Cisco Intersight プラットフォームのセキュリティ

セキュアなクラウドホスト型管理プラットフォームを提供

信頼できる組み込みセキュリティ

エンタープライズ データセンター、ネットワークの末端、リモートおよび分散拠点に IT インフラストラクチャを備えている場合、各ロケーションで別々のツールを使用すると管理が困難になります。Cisco Intersight™ プラットフォームは、Cisco Unified Computing System™（Cisco UCS®）と Cisco HyperFlex™ システムの管理を統合してシンプル化します。シスコの Infrastructure Management as a Service ポータルにより、セキュアなインターネット接続を介して、IT インフラストラクチャをロケーションに関わらず安全に導入、運用、管理することが簡単に行えるようになります。

目次

Cisco Intersight プラットフォーム

Cisco Intersight Software as a Service（SaaS）プラットフォームは、インテント（実現したいこと）に基づいたインフラストラクチャ設定、継続的管理、能動的な最適化を支援します。このクラウドベースのサブスクリプションモデル ソリューションを活用すれば、ユーザ インターフェイスでサーバ、ハイパーコンバージド インフラストラクチャ、ファブリック インターコネクトを登録し、サービスのライセンスを取得し、リソースを論理グループ（リモートもしくは分散拠点の場所、または仮想化クラスタなど）に分け、ロールベースおよびポリシーベースのインターフェイスを使用するだけで、リソースをロケーションを問わずに設定および管理することができます。

組み込みセキュリティ

Cisco Intersight プラットフォームは、業界標準のセキュリティ テクノロジーを基にして構築された階層型セキュリティ アーキテクチャを使用しています。また、データの暗号化、シスコの厳格なセキュリティおよびデータ処理標準の遵守、管理ネットワーク トラフィックと IT 実稼動ネットワーク トラフィックの分離による隔離性の強化も行っています。その結果、クラウドベースのシステム管理プラットフォームによって、必要とする強力なセキュリティを実現できるという信頼感を提供できます。

変わりゆく管理状況

従来の IT インフラストラクチャでは、複数のポイント製品が使用され、複数のエレメント マネージャで管理されます。シスコは、Cisco Unified Computing System™（Cisco UCS®）によって、IT インフラストラクチャとシステム管理方法の両面で、状況を一変させました。コンバージド インフラストラクチャと組み込みモデルベースの管理機能を兼ね備えた Cisco UCS は、コンピューティングのシンプル化と自動化によって、日常業務の簡易化と効率化を実現します。そして今、Cisco UCS および HyperFlex™ システムの適応型管理ビジョンが Cisco Intersight™ クラウドベース管理プラットフォームへと拡大され、運用管理が新しい時代へと進化しています。

Cisco Intersight の概要

シスコがホストする Cisco Intersight には、クラウドベース管理というメリットがあります。この管理方法は、同様のソリューションである Cisco Meraki™ プラットフォームなどを通じて、顧客から高い評価を受けるようになってきています。管理および自動化プラットフォームは、分析および機械学習技術による強化で効率性を高めるとともに、ますます複雑化する IT インフラストラクチャを管理するために継続的に進化しています。

ソフトウェアは、Cisco UCS 管理機能を使用するシステム インフラ コンポーネントの健全性と関係を監視します。遠隔監視および構成情報が収集され、シスコ情報セキュリティ要件に従って保存されます。データは、直感的なユーザ インターフェイスを介して分離されて表示されます。シンプルで一貫性のあるインフラストラクチャ管理アプローチである Cisco Intersight は、ソフトウェアの拡張が容易であり、動作に影響することなく頻繁に更新が実施されます。そのため、オンプレミスのツールおよびアプライアンスのサポートが容易になります（図 1）。

