとして機能しています。ドメイン5における統合は、マルチクラウド環境全体での高度な脅威ハンティングおよびイベント相関分析にAIとMLを活用することに重点を置いています。受験者は、クラウドネイティブのSIEM/SOARプラットフォームが一般的なクラウド脅威への対応を自動化できることを認識し、これにより人間のアナリストは、高度に複雑なAI駆動型の攻撃への対応に注力できるようになります。

運用面では、このドメインはセキュリティ関連の「モデルドリフト」を検出するためのAIパフォーマンスの「継続的モニタリング」にも取り組んでいます。CCSPは、AIサービスの運用ベースラインを維持する責任を負っており、モデル出力に何らかの異常が生じた場合は、潜在的なセキュリティインシデントとして調査を行うよう確保します。この積極的なアプローチにより、クラウドベースのAIシステムは、運用期間を通じて信頼性と安全性を維持できます。

ドメイン6:クラウドガバナンス - 法律、リスク、コンプライアンス

最後のドメインは、クラウドベースのAIを取り巻く複雑な規制環境を対象としています。CCSP試験概要では、自動化されたデータ処理の法的影響や、GDPRやEU AI法などの枠組みにおける「説明可能性」の要件に焦点を当てることで、AIの要素を取り入れています。CCSPは、特にAIモデルが国境を越えてデータを処理および保存する方法を考慮したクラウドデータライフサイクル監査の実施方法を理解している必要があります。

この分野のリスク管理には、AIサービスプロバイダーの「ベンダーリスク」を評価し、そのセキュリティ管理と倫理ガイドラインが組織の基準に沿っていることを確認することが含まれます。また、AIが関与するクラウド環境におけるeディスカバリやデジタルフォレンジクスの役割についても解説し、急速に変化する法的環境において、実務担当者がインシデントを効果的に調査し、コンプライアンス遵守の監査可能な証拠を提示できるよう支援します。

2024年6月15日発行のCGRC試験概要について

Certified in Governance, Risk and Compliance(CGRC)は、セキュリティ、プライバシー、組織戦略の交差領域を管理する専門家にとって決定的な認定資格です。AIが重要な経営判断を左右する時代において、CGRC試験概要は、インテリジェントシステムをガバナンスするための強固な枠組みを提供するため、改訂されました。CGRCは、AI固有のタスクとサブタスクをリスクマネジメントフレームワーク(RMF)全体に組み込むことで、専門家がアルゴリズムの透明性、「ブラックボックス」リスク、および急速に進化するAIの世界的な規制環境における複雑な状況に対処できるようにします。

ドメイン1:セキュリティとプライバシーのガバナンス、リスクマネジメント、コンプライアンスプログラム

AI時代のガバナンスにおいては、アルゴリズムの透明性と自律型エージェントの倫理的な利用を管理するため、専用の監督委員会を設置することが必要です。このドメインにおいて、我々は、機械学習モデルの特有の非決定論的な意思決定プロセスを考慮に入れるため、従来のリスク管理の原則を適応させることで、AIを統合しています。これには、NIST AIリスク管理フレームワーク(AI RMF: AI Risk Management Framework)やISO/IEC 42001など、複雑に絡み合うグローバルな要件を、既存の企業コンプライアンス管理ツールにマッピングし、AI導入において統一的かつ倫理的なアプローチを確保することが含まれます。

さらに、この分野では、AIに特化した情報のライフサイクルに取り組み、学習済みモデルから機密データを削除しなければならない際の「マシンのアンラーニング」という技術的課題に焦点を当てています。CGRCの専門家は、AIを活用した分析技術を用いてLLMのトレーニングに対する厳格なプライバシー保護策を策定することで、組織のガバナンスプログラムが知的財産とデータの機密性を保護しつつ、責任あるイノベーションを推進できるようにしています。

ドメイン2:システムのスコープ

従来のスコーピング設定手法は、現代の機械学習データパイプラインが持つ広範かつ継続的な性質を捉えるために拡張されてきました。ドメイン2において、CGRC試験概要は、商用既製ソフトウェア(COTS: commercial-off-the-shelf)に内在するものを含め、組み込まれたすべてのアルゴリズムを特定することを専門家に求めている点で、AIを試験内容に組み込んでいます。これには、AIサブシステムの確率的な性質を文書化し、AIを活用した自動マッピングツールを用いて、急速に進化するクラウドネイティブインフラストラクチャの変化に追従できる動的なシステム記述を維持することが含まれます。

正確なスコーピングには、基本的なAIモデルトレーニング環境とアクティブな推論エンドポイントを明確に区別する必要もあります。 CGRCの実務担当者は、自然言語処理(NLP: Natural Language Processing)ツールを用いて技術文書からスコープの境界を抽出し、検証することで、評価の範囲が正確に定義されるようにしています。これにより、「スコープクリープ」が防止され、AIシステムのセキュリティとプライバシーの義務がすべての利害関係者に明確に理解されるようになります。

