Cisco Intersight プラットフォームのセキュリティ

安全な Software as a Service 管理を実現

目次

信頼できる安全な管理

エンタープライズ データセンター、ネットワークエッジ、リモートおよびブランチオフィスに IT インフラストラクチャを設置している場合、それぞれの場所で別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®）サーバーと Cisco HyperFlex™ システムの管理を統合してシンプル化します。Intersight ソフトウェアへのアクセスが、クラウドベースの Software as a Service ポータルからであっても、データセンターでホストしているアプライアンスからであっても、情報テクノロジーの展開や運用、管理が安全かつ簡単になります。

変わりゆく管理状況

従来の IT インフラストラクチャ管理ツールでは、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。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、日常業務の簡素化と効率化を実現します。Cisco Intersight Software as a Service（SaaS）とオンプレミスの Cisco Intersight 仮想管理アプライアンスにより、あらゆる場所にある Cisco UCS と Cisco HyperFlex の両システムを対象に管理の範囲を拡張するという、次のステップを踏み出しました。

Cisco Intersight の概要

クラウドベースのポータルを使用する場合でも、ローカルアプライアンスを使用する場合でも、Cisco Intersight は、オンプレミスシステムと同様のセキュリティとクラウドベースの管理の利点を兼ね備えています。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ながら継続的に進化しており、ますます複雑化する IT インフラストラクチャを管理できるようになっています。

このソフトウェアは、Cisco UCS あるいは HyperFlex の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性を監視します。テレメトリ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ユーザに表示されます。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、代表的な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）。

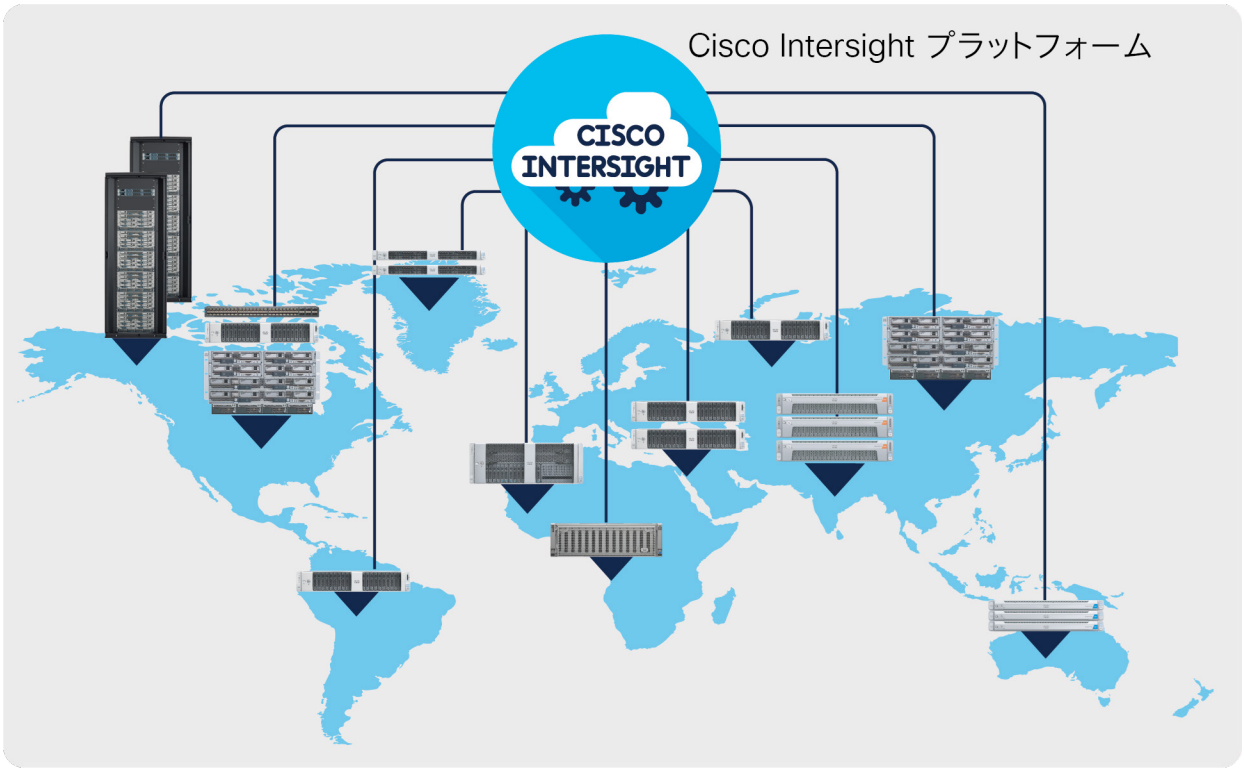

図 1.
Cisco Intersight は、IT リソースの場所に関係なく、インフラストラクチャ管理を簡素化

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 ソリューションで、次の手順に従うだけです。まず、ユーザーインターフェイスを使用して管理対象のサーバー、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ます。次に、サービスのライセンスを取得します。続いて、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）に分けます。最後に、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して、任意の場所にあるリソースを設定し管理します。

