

Cisco Secure AI Factory with NVIDIA に関する FAQ

目次

Cisco Secure AI Factory with NVIDIA について	2
定義	2
コンポーネント	4

Cisco Secure AI Factory with NVIDIA について

Cisco Secure AI Factory with NVIDIA (Secure AI Factory) により、企業は AI ユースケースの導入を加速させ、かつてないレベルのセキュリティを確保しながら、自信を持って差別化された成果を生み出せるようになります。この拡張性のあるセキュアで高性能な AI インフラストラクチャは、AI ワークロードの開発、展開、保護を合理化することを目的に設計されています。

シスコと NVIDIA 社は、企業が AI を導入するにあたって、一社一社異なる道をたどることを深く理解しています。そのため Secure AI Factory では、垂直統合型ソリューションと、ネットワーキング、コンピューティング、ストレージ、およびセキュリティのコンポーネントを各社固有のニーズに合わせて自由に導入できるモジュール型ソリューションの両方を提供しています。

Secure AI Factory が競合他社の AI インフラストラクチャソリューションと一線を画すのは、Secure AI Factory がセキュリティと、40 年にわたって企業から信頼されてきた市場をリードするシスコの高性能ネットワーキングを基盤として重視していることによります。これにより、企業は、卓越した柔軟性、セキュリティの強化、優れたパフォーマンスを実現できるようになり、進化する AI 環境において自信を持って導入を進めることができます。

定義

Q. Cisco Secure AI Factory with NVIDIA とは何ですか。

A. Cisco Secure AI Factory with NVIDIA の基盤は、2025 年 2 月 25 日に提携拡大の一環として発表された NVIDIA Enterprise Reference Architecture (ERA)、すなわち AI Factory です。このアーキテクチャは、プロセッサ、サーバー、ネットワーキングデバイス、ストレージ、管理機能、およびソフトウェアで構成され、検証済みデザインに基づいており、お客様は垂直統合型またはモジュール型の AI ソリューションのいずれかを選択できます。

Cisco Secure AI Factory with NVIDIA は、このリファレンスアーキテクチャ上に構築されており、シスコの広範なセキュリティポートフォリオの主要な機能でこのアーキテクチャを強化することで、他では得られない高度な保護を実現しています。

データは、AI を運用し、ビジネスを運営していくうえでの通貨のようなものです。AI とデータの統合に伴う固有のセキュリティ課題に対処するには、包括的なセキュリティソリューションが不可欠です。AI の核をなすデータを保護するうえでは、従来のファイアウォールが非常に重要なのですが、AI にはより多くのものが必要です。その中には、データからモデルに至るまで、AI エコシステムの各層を保護するセキュリティソリューションがあります。

Q. Secure AI Factory は、2025 年 2 月 25 日に発表されたシスコと NVIDIA 社の提携にどのように関連しているのでしょうか。

A. 2025 年 2 月 25 日、シスコと NVIDIA 社は、企業への AI 導入を加速するための提携拡大を発表しました。この提携の一環として、次のようなことが発表されました。

- シスコは、NVIDIA Spectrum イーサネット プラットフォームを使用したデータセンタースイッチを開発する予定です。このオープンエコシステムのアプローチによって、より多くの選択肢と柔軟性がお客様に提供されることになります。企業は、Cisco® と NVIDIA 両社のスイッチのシリコンをベースとするアーキテクチャを備えた NVIDIA Spectrum-X ネットワーキング プラットフォームを標準とすることにより、業界をリードする両社のテクノロジーを単一の管理ファブリックの下に統合することができます。
- シスコは、NVIDIA Spectrum-X をベースとする NVIDIA Cloud Partner (NCP) および Enterprise Reference Architecture を、NVIDIA と共同で構築し、検証していきます。これらは、Cisco Silicon One®、Cisco Nexus® Hyperfabric AI、Cisco UCS® Compute、Cisco Optical Networking などのシスコのテクノロジーを基盤としています。

