

Tenable での AI と機械学習の活用方法

最終更新日: 2026 年 10 月 5 日



目次

はじめに	4
概要: データと AI の接点	5
サイバーエクスポージャー管理における AI の現在の活用状況	7
機械学習	8
ディープラーニングと小規模言語モデル	8
Tenable One AI Exposure	8
生成 AI とエージェント型 AI	9
脆弱性の優先順位付け	9
攻撃経路リスクの評価	9
インベントリの管理	10
Exposure Signals のモニタリング	10
Tenable Hexa AI の活用	10
Tenable Research による AI の活用方法	11
リサーチエンジニア拡張コンテンツライティング	12
エージェントコンテンツライター	12
多言語検出評価	13
AI エージェントツールのリスク分類	13
開発パイプラインワークフロー	14
トレーニングデータ	15



サードパーティの AI プロバイダー	16
データ保持とガバナンス	16
機能および技術仕様例	17
結論	18
関連リンク	19



はじめに

Tenable は、機械学習と生成 AI を使用して、(1) サイバーエクスポージャーリスクをプロアクティブに特定し、優先順位を付ける、(2) セキュリティ運用の効率を高める、(3) 明確な可視性とインサイトを顧客に提供して、リスクに優先順位を付けて軽減する、といった 3 つの領域でサイバーセキュリティ製品を強化しています。

- [概要: データと AI の接点](#)
- [サイバーエクスポージャー管理における AI の現在の活用状況](#)
- [Tenable Research による AI の活用方法](#)
- [トレーニングデータ](#)
- [サードパーティの AI プロバイダー](#)
- [機能および技術仕様例](#)
- [結論](#)
- [関連リンク](#)



概要: データとAI の接点

この表は、本書で説明するすべての Tenable AI 搭載機能をまとめたものです。

機能	AI/ML テクノロジー	顧客データの使用	サードパーティ製 LLM の使用
Vulnerability Priority Rating (VPR) (脆弱性優先度格付け ((VPR)))	機械学習/生成 AI	なし: スコアは公開情報および商用の脅威インテリジェンスから算出され、環境データからは算出されません	あり (ニュースやアドバイザリコンテンツを読み取る生成 AI コンポーネント用。データは読み取りません)
CVSS Metrics Prediction (CVSS メトリクス予測)	機械学習	なし	なし
Operating System Prediction (オペレーティングシステム予測)	機械学習	あり: スキャンデータ (ネットワークレベルのホストメタデータのみ)	なし
User Criticality Rating (ユーザー重要度の格付け)	機械学習	あり: ユーザーの役職とアクセス権	なし
AI Threat and Misuse Detection (AI 脅威)	ディープラーニング/小規模言語モデル	あり: 接続されている AI プラットフォーム上でのアクティビティ	なし (Tenable トレーニング済みモデル)



機能	AI/ML テクノロジー	顧客データの使用	サードパーティ製 LLM の使用
威および誤使用の検出)			
Data Exposure Detection (データ漏洩の検出)	ディープラーニング/小規模言語モデル	あり: 接続されている AI プラットフォームを通過するコンテンツ	なし (Tenable トレーニング済みモデル)
Prompt Translation (プロンプト翻訳)	ディープラーニング/小規模言語モデル	あり: 英語以外の言語で送信するプロンプト	なし (Tenable トレーニング済みモデル)
Attack Path Summary (攻撃経路サマリー)、Attack Path Assistant (攻撃経路アシスタント)、Attack Path Mitigation Guidance (攻撃経路軽減ガイダンス)	生成 AI	あり: 攻撃経路、資産、脆弱性データ	あり (Google Vertex AI)
Asset Summary (資産のサマリー) と Natural Language Search (自然言語検索)	生成 AI	あり: 資産インベントリ	あり (Google Vertex AI)



機能	AI/ML テクノロジー	顧客データの使用	サードパーティ製 LLM の使用
Exposure Signals Description (Exposure Signals の説明) と Exposure Signals Summary (Exposure Signals のサマリー)	生成 AI	あり: Exposure Signals データ	あり (Google Vertex AI)
Tenable Hexa AI	生成 AI/エージェント型 AI	あり: すでに Tenable にある資産、脆弱性、アイデンティティ、設定、AI システムのデータと、入力内容	あり (Anthropic、AWS Bedrock 経由)
Adversary View (Tenable Hexa AI)	生成 AI/エージェント型 AI	あり: Tenable One にすでに収集されているエクスポートデータ、資産、脆弱性データ	あり
Tenable Research	生成 AI/エージェント型 AI	あり: スキャンデータ (ネットワークレベルのホストメタデータのみ)	あり (Anthropic、Claude Code 経由)