ドメイン3:フレームワーク、セキュリティ、プライバシーコントロールの選択と許可

AIシステムに適した防御策を選択するには、CSA AI Controls Matrixなどの専門的なオーバーレイを、従来のフレームワークのベースラインに統合する必要があります。このドメインでは、複雑でハイブリッドなアーキテクチャ全体にわたるコントロールの動的なマッピングと選択を自動化するために、AIの活用に重点を置いています。実務担当者は、主要なクラウドサービスプロバイダー（CSP）から引き継がれたAIセキュリティ対策を見極める方法を理解しており、AWS BedrockやAzure OpenAIなどの基盤モデルが、システムのセキュリティ計画において適切に考慮されるようにしています。

さらに、この統合は、プロンプトインジェクションや敵対的データポイズニングなど、AI固有の脅威を低減するための制御の調整に重点を置いています。AIアルゴリズムを活用し、モデルの固有のリスクプロファイルに基づいて最適な統制の選定を推奨することで、CGRCの専門家は複雑な統制の継承階層を迅速に文書化することができます。 これにより、選択した保護手段が国際標準に準拠しているだけでなく、最新のアルゴリズム攻撃に対しても技術的に有効であることが保証されます。

ドメイン4:セキュリティとプライバシーコントロールの実装

実装フェーズでは、分散型機械学習パイプラインへのAIネイティブのセキュリティ制御のシームレスな導入に取り組みます。この分野では、インテリジェントな「IaC: Infrastructure as Code」を活用して、これらの制御機能のプロビジョニングと設定を自動化し、ハイパースケール環境全体での一貫性を確保することに重点を置いています。実務担当者は、リアルタイムのAI推論エンドポイントに許容できないレイテンシーを発生させずに、セキュリティと運用パフォーマンスのバランスを取って、これらの保護手段を実装する戦略を開発する任務を負っています。

EU AI法などの新たな国際的要件に合わせて実装することによってさらにコンプライアンスが強化されます。CGRCの専門家は、保護されたテナントデータに対する不正なモデルの再学習を防止できるよう、プライバシー対策が技術的に十分に堅牢であることを保証します。予測分析を活用して導入スケジュールと資金調達要件をモデル化することで、組織のAIインフラストラクチャが財政的に責任のある方法で導入され、かつ根本的に安全な方法で導入されるようになります。

ドメイン5:セキュリティとプライバシーコントロールの評価と監査

AI駆動型環境での監査は、手動による検査から、広大なクラウド環境にわたるコンプライアンス証拠を相互に関連付けることができる、AIを活用した監査ツールの使用に移行します。このドメインでは、アルゴリズムバイアス、データポイズニング、ハルシネーションなどのリスクに対する「ブラックボックス」機械学習モデルの評価を統合しています。実務担当者は、予測AIを活用して自動スケーリング型MLインフラの範囲を正確に特定し、監査結果がシステムの実際の運用状況を反映するよう確保する方法を理解している必要があります。

説明責任 (アカウンタビリティ) はこの分野の基礎であり、特に監査期間中にAIシステムによって下される自律的な決定に関するものです。試験概要では、AI倫理担当者と機械学習エンジニアそれぞれの具体的な役割を明確にし、監査プロセスにおいてAIの性能に関する技術的側面と倫理的側面の両方が確実に把握されるようにしています。これらの複雑な監査のスケジュール設定とリソース割り当てを自動化することで、CGRCの専門家はシステムの真のコンプライアンス体制に関する忠実度の高いデータを承認担当者に提供できます。

ドメイン6:システムコンプライアンス

AIシステムの承認には、正式なリスク許容基準を通じて、生成AIに内在する不確実性に対処することが含まれます。ドメイン6において、CGRC試験概要では、AIガバナンスツールを活用し、システムセキュリティ計画(SSP)などの大規模なコンプライアンス承認パッケージの作成と提出を自動化することを盛り込んでいます。自然言語処理(NLP: Natural Language Processing)を活用して何千ページにも及ぶプライバシー文書を相互参照することで、実務担当者は不整合箇所を特定し、承認担当者の審査プロセスを効率化することができます。

さらに、このドメインは、アルゴリズムのバイアス監査やトレーニングデータの出所ログなど、インテリジェントシステムに必要な専門的な文書化にも対応しています。 AIによるオーケストレーションを活用し、これらの文書を複雑で多段階にわたるステークホルダーの承認ワークフローに振り分けることで、CGRCの専門家たちは、システムのリスクに対する透明性が高く包括的な理解に基づいた最終的な承認が行われることを確実にします。これにより、最も高度なAIの導入であっても、組織のリスク許容度に関する厳格な基準を満たすことが保証されます。

ドメイン7:コンプライアンスのメンテナンス

AIシステムのコンプライアンスを維持するには、MLOpsの急速なライフサイクル変化に対応できる、AI駆動型の継続的制御モニタリング(CCM: Continuous Control Monitoring)への移行が必要です。このドメインは、機械学習による更新を正式なシステム変更手順に基づいて取り扱い、継続的デプロイメントのガバナンスを統合しています。実務担当者は、提案されたアーキテクチャの変更が承認される前に、AIを活用してその「影響範囲」やコンプライアンスへの影響を予測する方法を理解しており、これにより、承認されたセキュリティ基準からの承認されていない逸脱を防ぐことができます。