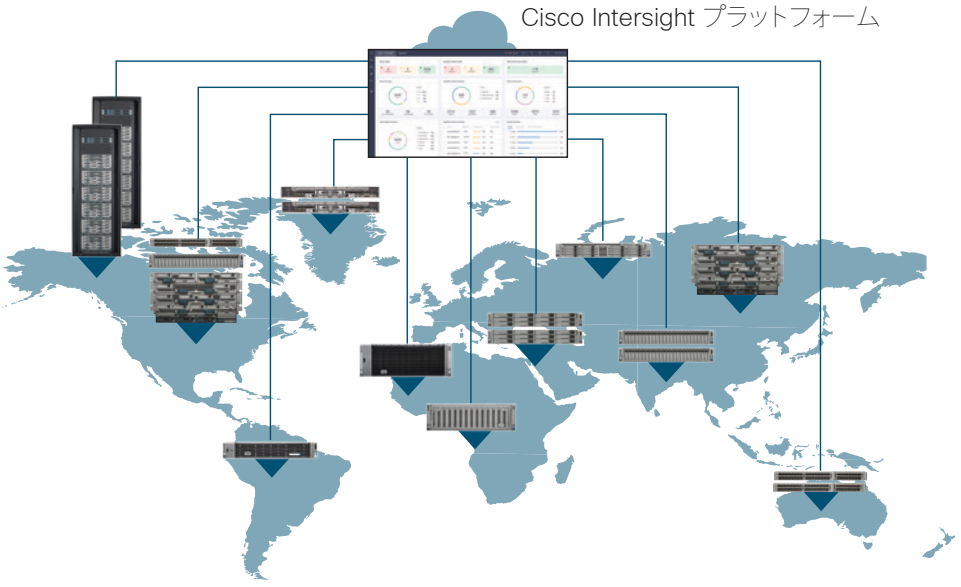

図 1 Cisco Intersight により、ロケーションを問わずにオンプレミス ツールおよびアプライアンスをサポートする上での問題を排除

「カスタマイズ可能なグラフィック ユーザ インターフェイスとビッグデータ対応 IT 運用分析でサポートされる API 主導型の統合管理ソリューションを使用して、一貫性のあるワークロード監視、パフォーマンスの最適化、インフラストラクチャのオーケストレーションができるようになることを、顧客は期待しています」。

IDC:『Worldwide Cloud Systems Management Software Forecast, 2017–2021(世界のクラウド システム管理ソフトウェア市場予測、2017 ～ 2021 年)』、2017 年 2 月、#US41374417。

継続統合/継続供給(CI/CD)プロセスをサポートするよう設計された Cisco Intersight は、適応型システム管理機能を提供します。このソフトウェアは、インストール ベース全体からデータを収集し、あらゆる顧客環境から学習します。データポイントが関連付けられて、問題の兆候を認識するモデルが作成されます。このデータが実践的な知識と結び付いて、Cisco Intersight の進化とスマート化に寄与します。Cisco Intersight の知識ベースが大きくなるにつれ、傾向が明らかになり、推奨エンジンを通じて新しい洞察力と情報が得られるようになります。

知識ベースは、シスコ テクニカル アシスタンス センター(TAC)サポートと緊密に統合され、Cisco UCS コミュニティの専門知識によって補足されます。TAC の膨大な知識ベースとともに Cisco Intersight を使用すると、能動的なシステム サポートが一層充実し、問題の防止に役立ちます。Cisco Insight の推奨エンジンにより情報は統合され、お客様に簡単に使える実用的な形式で提供されます。これらの洞察力および推奨を、自動化されたアクションと組み合わせることで、大幅に効率を向上させ、コストを削減し、解決までの時間を短縮することができます。

セキュリティの重要性

攻撃の高度化と頻度が持続的に進むサイバーセキュリティ情勢の急速な変化に、組織は対応していかなければなりません。Cisco Intersight プラットフォームの設計に着手したとき、シスコは、セキュリティが最重要課題になるであろうことを承知していました。Cisco Intersight には保護メカニズムが組み込まれているため、ユーザは、クラウドベースのシステム管理プラットフォームにより必要とする強力なセキュリティを実現できることを実感できます。

Cisco Intersight プラットフォームのセキュリティ

Cisco UCS と Cisco Intersight のプラットフォームは、どちらもシスコの組み込み保護アプローチを使用して、デバイス、システム、インフラストラクチャ、サービスにセキュリティを提供しています。階層型セキュリティ アーキテクチャを使用している Cisco Intersight は、インターネット e-コマースで広く使用されている業界標準のセキュリティ テクノロジーに基づいて構築されています。また、データの暗号化、シスコの厳格なセキュリティおよびデータ処理標準の遵守、管理ネットワーク トラフィックと IT 実稼動ネットワーク トラフィックの分離による隔離性の強化も行っています。

ロールベースのアクセス コントロール

Cisco Intersight フレームワークは、アクセス許可をリソース(ユーザ アクション、ビュー、オブジェクト)ごとに管理できるきめ細かなアクセス コントロール システムを使用しています。管理者、ユーザ、読み取り専用アクセス ユーザなど、共通のロールが実装されています。また、リソースおよびリソース グループを管理するカスタム ロールが作成可能な柔軟なシステムも提供します。