サイバーエクスポート管理における AI の現在の活用状況

以下のセクションでは、各手法について詳しく説明します。



機械学習

Tenable は機械学習を使用して脆弱性をプロアクティブに特定し、優先順位を付けることで、最も重大な脅威に集中できるよう支援します。

- **Vulnerability Priority Rating (VPR) (脆弱性優先度格付け ((VPR))) (脆弱性優先度格付け (VPR)):** 脆弱性が 28 日以内に悪用される可能性を予測し、リスクベースの優先順位付けを可能にします。Tenable One `[[[Undefined variable Tenable.ExposureManagementShort]]]` 全体で使用できます。
- **CVSS Metrics Prediction (CVSS メトリクス予測):** CVSSv3 メトリクスを予測し、(VPR) モデルに重要な入力情報を提供します。
- **Operating System Prediction (オペレーティングシステム予測):** 限られたスキャンデータでもリモートでのオペレーティングシステムのフィンガープリント精度を向上させ、より適切なデバイス管理をもたらします。Tenable Nessus プラグイン 132935 として利用できます。
- **User Criticality Rating (ユーザー重要度の格付け):** 役職とアクセス権に基づいて組織内の個々のユーザーの重要度を評価し、Tenable One Identity Exposure および Tenable One でリスクベースのサイバーエクスポージャー管理を可能にします。

ディープラーニングと小規模言語モデル

Tenable One AI Exposure

Tenable One AI Exposure は、ディープラーニングモデルと微調整された小型言語モデル (SLM) を使用して、チャットボット、エージェント、アプリケーションを含むあらゆる AI プラットフォームでのインタラクションを保護します。

- **AI Threat and Misuse Detection (AI 脅威および誤使用の検出):** AI プラットフォームを標的とする潜在的な敵対的攻撃を特定し、不正なデータアクセスや意思決定における AI への安全でない依存などの誤使用を検出します。



- **Data Exposure Detection (データ漏洩の検出):** AI エンジンやエージェントが露出または漏洩させた機密データを検出します。
- **Prompt Translation (プロンプト翻訳):** AI を使用して、英語以外の言語のプロンプトを分析用に英語に翻訳します。

これらのモデルは、オープンソースライブラリを使用して Tenable によってトレーニングされます。AI アクティビティは、リスクを特定するために事前に構築済みの検出ポリシーと照らして実行時に評価されます。このアクティビティは、モデルのトレーニングや変更には使用されません。

生成 AI とエージェント型 AI

Tenable は、Google の Vertex AI と Amazon の Bedrock プラットフォームが提供する生成 AI と事前トレーニング済みの大規模言語モデル (LLM) を活用し、以下の用途などで、明確かつ簡潔で、具体的な対応につながる情報を提供します。

脆弱性の優先順位付け

- **Vulnerability Priority Rating (VPR) (脆弱性優先度格付け ((VPR))) (脆弱性優先度格付け (VPR)):** サイバーニュースメディア、セキュリティアドバイザリ、ベンダーのブログ、関連ソースからの膨大な量のコンテンツを分析し、28 日以内に脆弱性が悪用される可能性を予測できるようにします。文脈に富んだ脆弱性のインサイトを脅威モデルへの入力情報として組み込み、主要な要因を更新し、脅威と修復のサマリーなどのメタデータを充実させます。Tenable One 全体で使用できます。

攻撃経路リスクの評価

- **Attack Path Summary (攻撃経路サマリー):** 複雑な攻撃経路を分かりやすいサマリーに抽出します。
- **Attack Path Assistant (攻撃経路アシスタント):** 特定の攻撃経路とそのコンポーネントについて、自然言語で質問できます。



- **Attack Path Mitigation Guidance (攻撃経路軽減ガイダンス):** 特定された攻撃経路リスクに対処するための手順を説明します。