最後に、CGRC試験概要では、基礎となるモデルの更新によってシステムのコンプライアンス態勢がどのように変化するか、または新たなバイアスが生じる可能性があるかを自律的に評価する上でのAIの役割について説明しています。CGRCの専門家は、トレーニングデータの構成の統計学的変化が規制要件に与える影響を評価することで、システムの運用期間を通じてコンプライアンスを維持します。このような予防的なメンテナンスアプローチにより、組織は長期的なセキュリティとコンプライアンスの目標を損なうことなく、最新のAIイノベーションを活用できるようになります。

2023年9月15日発行のCSSLP試験概要について

Certified Secure Software Lifecycle Professional (CSSLP) は、アプリケーションセキュリティの卓越性における最高水準を体現しています。AIがソフトウェア開発のあり方を変革する中、CSSLP試験の試験範囲は、特にAI駆動型およびAI統合型アプリケーションに関連する部分において、初期構想からサプライチェーン管理に至るまでのライフサイクル全体にわたるセキュリティに対応できるよう、最新の内容に更新されました。これにより、ソフトウェアの専門家は、機械学習を安全に活用したアプリケーションを設計、構築、保守できるようになり、AIがソフトウェアスタックにもたらす特有の非決定論的リスクからシステムを守ることができます。

ドメイン1:安全なソフトウェアの概念

CSSLPの基礎ドメインにおいて、AIの統合は、生成AIやLLMが従来のソフトウェアのセキュリティ境界をどのように根本的に変革するかという点に焦点を当てています。専門家は今、データポイズニングやモデルインバージョンといった機械学習特有の脆弱性に対処するために、情報セキュリティ概念の中核となる柱を再定義する必要があります。これには、確率的な出力に対してセキュアな設計原則を適用し、ソフトウェアの基盤となる概念が、統合されたAIコンポーネントの非決定論的な挙動に対して耐性を持つようにすることが含まれます。

さらに、このドメインでは、AI駆動型システムが、トレーニング段階での意図しない記憶により、機密性の高い独自コードや個人を特定できる情報(PII: Personally Identifiable Information)を漏洩させるリスクに対処します。CSSLPは、AIを活用して鍵管理の自動化とセキュリティプリミティブの継続的な適用を行うことで、セキュリティが単なる上乗せではなく、最初からソフトウェアの中核となる概念のロジックそのものに組み込まれることを保証します。

ドメイン2:安全なソフトウェアライフサイクル管理

開発チームが機械学習を導入する中、CSSLPは従来のDevSecOpsからMLSecOpsへの移行に焦点を当てています。このドメインでは、AIモデルの非線形かつ継続的な再学習ループの管理を、標準的なアジャイルスプリントに統合しています。セキュリティ管理者は、生成AIコーディングアシスタントの安全な利用を監督し、これらのツールが「ハルシネーション」のような脆弱性を生み出したり、

重要なセキュリティゲートを迂回したりすることなく開発ライフサイクルを加速させるようにします。

運用面では、この分野では、従来のアプリケーションセキュリティ基準に加え、LLM向けのOWASP Top 10などの新たなフレームワークの採用を重視しています。専門家は、AIモデルのバイアスやハルシネーションの発生率が安全基準値を超えた場合、CI/CDパイプラインにおいて明確なビルド中止基準を設定する役割を担っています。これにより、ポスト量子暗号の戦略的ロードマップから自動セキュリティチケット発行までのライフサイクル全体で、AI駆動型の開発のスピードと複雑さを管理できるようになります。

ドメイン3:安全なソフトウェアの要件

要件定義には、サードパーティ製のLLMやAIマイクロサービスの統合に関する厳格な境界の定義が含まれます。 専門家は、許可されていない自律的な動作をAIモデルが実行することを防ぐための機能要件を策定するとともに、許容可能なハルシネーション発生率やアルゴリズムのバイアス閾値に関する非機能要件を定義しなければなりません。この統合により、AIのビジネスユースケースの範囲が明確に定義され、管理不能なセキュリティリスクにつながる恐れのある「機能クリープ」が防止されます。

さらに、このドメインではAIを活用して要件定義プロセスそのものを強化しており、自然言語処理(NLP)を用いて複雑な要件文書を自動的に解析・検証しています。CSSLPは、組み込み型チャットボットや推論エンジンを具体的に標的とした「悪用事例」を特定することで、アプリケーションのインテリジェンス層に対する「jailbreak(脱獄)」や操作といった攻撃的な試みに耐えうる堅牢なセキュリティ要件を確保します。

ドメイン4:安全なソフトウェアアーキテクチャと設計

アーキテクチャの分野では、中核となるアプリケーションロジックを予測不可能なAI推論エンジンから切り離す、耐障害性の高いシステムの設計に重点が置かれています。アーキテクトは、機密性の高いベクトルデータベースやAI処理クラスターの周囲にゼロトラスト境界を設計する方法を熟知しており、機械学習の統合によってシステム全体のセキュリティアーキテクチャが損なわれることがないようにします。これには、設計段階でAIを活用した脅威モデリングを用いて、変化し続ける攻撃対象領域を自律的に可視化することが含まれます。