Q. Cisco Secure AI Factory は、NVIDIA AI Factory と何が違うのでしょうか。

A. 2 月下旬に発表したシスコと NVIDIA 社との提携拡大により、Cisco Secure AI Factory の基盤とフレームワークが確立されました。Cisco Secure AI Factory は、シスコのセキュリティソリューションを統合することにより、このフレームワークを拡張し、AI 固有のセキュリティ需要への対応に必要なとされる重要なセキュリティ機能を提供します。

Cisco Secure AI Factory with NVIDIA は、業界をリードするネットワーキングおよび NVIDIA Enterprise AI ソフトウェア プラットフォームで構成され、セキュリティが組み込まれた、フルスタックの検証済みアーキテクチャを提供します。お客様が必要としているのが垂直統合型ソリューションでも、モジュール型 AI アーキテクチャでも、Secure AI Factory はお客様のニーズに合った選択肢を用意し、最先端かつセキュアなインフラストラクチャを提供することで、次世代の AI アプリケーションの開発と展開を合理化および迅速化します。

Q. NVIDIA は Dell および HPE と AI Factory で提携していますが、これと Cisco Secure AI Factory はどのように違うのでしょうか。

A. Cisco Secure AI Factory は、次の 2 つの主要な領域で異なります。まず、Cisco Secure AI Factory は NVIDIA との提携拡大を基盤として構築されており、お客様にネットワーキングの選択肢を提供します。つまり、Silicon One を搭載した Cisco Nexus スイッチまたは NVIDIA Spectrum-X シリコンを搭載したシスコ スイッチのどちらかを選択できるということです。スイッチはすべて、Cisco Nexus Dashboard または Nexus Hyperfabric AI で管理されます。一方、NVIDIA と共同で AI Factory を構築している Dell、HPE、および市場の他の OEM には、このような柔軟性はありません。次に、Cisco Secure AI Factory は、AI モデルからフレームワーク、アプリケーションやワークロード、ネットワーク、ストレージ、コンピューティングに至るまで、ソリューションスタックのあらゆるレベルにおいて AI セキュリティを基盤にしている、利用可能な唯一のソリューションです。

コンポーネント

Q. シスコのセキュリティ製品はどのように **Secure AI Factory** に統合されるのでしょうか。

A. **Secure AI Factory** が、Dell、HPE、Lenovo などの競合他社の **AI** インフラストラクチャ ソリューションと一線を画するのは、その基盤として、ネットワークの選択肢とセキュリティを重視している点です。 **Secure AI Factory** は、シスコのセキュリティソリューションを単に付け足したものではなく、ソリューションを直接組み込んだものになっています。そして、複数の展開オプションから選択することができるため、ソリューションコンポーネントの統合は、お客様ごとのニーズと、シスコのセキュリティ製品の管理およびデータに関する要件によって決まります。また、セキュリティの統合は、選択したシスコのセキュリティオプションによって異なります。たとえば、**Cisco AI Defense** など、一部の製品は **SaaS** で提供され、より簡単に統合できます。 **Cisco Hypershield** などの他のソリューションでは、専用のプロセッシングユニットやアプライアンスなどの追加のインフラストラクチャが必要になる場合があります。

Q. **Cisco Secure AI Factory with NVIDIA** にはどのような製品が含まれますか。

A. **Secure AI Factory** には、基盤となるリファレンスアーキテクチャと追加のセキュリティソリューションという 2 つの柱があります。 **AI Factory** リファレンスアーキテクチャには、次のカテゴリの製品とソリューションが含まれます。