これらの機能は、Tenable の既存の攻撃経路 Analysis によってすでに特定された攻撃経路を要約し、説明するものです。これらは、以下で説明する Hexa AI の機能である Adversary View とは異なります。Adversary View は、すでに見つかったものを説明するのではなく、Claude Mythos を使用して未加工のエクスポージャーデータを横断的に推論し、新たな攻撃チェーンを明らかにします。

インベントリの管理

- **Asset Summary (資産のサマリー):** 資産の詳細な説明を提供し、最も重大なエクスポージャーをハイライトします。
- **Natural Language Search (自然言語検索):** 自然言語を使用して資産インベントリを検索できます。

Exposure Signals のモニタリング

- **Exposure Signals Description (Exposure Signals の説明):** 特定のエクスポージャーインサイトを説明します。
- **Exposure Signals Summary (Exposure Signals のサマリー):** 資産が特定のエクスポージャーインサイトに含まれる理由を説明します。

Tenable Hexa AI の活用

Tenable Hexa AI はエージェント型 AI を使用して、独自の Tenable データに対してマルチステップのセキュリティワークフローを計画し、実行します。複雑なリクエストを一連のステップに分割し、Tenable の既存のプラットフォーム機能を通じてアクションを実行し、Tenable 製品がすでに収集した脆弱性、資産、アイデンティティ、設定、AI システムデータに加えて、直接入力したデータすべてを処理対象とします。

Tenable は Anthropic と提携して、これらのエージェント機能を Tenable One 全体に提供します。基になるモデルのトレーニングに顧客データは使用されません。

ユーザーは、次の 2 つのチャネルを通じて Tenable Hexa AI とやり取りします。



- **チャット**: Tenable One、Tenable One Vulnerability Management、Tenable One Cloud Exposure に組み込まれている会話型インターフェース。ユーザーが達成したいことを自然言語で伝えると、Hexa AI はステップを計画し、推論内容を提示して、変更を加える前に確認を求めます。
- **Model Context Protocol (MCP)**: 顧客が選択した MCP 対応 AI アシスタントに Hexa AI の機能を提供する、Tenable がホストするエンドポイントです。顧客は、すでに使用している AI クライアントを通じて Hexa AI を利用できます。

Hexa AI の機能は、以下を含む一般的なセキュリティワークフローや Tenable 製品の機能をサポートします。

- **Asset Tagging and Organization (資産のタグ付けと整理)**: 自然言語を使用して資産インベントリを検索し、タグとタグカテゴリを作成して、条件に一致する資産に一括でタグを適用します。
- **Exposure Investigation and Organization (エクスపోージャーの調査と整理)**: Tenable One 全体の脆弱性とエクスపోージャーを検索して調査し、影響を受ける資産や資産の詳細を確認したり、検出結果のリスクを調整したりします。
- **Dashboard and Report Creation (ダッシュボードとレポートの作成)**: 必要に応じてダッシュボードを作成、更新、削除します。
- **Scan Operations (スキャン操作)**: スキャンとスキャンポリシーを作成、設定し、スキャンを開始してモニタリングします。
- **修正ワークフロー** 組み合わせとイニシアチブを作成、更新、削除し、サードパーティとの連携を活用してチケットングや変更管理アーティファクトを作成します。
- **Adversary View (Attack Path Discovery (攻撃経路検出))**: Anthropic の Claude Mythos モデルを活用し、Tenable One にすでに収集されているエクスపోージャー、資産、および脆弱性データを横断的に推論することで、攻撃者が最初の侵入地点から重大なシステムへと移動する経路を再構成します。各ステップの根拠を提示し、その経路を遮断するための修復アクションを推奨します。上記のタグ付け、ダッシュボード、修復ワークフローの機能とは異なり、Adversary View は読み取り専用です。分析と推奨は行いますが、それ自体がデータを変更することはありません。

Tenable Research による AI の活用方法



Tenable Research は、脆弱性の開示ペースの加速と高品質なエクスポートインテリジェンスへの需要に対応するため、Tenable One 全体のすべてのセンサーを対象に、AI 支援型のワークフローを導入しています。この取り組みは、次の3つの領域で価値を提供することを目指しています。サイバーエクスポートへの高品質なカバレッジと文脈を踏まえたインテリジェンスの提供を迅速化すること、顧客の優先順位付けと修復を支援する新機能を提供すること、そして、サイバーエクスポート管理の将来を形作る新たな脅威、アタックサーフェス、技術を明らかにする最先端の研究を行うことです。