また、アーキテクトは、機械学習の確率的な性質や特有のサプライチェーンを考慮に入れるため、SABSA(Sherwood Applied Business Security Architecture)のような高レベルのフレームワークを適応させています。CSSLPは、フェデレーテッドラーニングを活用する分散コンピューティングノードを確保し、AI推論に必要な大容量のメッセージキューイングを管理することで、ソフトウェアアーキテクチャが優れたパフォーマンスを発揮すると同時に、AIシステム特有の障害モードに対しても堅牢であることを保証します。

ドメイン5:ソフトウェアのセキュアな実装

現在、実装の焦点は、AIを活用したコーディングの安全な利用と、組み込み機械学習アルゴリズムのセキュリティ対策に置かれています。専門家は、プロンプトインジェクションを低減し、AIによって生成されたコード・スニペットの出所を確実にするために明示的に設計された安全なコーディング標準を遵守しなければなりません。このドメインは、LLMに送信されるすべての入力の厳格なサニタイズに重点を置いており、NLPを活用した検証により、従来の入力フィルターでは見逃されがちな悪意のあるペイロードを意味論的に理解し、ブロックします。

さらに、実装段階では、AIを活用して、宣言型セキュリティポリシーを実行時に強制力のある命令型コードへと自律的に変換する手法に取り組んでいます。CSSLPは、これらの宣言的な境界がAIエージェントの自律的な行動をどのように制限するかを評価することで、設計から本番への移行中に脆弱性が導入されるのを防ぎながら、高スループットのAIワークロードを処理できるほどコード実装が堅牢であることを保証します。

ドメイン6:ソフトウェアのセキュリティテスト

ソフトウェアテストは、純粋に決定論的な手法から、AIモデルの出力に必要な確率論的テストへと進化してきました。このドメインでは、専門家たちは組み込み機械学習モデルのバイアス、ドリフト、有害性、および敵対的回避への脆弱性を評価するため、特定のテストフェーズを組み込んでいます。これには、AIを活用して複雑でエッジケースを含むセキュリティテストスクリプトを機械並みの速度で自律的に生成し、テストの網羅性がアプリケーションの複雑さに追いつくようにすることが含まれます。

テストには、自律型AIエージェントの機能的な論理的境界も含まれており、意図された範囲外で重要なコマンドを実行できないことを検証します。CSSLPは、AIモデルに対してトークン制限を用いたストレステストを実施し、NIST AIリスク管理フレームワーク(AI RMF: Risk Management Framework)に基づいて評価を行うことで、AIコンポーネントの性能低下や敵対的干渉が発生した場合でも、アプリケーションが安全に停止し、信頼性を維持できるようにします。

ドメイン7:ソフトウェアのセキュアな導入、運用、保守

この分野では、非決定論的AIモデルを決定論的ソフトウェア環境に導入する際に生じる特有の運用リスクに焦点を当てています。我々は「AIOps」を導入し、ソフトウェアインフラストラクチャの監視と保守を自動化することで、運用上の異常に対してリアルタイムで対応

できる自己修復型システムを実現しています。メンテナンスには、運用環境で発生するアルゴリズムドリフトや敵対的AI攻撃の兆候を特定するための管理者のトレーニングが含まれるようになりました。

また、実務担当者は、本番環境への完全なデプロイに先立ち、更新されたAIモデルの重みの挙動をテストするために特別に設計された、隔離されたサンドボックス型のステージング環境を構築する役割も担っています。CSSLPは、AIで生成されたコードの法的リスクと著作権リスクを管理し、EU AI Act法などの新しい法律の遵守を確保することで、AI駆動型ソフトウェアの継続的な運用と保守が透明性、コンプライアンス、および安全性を維持できるようにします。

ドメイン8:セキュアなソフトウェアサプライチェーン

ソフトウェアのサプライチェーンは、外部の基盤モデルへの依存や膨大な公開データセットといった、AIエコシステム特有のリスクも包含するように拡大しています。このドメインでは、従来のSBOMから、モデルの重み、トレーニングデータセット、MLライブラリを追跡する「AI-BOM (AI Bill of Materials)」への進化に焦点を当てています。専門家は、オープンソースのAIモデルを選択するための厳格なセキュリティ基準を確立し、悪意のあるバックドアや偏ったコンポーネントの統合を防ぐ方法を理解している必要があります。

最後に、このドメインではAIツールを活用して、深く入り組んだ複雑なサプライチェーンを自律的にマッピングして保護しています。CSSLPは、「モデルポイズニング」のリスクを定量化し、事前学習済みのオープンソースモデルの固有のバイアスを評価することで、上流の脆弱性からソフトウェアの完全性を保護します。この総合的なアプローチにより、サードパーティのライブラリからトレーニングデータそのものまで、すべてのコンポーネントが組織のセキュリティおよび倫理基準を満たしていることが保証されます。