既存の顧客の認証要件に対応するため、Cisco Intersight のロードマップには、多要素認証(MFA)のサポートと、外部の ID 管理システム(IMS)との統合が含まれています。

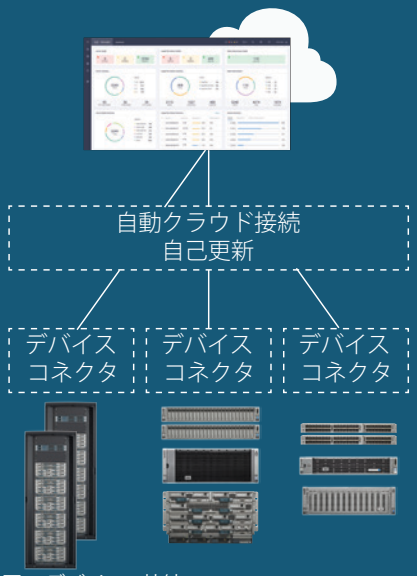

図 2 デバイスの接続

デバイスの接続

Cisco UCS および Cisco HyperFlex システムは、各システムの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight ポータルに接続されます（図 2）。デバイス コネクタは、接続されているデバイスに対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

二要素認証によるセキュアなデバイス登録

最初の手順として、Cisco Intersight プラットフォームで使用するデバイスを登録します。ブラウザを使用してポータルに移動し、[デバイスの登録（Claim Devices）] タブをクリックします。デバイス ID と登録コードを入力します。どちらも、デバイス固有の情報であり、そのデバイス自体から取得できます。デバイス ID は、[管理（Admin）] タブを開いて検索できます。さらに安全対策として、登録コードは 10 分ごとに更新されます。

二要素認証を使用して、登録する各デバイスの ID と信頼性が確認されます。この認証メカニズムにより、デバイス登録プロセスのセキュリティがさらに強化されますが、デバイスへのアクセスだけでなく、Cisco Intersight アカウントと照らし合わせて検証されるデバイス ID 情報も必要です。不正ユーザにデバイス情報を推測されたり知られたりしても、デバイスに物理的にアクセスすることなくデバイスを登録することはできません。

また、デバイスの登録解除やリストから削除も、ポータルを通じて行えます。

データ暗号化と接続セキュリティ

Cisco UCS デバイスと Cisco Intersight プラットフォーム間で交換されるすべてのデータに、業界標準の暗号化およびセキュリティ プロトコルが使用されます（図 3）。接続されたデバイスは、標準の HTTPS ポート 443 上で、限定された暗号方式と HTTPS を伴う Transport Layer Security（TLS）を使用して、Cisco Intersight のみと通信します。Cisco Intersight に送信されるすべてのデータは暗号化され、すべての接続がデバイスからアウトバウンドで開始されます。ファイアウォールでは、すべての着信接続要求をブロックできます。HTTPS ポート 443 のみ、アウトバウンド接続に対して有効にする必要があります。つまり、Cisco Intersight 接続を有効化するのに、ファイアウォールで他に特別な設定は不要です。インターネットからデバイスに直接アクセスされないようにするため、HTTPS プロキシ サーバを使用するようデバイスを設定することができます。

接続セキュリティの確保および中間者攻撃の防止の一環として、Cisco UCS および Cisco HyperFlex デバイスは、Cisco Intersight ポータルのみを接続先とします。つまり、単一宛先の HTTPS URL を使用します。ポータルは、認証局（CA）によって署名された証明書を提示します。未署名の証明書が提示された場合、デバイスはポータルに接続しません。Cisco Intersight ソフトウェアとデバイス コネクタは、デバイス セキュリティ関連のリアルタイム情報を提供するセキュアな管理フレームワークを作成します。このアプローチでは、接続デバイスおよび Cisco Intersight を最新の接続セキュリティ更新と同期させたままにしておくことも可能です。

ポータル インフラストラクチャ

Cisco Intersight ポータルは、Cisco Intersight ポータルを介して供給される SaaS 管理ソリューションです。シスコのスタッフが 24 時間 365 日体制で、ロジスティック上のセキュリティ、運用、および変更管理サポートに対応しています。万一データセンターに障害が発生してもユーザ サービスのフェールオーバーを迅速に実施できるよう、独立した複数のデータセンターにすべてのサービスが複製されています。