Tenable Research (Tenable のプラグインフィードを支える検出機能と脆弱性コンテンツを構築するチーム) は、コンテンツ開発プロセス全体で AI を活用しています。これはリサーチエンジニア向けの用途であり、検出コンテンツの構築を支援するために Tenable の開発環境内で実行されます。使用される AI モデルは、顧客が受け取るプラグインフィード、監査ファイル、その他のコンテンツにパッケージ化されたり、その一部として配布されたりすることはありません。

リサーチエンジニア拡張コンテンツライティング

個々のリサーチエンジニアは、主に複雑な開発タスクにおいて、ローカル環境で AI ツールを使用し、手作業によるコンテンツ開発、自動化されたフィード開発、およびサイバーエクスポートインテリジェンスの収集と分析を迅速化しています。Tenable Research は、こうした業務をより多く担えるよう、新たな AI スキル、エージェント、ツールの開発とチーム全体での共有を継続しています。

エージェントコンテンツライター

Tenable Research は、エージェントのコンテンツライティングスキルを開発パイプラインに組み込んでいます。このモデルでは、AI エージェントが初期段階のコンテンツ開発の大部分を処理し、リサーチエンジニアがレビュー、承認、リリースを担当します。これは、品質と正確性に関するリサーチエンジニアの判断に取って代わるものではなく、手作業によるコンテンツライティングを補完するものです。

ベンダーのアドバイザリを実行可能な検出コンテンツに変換することは、必ずしも容易ではありません。ベンダーのアドバイザリには、人間による解釈が必要な注意事項や回避策が含まれていることが多いからです。Tenable Research は、AI エージェントとエージェント型の判定モデルを活用して、ベンダーの意図



について高精度なコンセンサスを形成し、こうした手法なしでは実現できない範囲のプラグインによる検出を自動化しています。

脆弱性構成カバレッジのごく一部は、人間によるレビューなしでリリースされます。ただし、以下の両方の条件を満たす場合に限られます。

- コンテンツが、承認済みのベンダー設定コマンドまたは正規表現を定めた厳格な許可リストに一致していること。これにより、悪意のあるコマンドの生成を防ぎます。すべてのコマンドは、いかなる設定も変更できない、読み取り専用の「show」コマンドに厳密に限定されています。
- 複数の独立したエージェント型の判定モデルが、非常に高い確信度で結果に同意していること。

いずれかの条件を満たさない場合、コンテンツはリリース前に人間によるレビュー担当者に送られます。

多言語検出評価

Tenable Research は、AI を活用して AI Exposure 検出モデルを他の言語に拡張し、評価セットとトレーニングセットに対して自動翻訳パイプラインを実行しています。これにより、Tenable は、複数の言語とより幅広いセキュリティユースケースにわたって高い忠実度で検出を構築できます。

AI エージェントツールのリスク分類

組織が Microsoft 365 Copilot Studio などのプラットフォームを通じて AI エージェントをエンタープライズデータに接続する中、Tenable Research は AI を活用して、利用可能な各エージェントツールがもたらすセキュリティリスクを評価します。1 つの AI エージェントは、数百のコネクタ (Salesforce、OneDrive、Dataverse など) を呼び出すことができ、各コネクタは、行の更新、ファイルの取得、アイテムの削除など、多くの個別のアクションを公開します。自律型エージェントが実行する際にどのアクションがリスクを伴うかを判断する作業は、専門的な判断を大量に必要とするため、AI 支援レビューに適しています。

リサーチエンジニアによる監督を維持するため、複数のガードレールが設けられています。

- **Governed question lifecycle (管理対象質問のライフサイクル):** 新しいリスク質問は評価状態で開始され、リサーチエンジニアが本番環境にプロモーションした後にのみ、実際のリスクスコアに影響