2025年8月1日発行のISSAP試験概要について

Information Systems Security Architecture Professional (ISSAP) 認定は、セキュリティ設計の最高峰です。組織がAIネイティブなインフラストラクチャに移行するにつれて、ISSAP試験概要は進化し、アーキテクトがAIを強力な防御資産であると同時に価値の高い保護対象領域としても扱う、複雑で回復力のある環境を設計できるようになりました。ISSAP試験概要では、AIに関する考慮事項をアーキテクチャライフサイクルに組み込むことで、シニアアーキテクトがビジネス主導のAIイノベーションを最も厳しいセキュリティエンジニアリング基準に合わせることができるようになります。

ドメイン1:ガバナンス、リスク、コンプライアンス (GRC)

アイデンティティ・アーキテクチャの分野において、ISSAP試験概要は、自律型AIエージェントや自動化されたサービスアカウントのアイデンティティ管理という複雑な課題に取り組んでいます。アーキテクトの任務は、「サービスとしてのアイデンティティ（IDaaS: Identity-as-a-Service）」フレームワークを設計することです。これはAIシステムが企業内を移動する際に権限を昇格させないようにするために、人間以外のエンティティに最小権限の原則を適用するものです。このドメインでは、組織を真のゼロトラスト体制へと導くために、行動バイオメトリクスとAI駆動型の適応認証のアーキテクチャ統合に重点を置いています。

さらに、ハイブリッドおよびマルチクラウド環境全体におけるアクセス制御の連携を強化するため、AIを活用しています。アーキテクトは、検出されたユーザー行動の異常にリアルタイムで対応する自動プロビジョニングおよびプロビジョニング解除ワークフローを設計する方法を理解している必要があります。ISSAPは、アイデンティティ・オーケストレーションの中核にAIを据えることで、ますます自動化・分散化が進む労働環境のニーズに対応できるよう、アーキテクチャの拡張性を確保しています。

ドメイン2:セキュリティアーキテクチャモデリング

セキュリティアーキテクチャモデリングの分野は、「インテリジェントSOC」のアーキテクチャ設計に焦点を当てています。セキュリティ・オーケストレーション、オートメーション、およびレスポンス(SOAR: Security Orchestration, Automation and Response)プラットフォームや、AIを活用したセキュリティ情報イベント管理(SIEM: Security Information and Event Management)システムのインフラ要件に対応することで、AIを統合しています。アーキテクトは、遅延やデータ損失を招くことなく、大量のテレメトリを ML 搭載の相関エンジンに送ることができる高スループットのデータパイプラインを設計する方法を理解してる必要があります。

このドメインでは、防御的な自動化だけでなく、AIモデル自体の監視と防御に必要なアーキテクチャも対象としています。これには、プロンプトインジェクションやモデル回避の試みを検知するように設計された、専用の「AIファイアウォール」や監視プローブの導入が含まれます。

ISSAPは、統一された可視化レイヤーを設計することで、セキュリティ運用が従来の資産と高度な機械学習パイプラインの両方にわたってまとまりのある防御戦略を維持できるようにします。

ドメイン3:インフラストラクチャとシステムセキュリティ

インフラストラクチャアーキテクチャは、AIのトレーニングと推論に必要な、特殊で高性能なコンピューティング環境を考慮しています。この統合では、「ハードウェア基盤の信頼性(Hardware-Rooted Trust)」および信頼実行環境(TEE: Trusted Execution Environments)を活用し、物理レイヤーレベルで機密性の高いモデル重みやトレーニングデータを保護することに重点を置いています。アーキテクトは、AIワークロードを隔離するセキュアなエンクレーブとマイクロセグメンテーション戦略を設計し、攻撃者が侵害されたAIインターフェースを利用してデータセンター内でのラテラルムーブメントを防ぐ役割を担っています。

また、ネットワーク及び物理的な境界を守るためのAIの役割についても取り上げています。アーキテクトは、AIを搭載したネットワークセンサーと、新たな脅威に動的に適応できるソフトウェア定義境界(SDP: Software-Defined Perimeter)ソリューションを統合する方法を理解している必要があります。ISSAPは、耐障害性が高く、AIに対応したインフラを構築することで、企業の基盤層が、現代のインテリジェンスシステムが抱える膨大な計算処理およびセキュリティの要件を確実に満たせるようにサポートします。

ドメイン4:アイデンティティとアクセス管理 (Identity and Access Management: IAM) のアーキテクチャ

アーキテクチャレベルでは、GRCの統合には「設計上安全で規制に準拠した」システムの設計が含まれます。このドメインでは、NIST AI RMF(Risk Management Framework)のアーキテクチャ上の実装や、「説明を受ける権利」などの世界的な規制要件に焦点を当てています。アーキテクトは、AIの意思決定に関する監査可能なログを提供する透明性の高いシステムアーキテクチャを設計する方法を理解しており、これにより、自動化されたプロセスが人間の監督者や法務監査人によって検証可能となるよう確保します。

さらに、このドメインは、サードパーティとサプライチェーンのAI統合のリスクアーキテクチャにも対応しています。AIサービスプロバイダーを企業システムに統合する前に、そのセキュリティ態勢を評価する「ベンダー・リスク・アーキテクチャ」の構築を重視しています。ISSAPは、リスク管理をアーキテクチャの設計図に直接組み込むことで、AIの導入が組織の定めたリスク許容度および法的枠組みの範囲内にとどまることを保証します。