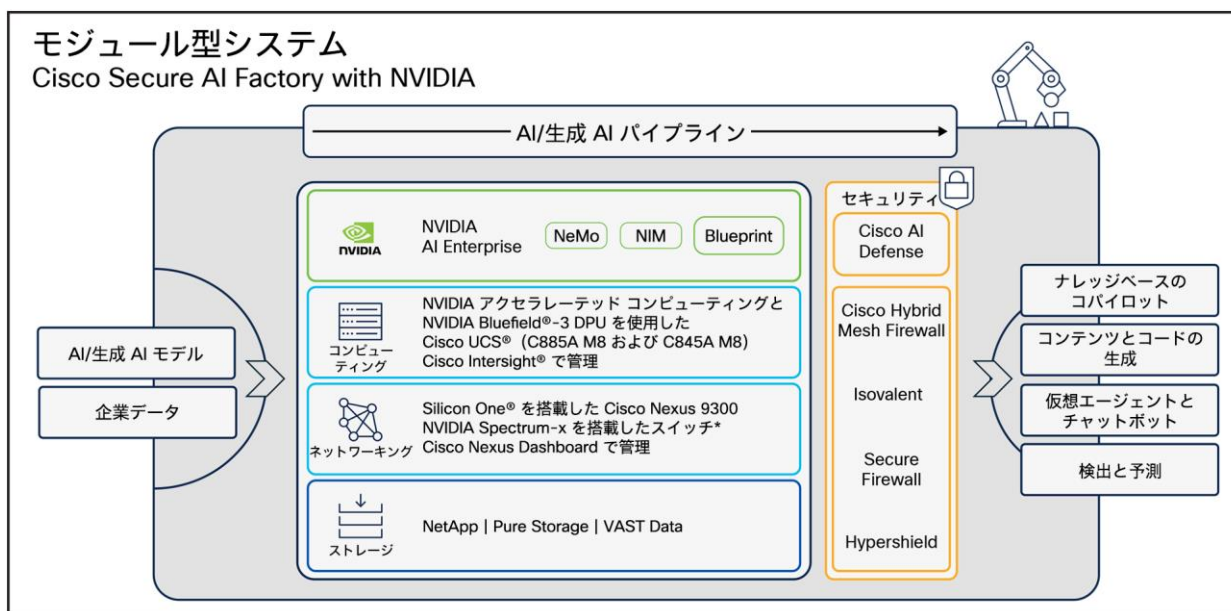


図 1.
モジュール型ソリューションオプション

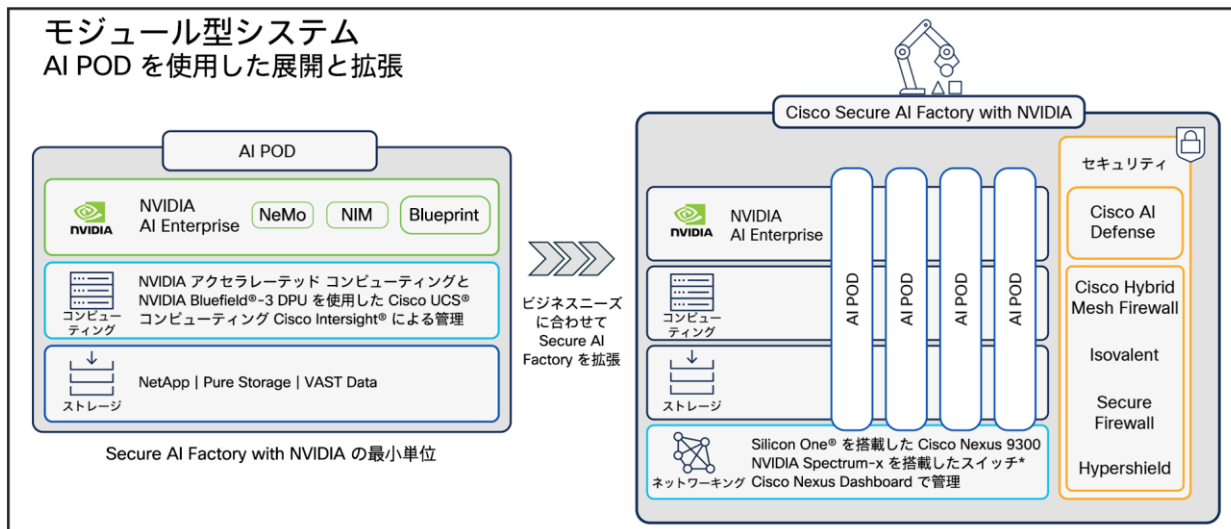


図 2.
Cisco AI POD を使用したモジュール型ソリューションオプション

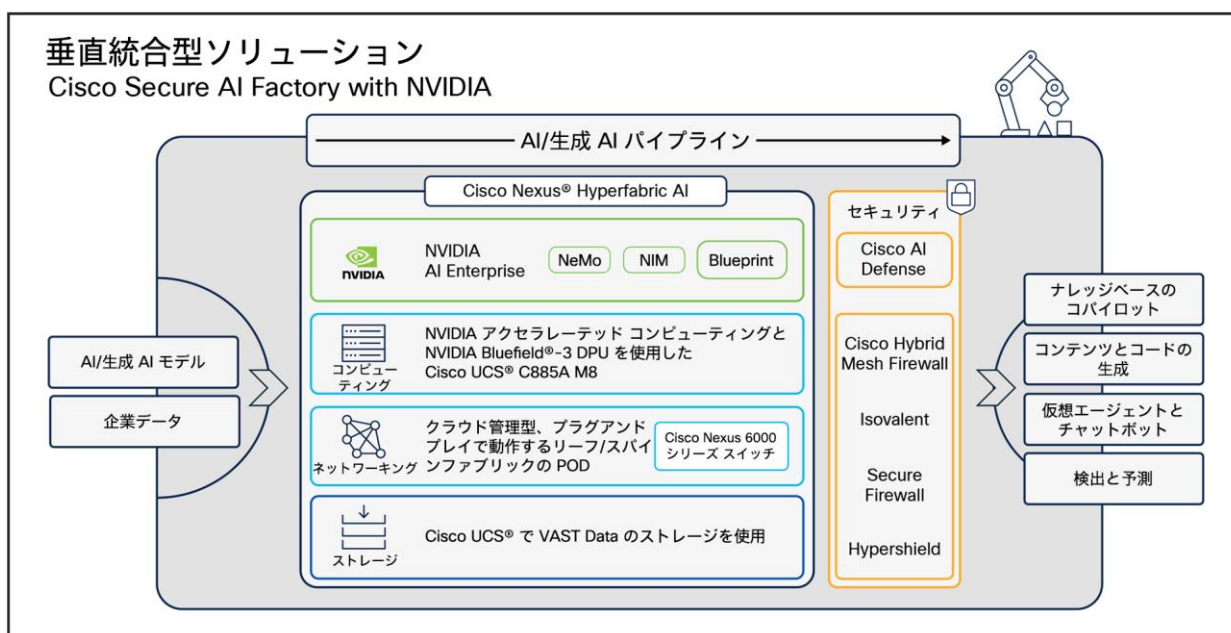


図 3.
垂直統合型ソリューションオプション

Secure AI Factory のフレームワークは、垂直統合型ソリューションとモジュール型ソリューションの 2 つの展開オプションを提供します。これにより、ニーズや希望に応じて製品を選ぶ選択肢が広がります。

たとえば展開しやすいクラウドベースのソリューションを希望する場合、Cisco Nexus Hyperfabric AI と Cisco 6000 スイッチが、ネットワーキングの最適な垂直統合型オプションです。オンプレミス インフラストラクチャを希望するお客様には、Cisco Nexus 9000 シリーズ スイッチと Nexus Dashboard が推奨されるソリューションです。さらに、Cisco AI POD は、ソリューションの構築に使用できる最小単位であり、