します。

- **Evaluation against a human-labeled golden dataset (人間がラベル付けしたゴールデンデータセットに対する評価):** プロモーション前に、パイプラインは、人間の専門家によって正しいリスクテータスが設定された厳選された一連のアクションに対して分類を再実行し、提案された変更の正確な影響と、その変更がどのアクションに影響するかを正確に報告します。
- **Human review and override (人間によるレビューとオーバーライド):** リサーチエンジニアは、すべてのアクション、そのAI生成サマリー、その分類を調べることができ、自動化された結果をオーバーライドできます。人間の判断は常にモデルよりも優先されるため、リサーチエンジニアがリスクがないとマークしたアクションは、計算されたスコアに関係なく除外され、その逆も同様です。
- **Coverage and redundancy analysis (カバレッジと冗長性の分析):** ツールは、各質問が検出するリスクのあるアクションの数を報告し、リサーチエンジニアが質問セットを高いシグナルで冗長性のない状態に保つのに役立ちます。

開発パイプラインワークフロー

Tenable Research のすべてのコンテンツは、新しいプラグインや変更されたプラグインの品質を自動的にテストする CI/CD パイプラインを通過し、さらに、基盤となる NASL コードをフィードにマージして Tenable 製品で出荷する前に、複数のレビュー担当者が承認する必要があるピアレビュープロセスを経ます。1つの例外は、上記のエージェントコンテンツライターで説明した、脆弱性に関連する設定カバレッジの限定的なエージェント型の判定経路です。本ドキュメントの残りの部分で説明しているものと同様に、このパイプラインで使用される AI モデルは、顧客の環境に届くコンテンツの一部としてパッケージ化されたり、配布されたりすることはありません。

Tenable のプラグイン QA/QC プロセスの詳細については、「[Customer Outreach on Tenable Plugin QA/QC Processes](#) (Tenable のプラグイン QA/QC プロセスに関する顧客向けの案内)」を参照してください。



トレーニングデータ

Tenable は、公開情報、商用情報、匿名化された内部情報など、さまざまなデータソースを活用して機械学習モデルをトレーニングします。Tenable は、データ漏洩のリスクを排除するように設計されていますが、大規模言語モデルを含むいかなるモデルのトレーニングにも、顧客を特定できるデータを使用しません。



サードパーティの AI プロバイダー

Tenable は、特定のケースにおいて、Tenable 固有のモデルのトレーニングや Tenable AI ソリューションの構築のために AI サービスを購入します。Tenable は、Tenable 社内の AI ガバナンス評議会が承認したプラットフォームを通じてのみ、アプリケーションで生成 AI を使用します。同評議会は、Tenable の企業および製品における AI の技術と方法の使用を定期的に見直します。

Google Cloud の Vertex AI プラットフォームは、上記の Tenable One の生成 AI 機能を強化します (サイバーエクスポージャー管理における AI の現在の活用状況を参照)。Amazon Web Service (AWS) Bedrock と Anthropic は、Tenable Hexa AI を支え、エージェントによる推論、計画、ツールの使用のための基盤モデルに加え、コンテンツの安全性確保とポリシーの実施機能を提供します。特に Adversary View は、攻撃経路の推論に Anthropic の Claude Mythos モデルファミリーを使用しています。

Tenable が承認したサードパーティプロバイダーは、応答を生成する目的でのみ顧客のデータにアクセスします。契約条件により、そのデータの保持や、自社モデルのトレーニングへの使用は禁止されています。推論のために送信されたデータは、応答の生成に必要な範囲を超えて、プロバイダーによってログに記録されたり、キャッシュされたり、再利用されたりすることはありません。唯一の例外は、Adversary View (Anthropic の Claude Mythos モデルを使用) です。Anthropic は、推論時の処理のみに限定するのではなく、信頼性と安全性の確保を目的として、送信されたデータを 30 日間保持します。この保持期間中も、Anthropic がそのデータをモデルのトレーニングに使用することはありません。

データ保持とガバナンス

ML または生成 AI 製品の機能に関連して処理された顧客データおよび入力やプロンプトは、リクエストされたサービスを提供するために合理的に必要とされる期間のみ保持されます。上記の機能は、Tenable プラットフォーム内に存在する顧客収集データに適用されます。これらのデータには、Tenable 基本サービス契約が適用されます。Tenable による顧客データの保護方法の詳細については、tenable.com/trust/assurance を参照してください。



機能および技術仕様例

Tenable による AI 活用の一例が、Vulnerability Priority Rating (VPR) (脆弱性優先度格付け ((VPR))) モデルです。このモデルは機械学習を使用して、CVE が今後 28 日以内に悪用の標的となる可能性を予測します。この動的モデルは 24 時間ごとに実行され、最新の脅威および脆弱性データを考慮して (VPR) スコアを更新します。このモデルは、28 日間に悪用された CVE をターゲット変数として使用するランダムフォレスト分類子を使用してトレーニングされています。