データセンターの信頼性と可用性

- 複数のオペレーション チームにまたがる迅速なエスカレーション手順
- 独立した停止アラート システム
- データセンター間での全データの複製（メトリックおよびデバイス設定を含む）
- データセンター間でのリアルタイムのデータ複製
- ハードウェア障害またはその他のデータセンター停止が起きた場合の、Cisco Intersight サービスの迅速なフェールオーバー
- アウトオブバンド アーキテクチャにより、ポータル接続が中断された場合でも、エンドユーザ ネットワーク機能を保全
- フェールオーバー手順の定期検査

セキュアなアウトオブバンド アーキテクチャ

- 接続が遮断されても IT 実稼動ネットワークや管理ネットワークの中断はなし
- 管理ネットワーク データ専用のストレージ
- 機密データ保存時の暗号化
- データセンターの定期侵入テスト

データセンターの認定と適合規格

データセンターの認定および適合規格レポートに関する個別の質問については、Cisco Intersight セキュリティおよびデータ プライバシー チームまでお問い合わせください。

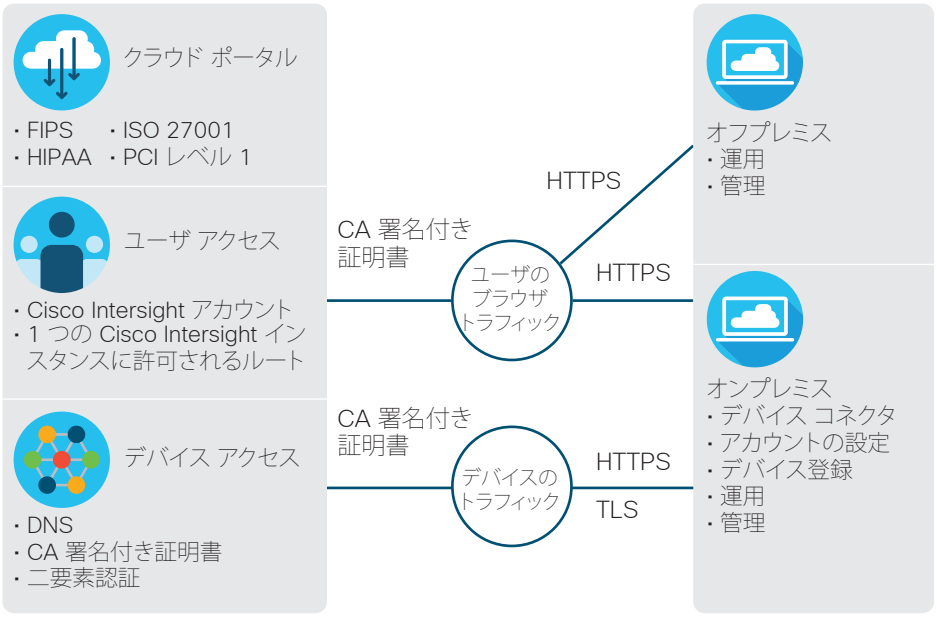

図 3 Cisco Intersight プラットフォームが、ユーザとデバイスのトラフィックを分離し、業界標準のプロトコルを使用して通信

業界標準セキュリティによるコンプライアンス対応

Cisco Intersight プラットフォームは、複数の業界標準セキュリティ プロトコルを使用することにより、情報セキュリティ要件に適合、あるいは要件を上回っています。

- クレジットカード データ保護基準（PCI DSS）は、支払いとクレジット カード情報のセキュリティを保護します。Cisco Intersight 管理はアウトオブバンド方式です。顧客のトラフィック（カード所有者データを含む）は Cisco Intersight プラットフォームを経由しません。Cisco Intersight データセンターは PCI 監査の対象外と見なされていますが、シスコでは、追加措置として、これらのデータセンターについて PCI 認定も取得しています。
- 医療保険の相互運用性と説明責任に関する法令（HIPAA）は、医療情報を保護するものです。ネットワーク上の IIHI（個人を特定できる健康情報）が Cisco Intersight ポータルに送信されることは、決してありません。Cisco Intersight データセンターは HIPAA 監査の対象外と見なされていますが、シスコでは、これらのデータセンターについて HIPAA 認定も取得しています。
- 国際標準化機構（ISO）により公開されている情報セキュリティ標準、ISO 27001 は、情報セキュリティ管理システム（ISMS）を作成するために推奨されるベストプラクティスを提供しています。ISMS は、組織の情報リスク管理プロセスに関わるすべての法律、管理、物理、および技術面の制御を含む、ポリシーと手順のフレームワークです。
- 連邦情報処理標準（FIPS）140-2 は、ハードウェア、ソフトウェア、ファームウェアのソリューションで使用される暗号化機能を検証します。