2025年8月1日発行のISSEP試験概要について

Information Systems Security Engineering Professional (ISSEP) 認定資格は、厳格なシステムエンジニアリングと高度なサイバーセキュリティが融合したものです。AIがミッションクリティカルなシステムの主要な構成要素となる中、ISSEP試験概要は、セキュリティエンジニアがAI駆動型コンポーネントの完全性を、数学的およびアーキテクチャ的な観点から検証できます。ISSEP試験概要は、システムエンジニアリングのライフサイクルにAIを組み込むことで、システムの「インテリジェンス」がハードウェアやソフトウェアと同様に防御可能で予測可能であることを保証します。

ドメイン1:システムセキュリティエンジニアリングの基礎

ISSEPの基盤ドメインにおいて、AIの統合は、システムのセキュリティアーキテクチャ内における機械学習モデルの数学的および理論的な検証に重点を置いています。セキュリティエンジニアは現在、AIコンポーネントに形式手法を適用し、システムのライフサイクル全体を通じて「アルゴリズムの完全性」が維持されるよう確保することが求められています。これには、AI固有の脅威モデリング（敵対的回避に対する脆弱性の特定など）を初期設計要件に直接統合して、システムのベースラインが非決定論的脅威に対して耐えられるようにすることが含まれます。

さらに、このドメインでは、「セキュリティ設計原則」へのAIの組み込みについても取り上げています。エンジニアは今、ニューラルネットワーク特有の計算要件とデータ処理要件を考慮して、AIサブシステムの統合が確立されたセキュリティ領域や信頼境界に違反しないようにする必要があります。ISSEPは、MLモデルを価値の高いエンジニアリング資産として扱うことで、システムの基盤が従来の攻撃ベクトルとAIによって拡張された攻撃ベクトルの両方に耐えられるように構築されていることを保証します。

ドメイン2:リスクマネジメント

セキュリティエンジニアのリスク管理は、AIに内在する確率的なリスクも対象に含めるよう進化してきました。このドメインにおいて、ISSEP試験概要では、本番環境における「モデルの堅牢性」およびロジックのドリフトの可能性を評価するための手法が統合されています。実務担当者は、AI駆動型の評価ツールを活用して、複雑なシステムの相互依存性を継続的に自動的にスキャンし、特定時点の監査からシステムのリスク状況のリアルタイムな理解へと移行します。

さらに、ISSEP試験概要では、リスク低減の核心的な戦略として、「説明可能なAI」の設計に重点を置いています。透明で監査可能な意思決定の道筋を提供するシステムを設計することで、エンジニアはセキュリティ認証や認証に必要な証拠を提供できます。この統合により、最も複雑なディープラーニングコンポーネントでも、高保証環境に必要な厳格な文書化および検証基準を確実に満たすことができます。

ドメイン3:セキュリティ計画と設計

このドメインは、「構築」フェーズに焦点を当てており、AIをセキュアシステム開発ライフサイクル(SSDLC: Secure Systems Development Lifecycle)に統合することを目的としています。セキュリティエンジニアは、トレーニング段階で「データポイズニング」を防止する安全なデータ取り込みパイプラインを設計する任務を負っています。この統合では、物理層における不正アクセスや改ざんからAIモデルの重みや推論ロジックを保護するため、Trusted Execution Environments(TEE)などのハードウェアに根差した信頼性の活用に重点が置かれています。

さらに、ISSEP試験概要では、AIAPIとサードパーティのMLライブラリの安全な統合についても取り上げています。エンジニアは、事前にトレーニングされたモデルの「出所」を評価して、システムのインテリジェンスのためのソフトウェアサプライチェーンがコード自体と同じくらい安全であることを確認する必要があります。 ISSEPは、AIセキュリティ要件を機能設計仕様書に組み込むことで、完成したシステムがインテリジェントであるだけでなく、アーキテクチャ的にも堅牢で、防御可能なものとなるよう保証します。

ドメイン4:システムセキュリティの実装、検証、妥当性確認

検証と妥当性確認はエンジニアリングにおいて非常に重要であり、この分野には、確立されたセキュリティポリシーに対するAI出力のテストが含まれます。統合には、「敵対的テスト」プロトコルの開発が含まれます。これは、エンジニアがAI駆動の制御システムを欺いたり迂回させたりすることで、その耐性を検証するものです。これにより、システムの自動応答が一貫して予測可能になり、ミッションの成功を危うくする可能性のある「ハルシネーション」が発生することがなくなります。

機械学習を利用して大量のテストデータとシステムログを解析することで、エンジニアは従来のテストでは見落とされがちなエッジケースやロジックの欠陥をより効果的に特定できます。この双方向の統合により、システムの複雑化が進んでも、その検証に用いられるエンジニアリング・ツールは、同様に高度かつ効果的な状態を維持できるようになります。