別の例として、事前トレーニング済みの大規模言語モデルを利用して特定の攻撃経路の文脈を踏まえたサマリーを提供する、Attack Path Summary (攻撃経路サマリー) 機能があります。ユーザーは、機能の精度と有効性向上のために、高評価/低評価システムを使用してフィードバックを提供できます。詳細については、以下の[関連リンク](#)を参照してください。

さらに、Tenable Hexa AI はエージェント型 AI を適用した一例です。ユーザーが Hexa AI に「すべての Windows Server 資産にタグを付けて、コンプライアンスダッシュボードを作成して」と依頼すると、Hexa AI はそのリクエストを一連のステップに分解します。まず、資産インベントリから Windows Server 資産を検索し、適切なタグを特定または作成します。次に、タグを一括適用するためにユーザーの承認を求め、承認後にタグを適用します。その後、新しいタグをコンテキストフィルターとして適用し、関連するテンプレートからダッシュボードを作成します。データを変更する各ステップ (タグの適用、ダッシュボードの作成) は、実行前にユーザーの明示的な承認を必要とします。Hexa AI は、ユーザーが直接利用するものと同じ Tenable プラットフォーム機能を通じて動作するため、すべてのアクションはユーザーの既存のアクセス許可に従い、完全に監査可能です。



結論

Tenable は、従来の分類モデル、生成 AI、人間による監督の下で複数ステップのワークフローを実行するエージェント型 AI など、さまざまな AI 技術を製品ポートフォリオと研究業務に統合するとともに、顧客が受け取るプラグインフィードについて人間のレビュー担当者が確認する体制を維持した、AI 支援型のコンテンツ開発パイプラインを導入しています。Tenable の AI ガバナンス評議会は、これらの AI の活用状況を継続的にレビューしています。



関連リンク

- [Threat score prediction model \(脅威スコア予測モデル\) \(Google Patents\)](#)
- [Automatic generation of vulnerability metrics using machine learning \(機械学習を使用した脆弱性メトリクスの自動生成\) \(Google Patents\)](#)
- [Host operating system identification using transport layer probe metadata and machine learning \(トランスポート層プローブメタデータと機械学習を使用したホストオペレーティングシステムの識別\) \(Google Patents\)](#)
- [予測に基づいた優先順位付け: 最も重要度の高い脆弱性に集中する方法 \(Tenable ホワイトペーパー\)](#)
- [「VPR」とは何か。「CVSS」とはどう違うのか。 \(Tenable ブログ\)](#)
- [How VPR Helped Prioritize the Most Dangerous CVEs in 2019 \(VPR が 2019 年の最も危険な CVE の優先順位付けにどのように役立ったか\) \(Tenable ブログ\)](#)
- [How to Use VPR to Manage Threats Prior to NVD Publication \(NVD 公開前に VPR を使用して脅威を管理する方法\) \(Tenable ブログ\)](#)
- [Tenable Exposure AI を活用して先行的なサイバーセキュリティを実現 \(Tenable ブログ\)](#)
- [Crushing the Axios supply chain threat with Tenable Hexa AI: Use cases for agentic AI \(Tenable Hexa AI で Axios のサプライチェーンの脅威を解決: エージェント型 AI のユースケース\)](#)
- [Beating the Mythos clock: Using Tenable Hexa AI custom agents for automated patching \(Mythos との時間勝負に勝つ: Tenable Hexa AI カスタムエージェントを活用したパッチ適用の自動化\)](#)
- [Vulnerability remediation: Match CVEs to asset owners in seconds with Tenable Hexa AI \(脆弱性の修正: Tenable Hexa AI で CVE と資産所有者を数秒でマッチング\)](#)
- [Customer Outreach on Tenable Plugin QA/QC Processes \(Tenable のプラグイン QA/QC プロセスに関する顧客向けの案内\)](#)
- [Tenable to Bring Claude Mythos 5 into the Tenable One Exposure Management Platform \(Tenable、Claude Mythos 5 を Tenable One サイバーエクスポージャー管理プラットフォームに導入\)](#)