NVIDIA プロセッサとサードパーティのストレージ、仮想化、コンテナを組み込んだ検証済みデザインを提供します。

Secure AI Factory では、以下に示すとおり、すべてのレイヤにセキュリティが組み込まれています。

- **インフラストラクチャの保護**：シスコの **Hybrid Mesh Firewall** は、ネットワークスイッチ、従来型のファイアウォール、ワークロードエージェントなどの複数の適用ポイント間で、統合されたセキュリティ管理と一貫性のあるポリシーを提供します。この統合アプローチにより、ディープ パケット インスペクションから広範なインフラストラクチャ カバレッジ、攻撃者の検出、ブロック、封じ込めに至るまで、広範で一貫性のあるセキュリティが確保されます。**Cisco Hypershield** (**Hybrid Mesh Firewall** の一部) は、将来的に、広範なセキュリティ適用を拡張して **NVIDIA Bluefield-3** の管理を組み込み、**AI** クラスタの境界ファイアウォールを実現する予定です。
- **ワークロードの保護**：**Cisco Hypershield** は、攻撃者のラテラルムーブメントを阻止し、パッチを適用せずともプロアクティブに脆弱性を緩和します。これらはすべて単一の管理インターフェイスから行えます。また、プロセスの実行、ファイルアクセス、およびネットワークアクティビティを監視して制御することで、**AI** ワークロードを詳細に可視化し、ランタイムに精密にセキュリティを適用します。将来の機能強化では、**NVIDIA Bluefield-3** の **DOCA AppShield** との統合によってワークロード保護をさらに強化し、**AI** に重点を置いた仮想マシンとコンテナでの侵入検知を実現します。
- **AI アプリケーションの保護**：**Cisco AI Defense** により、セキュリティチームと **AI** チームは、生成 **AI** アプリケーションの堅牢なテストとランタイムセキュリティを実現する包括的なツールを利用できるようになります。**AI Defense** では、アルゴリズムによるレッドチーム手法を利用して、アプリケーションに変更を加えることなく、多様なセキュリティリスク（データプライバシー、プロンプトインジェクションなど）や安全性リスク（有害な動作など）に照らして、生成 **AI** モデルのアプリケーションを評価します。さらに、**AI Defense** はランタイム制御を適用して、アプリケーションが **OPSWAT** の **LLM** や **MITRE ATLAS** などの主要なフレームワークに準拠するようにします。

シスコと **NVIDIA** はそれぞれ、お客様の **AI** インフラストラクチャのニーズを独自に把握しているため、そのインサイトを組み合わせることにより、実証済みのリファレンスアーキテクチャと柔軟な展開モデルを提供できます。**Cisco Secure AI Factory with NVIDIA** は、拡張性のある高性能な **AI** インフラストラクチャを企業に提供します。これにより、**AI** 導入のあらゆる段階にあるお客様をサポートし、すべての段階でセキュリティを組み込みます。

繰り返しになりますが、**Secure AI Factory** では、モジュール型の性質上、クラウドまたはオンプレミス管理のオプションなど、お客様の要件に合わせて統合型ソリューションが調整されます。

Q. Cisco Secure AI Factory with NVIDIA はどのように管理されますか。

A. Secure AI Factory の管理により、幅広い **AI** イニシアチブのサポートに必要となる、柔軟性とパフォーマンスの最適な組み合わせを確保できます。サーバー運用の管理は、**Cisco Intersight** が行います。データサイエンティスト向けの **AI/ML** ツールは、**NVIDIA AI Enterprise** ソフトウェアによってサポートされます。また、シスコが以前 **NVIDIA** 社と共同で構築したシスコのネットワーキングは、**Cisco Nexus Hyperfabric AI** で管理します。このソリューションの直感的なインターフェイスにより、**AI** ファブリックの作成と管理を簡単に行えるようになります。管理機能にはファブリックの包括的な制御が含まれます。また、**NVIDIA** 独自のインサイトを **Silicon**

One に直接取り込むことで、ワークロードの接続性に対する可視性が強化されます。シスコ製品と NVIDIA 製品の統合は、今後も緊密になると予想しています。また、Nexus Dashboard を管理プラットフォームとして提供する予定です。セキュリティソリューションの管理は、Cisco Security Cloud Control で行われ、単一のダッシュボードから AI 関連のセキュリティソリューションにアクセスできるようになります。

Q. Secure AI Factory リファレンスアーキテクチャはいつ頃利用可能になりますか。

A. 具体的な時期は現在検討中です。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム (オランダ)

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/jp/go/offices) をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)