ドメイン5:セキュアオペレーション、変更管理、廃棄

最後のドメインは、AIを統合したシステムの長期的な持続可能性に取り組むものでエンジニアには、モデルのパフォーマンスと整合性を長期にわたって具体的に追跡する「継続的監視」フレームワークを設計する任務があります。これには、「コンセプトドリフト」やセキュリティ侵害が検出された場合のモデル再トレーニングやシステムロールバックの自動トリガーの設定が含まれます。これにより、システムが運用期間全体にわたって許可されたセキュリティパラメータの範囲内にとどまることが保証されます。

メンテナンスには、現場でのAIモデルの安全なパッチ適用と更新も含まれます。ISSEPは、大規模なモデル更新のための安全な配信メカニズムを設計し、更新プロセスのすべての段階で「インテリジェンス」の整合性が検証されるようにする必要があります。ISSEP試験概要では、AIを保守サイクルに組み込むことで、システムが進化する脅威に対して強靭性を維持し、「ヒューマン・イン・ザ・ループ」が自律的なシステム機能を監督・制御する能力を保持できるようにしています。

2025年8月1日発行のISSMP試験概要について

The Information Systems Security Management Professional (ISSMP) 認定資格は、技術的セキュリティと組織戦略の間のギャップを埋めるリーダーを対象としています。AIがビジネス革新の中核的な原動力となる中、ISSMP試験概要には、AIおよび機械学習を統括するために不可欠な管理能力が盛り込まれています。倫理的ガバナンスの確立からレジリエントなAIを活用したセキュリティ運用の設計まで、統合された ISSMP 試験概要により、上級セキュリティマネージャーは、強固で規制に準拠したセキュリティ体制を維持しながら、アルゴリズム時代の複雑な状況を乗り越えて組織を導くことができます。

ドメイン1:リーダーシップと組織管理

戦略的リーダーシップの分野において、AIの統合は、中核となる業務機能への機械学習の安全な導入を通じて、経営陣を導くことに重点を置いていますこのドメインでは、アルゴリズムの透明性と自動意思決定のための説明責任を保証する倫理的なAIガバナンスモデルの確立に重点が置かれています。セキュリティ管理者は、安全なAI実験を促進する文化を醸成すると同時に、「シャドーAI」――データ漏洩や評判の失墜につながる恐れのある、公的なAIツールの無断利用――に伴うリスクを未然に防ぐ役割を担っています。

さらに、このドメインは、セキュリティに関するビジョンをAI時代の特有のニーズと整合させることにも取り組んでいます。これには、生成AIの時代において知的財産を保護するための組織のミッションを更新し、セキュリティチェックポイントをデータサイエンスのワークフローに直接組み込むことが含まれます。ISSMPは、AI支援の運用速度を考慮して組織のプロセスを再定義することで、セキュリティが進歩のボトルネックではなく、イノベーションを可能にする要因であり続けることを保証します。

ドメイン2:システムライフサイクル管理

従来の決定論的システムから連続的で確率的な機械学習パイプラインへの移行は、このドメインの主な焦点です。セキュリティ管理者は、「MLSecOps」のライフサイクルを管理する方法を熟知しており、各フェーズにおいて自動化されたAI駆動型のセキュリティテストと動的な検証を統合します。この統合により、開発プロセス内に明確な決定ゲートが導入され、AIモデルのバイアスまたは「ハルシネーション」が確立されたしきい値を超えた場合に展開を停止し、安全で信頼性の高いモデルのみが本番環境に届くようになります。

さらに、このドメインには、エンタープライズアーキテクチャの管理を強化するためのAIの使用も含まれます。実務担当者は、AIシステムに投入される膨大な量の非構造化データを分類するために、自律的な探索・分類ツールを活用することが求められています。ISSMPは、アクティブなモデルの保護と再トレーニングに必要な継続的なフィードバックループを管理することで、基盤となる機械学習ロジックが時間の経過とともに進化しても、アプリケーションのセキュリティが維持されることを保証します。

ドメイン3:リスクマネジメント

リスク管理は、静的なポイントインタイム評価から動的なリアルタイム評価へと進化しました。ISSMP試験概要では、NIST AIリスク管理フレームワーク(AI RMF: AI Risk Management Framework)やISO/IEC 42001といった世界的に認められたフレームワークと従来の戦略を統合しており、これにより管理者は生成AIの倫理的な利用と調達を適切に管理できるようになります。リスクスコアリングに予測機械学習モデルを利用することで、組織はより積極的な姿勢に移行し、独自のモデルウェイトやアルゴリズムに対する脅威を悪用される前に特定して低減することができます。

リスク管理の範囲も拡大し、サードパーティのLLMの複雑なエコシステムや、継続的な学習に必要な大規模なデータレイクも含まれるようになりました。ISSMPは、最高データ責任者やAI倫理委員会などの新しい利害関係者を関与させて、許容できるエラーの閾値を定義し、AI駆動型の意思決定による評判への影響を低減する役割を担います。これにより、組織のリスク戦略は、人的脆弱性とアルゴリズム的脆弱性の両方をカバーできるほど包括的であることが保証されます。