「私たちは、信頼性、透明性、説明責任を果たすことを目指して努力しています。つまり、当社のインフラストラクチャまたはデータへの脅威を検出するために、あらゆる手段を講じています」。

シスコ最上級エンジニア兼チーフ セキュリティ アーキテクト、Michele Guel

すべてのデータの暗号化

データはすべて、128 ビット セキュア ソケット レイヤ（SSL）セキュリティを使用して、デバイスから Cisco Intersight プラットフォームに送られます。デバイスとポータルの間を移動するデータはすべて、ランダムに生成された 256 ビットのキーによる Advanced Encryption Standard（AES）を使用して暗号化され、公開キー メカニズムによって配信されます。さらに、ポータルへのすべてのデバイス接続に、暗号トークンによる認証が実施されるため、正規のデバイスのみ管理可能となります。

シスコのセキュリティおよびデータ処理標準へのコンプライアンス

インフラストラクチャとデータを保護するには、シスコの IT 部門と情報セキュリティ（InfoSec）部門の間の緊密な連携が必要です。シスコのセキュリティおよび信頼部門（STO）の一部である InfoSec は、シスコの IT 部門と協力して、シスコが構築する製品およびシスコが運営するインフラストラクチャの安全確保に寄与しています。これらのグループは連携して、内外の脅威からシスコのシステムとデータを守りながら、ビジネスの生産性をサポートしています。セキュリティ ハードウェアおよびソフトウェアのみに対象を絞るのでなく、セキュリティに対し、下記のような総合的かつ普遍的なアプローチを取っています。

- 攻撃対象領域を減らし、堅牢なセキュリティ ポスチャを提供するために、セキュリティ意識の高い文化を育成します。
- セキュリティに焦点を当てたポリシーとプロセスを履行します。
- シスコのインフラストラクチャ全体にセキュリティを組み込みます。

シスコでは、人およびプロセスを重視するとともに、セキュリティに焦点を当てたポリシーを適用しています。

- **アクセス管理**：認証、認可、および監査を適正にコントロールすることにより、情報資産および情報システムに対するユーザ アクセスと管理者アクセスの管理についての要件を適用します。
- **監査とリスク評価**：セキュリティおよびデータ整合性のポリシーを遵守し、必要に応じてインシデントの調査やユーザおよびシステムのアクティビティの監視を実施します。
- **クラウド セキュリティ**：ホステッド サービス向けにシスコが構築するクラウドおよびシスコが使用するクラウドに対し、最小限のセキュリティ要件を設定します。
- **暗号化コントロール**：暗号化コントロールを使用して情報資産の機密性、整合性、可用性を保護する方法を説明します。

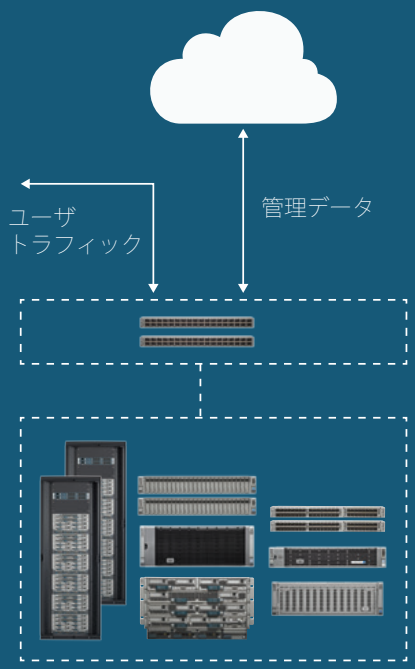

図 4 トラフィックの分離

- **データ保護**：データを分類、ラベリング、保護するための要件を指定します。これらのポリシーによって、情報の相対機密度が定義され、この情報の扱われ方や、シスコの従業員およびその他の当事者への開示方法が定められます。
- **情報セキュリティ**：情報資産の機密性、整合性、可用性を指定するポリシーを適用します。
- **ネットワーク アクセス**：シスコのネットワークにアクセスできる認可済みユーザおよびデバイスを特定します。