ドメイン4:セキュリティの運用

現代のセキュリティオペレーションセンター(SOC)では、AIは強力な防御ツールであると同時に、新しい攻撃対象領域でもあります。このドメインでは、「AIOps」の運用に重点を置き、脅威を自律的に検知・是正することで、事後対応的なアラートの優先順位付けから、AIを活用した先制的な脅威ハンティングへと移行します。

セキュリティマネージャーは、特に組織のAIモデルのロジックを対象とするプロンプトインジェクションやデータポイズニングなどの新たな敵対的攻撃に対する運用上の対応を監督する責任があります。

業務の統合には、生成AIを活用して複雑なプレイブックやランブックを迅速に作成・更新することも含まれます。データサイエンティストと機械学習エンジニアは、インシデント対応プロセスの主要な利害関係者です。アルゴリズムによる回避戦術のリバースエンジニアリングを専門とするAIセキュリティアナリストをチームに配置することで、ISSMPは、マシンレベルの速度で展開される攻撃に対してもSOCの耐性を確保します。

ドメイン5:コンティンジェンシーマネジメント

レジリエンシー計画では、現代のAIが必要とする大規模で特殊なインフラストラクチャを考慮に入れる必要があります。このドメインでは、生成モデルを活用してAIを統合し、極めて複雑な災害復旧(DR)計画をシミュレーションおよび作成します。セキュリティマネージャーは、重要なデータ取り込みパイプラインや大規模なベクトルデータベースの復旧を優先する緊急時対応戦略を策定する方法を熟知しており、障害発生時においても、ビジネスに不可欠なAIの予測精度が低下しないよう確保しています。

ISSMP試験概要では、継続リスクとしての「モデルドリフト」という特有の課題も取り上げています。ISSMPは、大規模なLLMをホストするクラウドアーキテクチャの耐障害性を分析し、モデルをゼロから再トレーニングするために必要な膨大な計算リソースを考慮した復旧時間目標(RTO:Recovery Time Objectives)を確立する必要があります。予測型AIを活用してさまざまな災害シナリオのビジネスへの影響をモデル化することで、実務担当者は組織のレジリエンシーがAIに依存する企業の要求に遅れないようにすることができます。

ドメイン6:法律、倫理、セキュリティコンプライアンス管理

このドメインは、EU AI法のような国際的な規制や、アルゴリズムの責任に関する新たな基準など、急速に変化する法的環境に対応しています。統合の取り組みは、データ最小化要件と継続的な機械学習による大量のデータ取り込みニーズとの間の対立を管理することに重点を置いています。ISSMPは、集中管理型のエンタープライズLLMをトレーニングする際、地域ごとの越境データ流通規制に準拠するために、動的なデータルーティングをどのように実装すべきかを理解している必要があります。

倫理とコンプライアンスには、自動プロファイリングの背後にあるロジックについてユーザーに知らせる必要がある「説明の権利」も含まれます。このドメインに含まれるサブタスクは、オープンソースのAIモデルを使用する際の知的財産リスクや、プライバシー関連法規に準拠して会話プロンプトの履歴を維持する必要性に対処するものです。

ISSMPは、AIシステムが透明で、偏りがなく、ユーザーのプライバシーを尊重することを保証することで、自動化された世界における組織の法的および倫理的完全性を守る役割を果たします。

追加の試験情報

試験概要と経験要件を確認

すべての受験者は、試験を選択して受験する前に、試験の概要と経験要件を十分に確認することをお勧めします。このドキュメントは、受験者が認定試験中に遭遇することが予想される分野やトピックに関するガイダンスの情報源となるISC2認定試験の概要に代わるものではありません。試験の概要は、Webページ **www.ISC2.org/Certifications** でご覧いただけます。

試験の方針と手続き

ISC2は、受験者が試験に登録する前に、試験の方針や手続きを確認することをお勧めします。この重要な情報の包括的な内訳は、**www.ISC2.org/Register-for-Exam**よりご覧ください。

ISC2 について

ISC2 は、世界をリードするサイバーセキュリティ専門家のための会員団体であり、安全で安心なサイバーワールドの実現に向けて活動しています。265,000人を超える認定メンバー、および

アソシエイトは安全で安心なサイバー世界の実現に向けて活動するサイバーセキュリティの専門家による世界最大の団体を構成しています。サイバーセキュリティ分野で最高峰の認定資格であるCISSP®をはじめ、数々の受賞歴を誇る ISC2 の認定資格は、専門家がキャリアのあらゆる段階でその知識、スキル、能力を証明することを可能にします。ISC2は、アドボカシー活動、専門知識の提供、そして人材の育成を通じて、サイバーセキュリティ業界の影響力、多様性、活力を強化し、相互につながる世界におけるサイバーの安全性とセキュリティの向上を加速させます。私たちの慈善団体である Center for Cyber Safety and Educationは、サイバーキャリアへのアクセスの拡大を支援し、一般の人々に教育を提供するというコミットメントによって支えられていますISC2の活動に参加、またはISC2のCandidateになって、ISC2.org. でサイバーセキュリティのキャリアを築きましょう。X, Facebook and LinkedIn.

ISC2