管理ネットワークの分離

Cisco Intersight プラットフォームのアウトオブバンド コントロール プレーンは、管理データを、IT 実稼動およびアプリケーション データから分離します（図 4）。設定、監視情報、統計などの管理データは、デバイスから Cisco Intersight ポータルに送られます（図 5）。IT 実稼動およびアプリケーション データは、実稼動データ ネットワーク上の宛先に直接送られます。

アウトオブバンド アーキテクチャを使用すると、インターネットなどのサービスの中断によりデバイスが Cisco Intersight と通信できなくなった場合でも、ユーザには影響が及びません。ユーザはその場合も、ローカルの管理および実稼動ネットワークにアクセスでき、すべての Cisco UCS および Cisco HyperFlex ポリシーと設定が引き続き適用されます。さらに、ローカル ユーザ認証も影響を受けず、Cisco UCS Manager などのローカル設定ツールも、利用可能な状態を維持します。

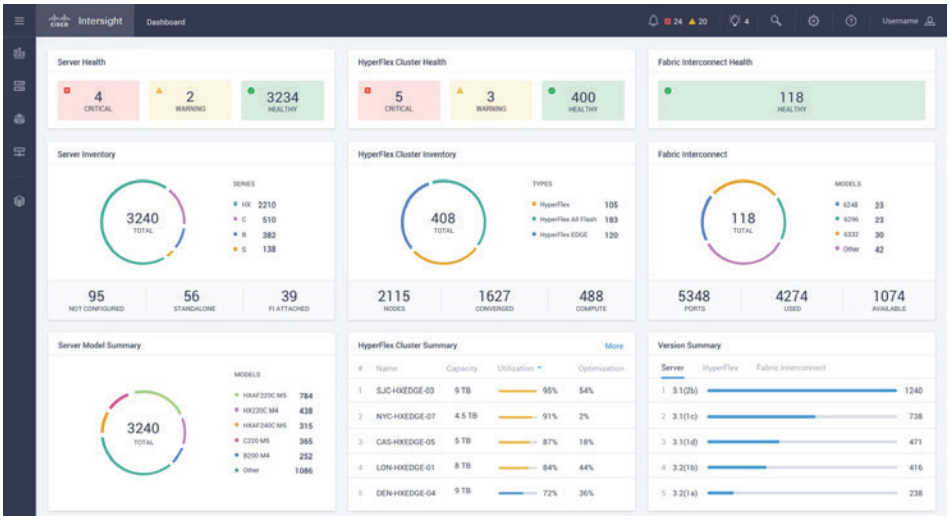

図 5 Cisco Intersight のダッシュボード

詳細情報

Cisco Intersight プラットフォームの詳細については、http://www.cisco.com/go/intersight を参照してください。

運用セキュリティに対するシスコのアプローチの詳細については、http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html を参照してください。

Cisco UCS の詳細については、http://www.cisco.com/web/JP/product/hs/ucs/index.html を参照してください。

Cisco HyperFlex システムの詳細については、http://www.cisco.com/c/ja_jp/products/hyperconverged-infrastructure/index.html を参照してください。

セキュリティ上の優位性の提供

Cisco Intersight プラットフォームの SaaS 管理アプローチは、ローカルおよびエージェント ベースの監視/管理ツールと比較して、セキュリティ上、多くの優位性があります。

- シンプルさ：Cisco Intersight ポータルにより、プラットフォーム管理責任の負担が軽減するので、IT スタッフがその他のタスクや優先事項に集中することができます。
- デバイスの接続性：Cisco Intersight によって管理されるデバイスは、設定および動作ステータス（ファームウェアおよびソフトウェアの現行バージョンを含む）に自動的に接続し、それを報告します。
- 自律性：最初の接続以降は、デバイスでのユーザ操作の必要がなくなります。エージェントまたは他のソフトウェアをインストールしたり保守したりする必要はありません。
- 同期：自己更新デバイス コネクタにより、各デバイスが自動的に Cisco Intersight と同期します。必要なときに、ユーザ操作なしで、パッチやセキュリティ更新プログラムをデバイス コネクタにプッシュすることができます。
- 分析：最新のシスコ検証済み構成に対するハードウェア、ファームウェア、ソフトウェアの適合性を維持するために必要なインフラストラクチャ更新について、Cisco Intersight が、自動収集されたデータに基づく推奨事項を提供します。
- シンプルさ：Cisco Intersight では、エンドポイントのセキュリティとコンプライアンスを追跡および報告するための場所が一元化されています。

LE-63304-00 11/17