組み込みのセキュリティ

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、データを暗号化してシスコの厳格なセキュリティおよびデータ処理標準を遵守し、管理ネットワークと IT 実稼働ネットワークのトラフィックの分離によってさらなる隔離を実現します。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で必要とする強力なセキュリティを実現できるということに確信を持てます。

「カスタマイズ可能なグラフィック ユーザー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。

セキュリティの重要性

攻撃の高度化が持続的に進み頻度が増え続けるという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。シスコは、必要とされている強力なセキュリティを実現するクラウドベースの SaaS 管理プラットフォームを構築しました。ローカル管理サーバをホストすることを好む組織もあるため、同じサービスを実現する Cisco Intersight 仮想アプライアンスも提供しています。これらの製品はいずれも SaaS であり、シスコの継続的な統合プロセスによって最新の状態に保たれます。

Cisco Intersight プラットフォームのセキュリティ

Intersight プラットフォームは、シスコのセキュアな開発ライフサイクルのガイドラインに従って開発、統合、テストされています。このセキュアな製品開発および展開のプラクティスには、設計と開発に関する固有のプラクティス、実装のテスト、展開に関する一連の推奨事項の作成など、いくつかのコンポーネントがあり、最大限のセキュリティを確保しています。シスコの開発プロセスは ISO 27001 の認証を取得しており、Intersight 開発に特化した認証について現在監査が進んでいます。

その結果、デバイス、システム、インフラストラクチャ、およびサービスのセキュリティを提供するためのビルトインされた保護が実現しています。階層型セキュリティアーキテクチャを採用することで、Intersight は、インターネット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、データを暗号化してシスコの厳格なセキュリティおよびデータ処理標準を遵守し、管理ネットワークと IT 実稼働ネットワークのトラフィックの分離によってさらなる隔離を実現します。

シングルサインオン

シングルサインオン（SSO）認証では複数のアプリケーションへのログインに単一のログイン情報を使用できます。SSO 認証では、シスコ アカウントの代わりに企業のログイン情報を使用して Intersight にログインできます。Intersight は SAML 2.0 を介して SSO をサポートし、サービスプロバイダ（SP）として機能して、SSO 認証のために ID プロバイダ（IdP）と統合できます。

ユーザ認証とロールベースのアクセス制御

Intersight アカウントは、ユーザの認証ドメインを形成します。アカウントはすべてのリソースアクセスを制御し、認証されたユーザでも、許可されていないアカウント内のデータを見ることはできません。SaaS プラットフォームでは、Cisco.com の ID プロバイダーでの認証にシスコ アカウントを使用できます。これには多要素認証のサポートが含まれます。Intersight の実装が SaaS であってもオンプレミスであっても、外部の ID 管理システムと統合して、既存の顧客認証要件を満たすことができます。

Cisco Intersight フレームワークは、リソースごとに管理される権限を使用して、きめ細かなアクセス制御を行います。Intersight ソフトウェアでは、ユーザとグループを複数のロールに設定でき、各ユーザまたはグループは複数のロールのメンバーになることができます。実装されるロールには、次の権限が含まれます。

- **アカウント管理者：**Cisco Intersight アカウントおよび管理対象デバイスの完全な制御と管理の機能
- **読み取り専用：**管理下のリソースに対する読み取り専用の可視性
- **デバイス技術者：**Cisco Intersight アカウントへのデバイスの登録を含むデバイスに対する管理アクション

- **デバイス管理者：**Cisco Intersight アカウントからのデバイスの削除を含むデバイスに対する管理アクション
- **HyperFlex クラスタ管理者：**HyperFlex クラスタのライフサイクルとポリシーベースの管理
- **サーバー管理者：**サーバーのライフサイクルとポリシーベースの管理
- **ユーザーアクセス管理者：**ユーザー、グループ、および ID プロバイダの設定

ロールとリソースの管理の詳細については、Intersight のヘルプページを参照してください。

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 SaaS プラットフォームもしくはオンプレミスの仮想アプライアンスに接続されます（図 2）。デバイスコネクタは、Intersight プラットフォームとの間でデバイスが情報を送信し制御命令を受信するために、暗号化された接続をサポートします。

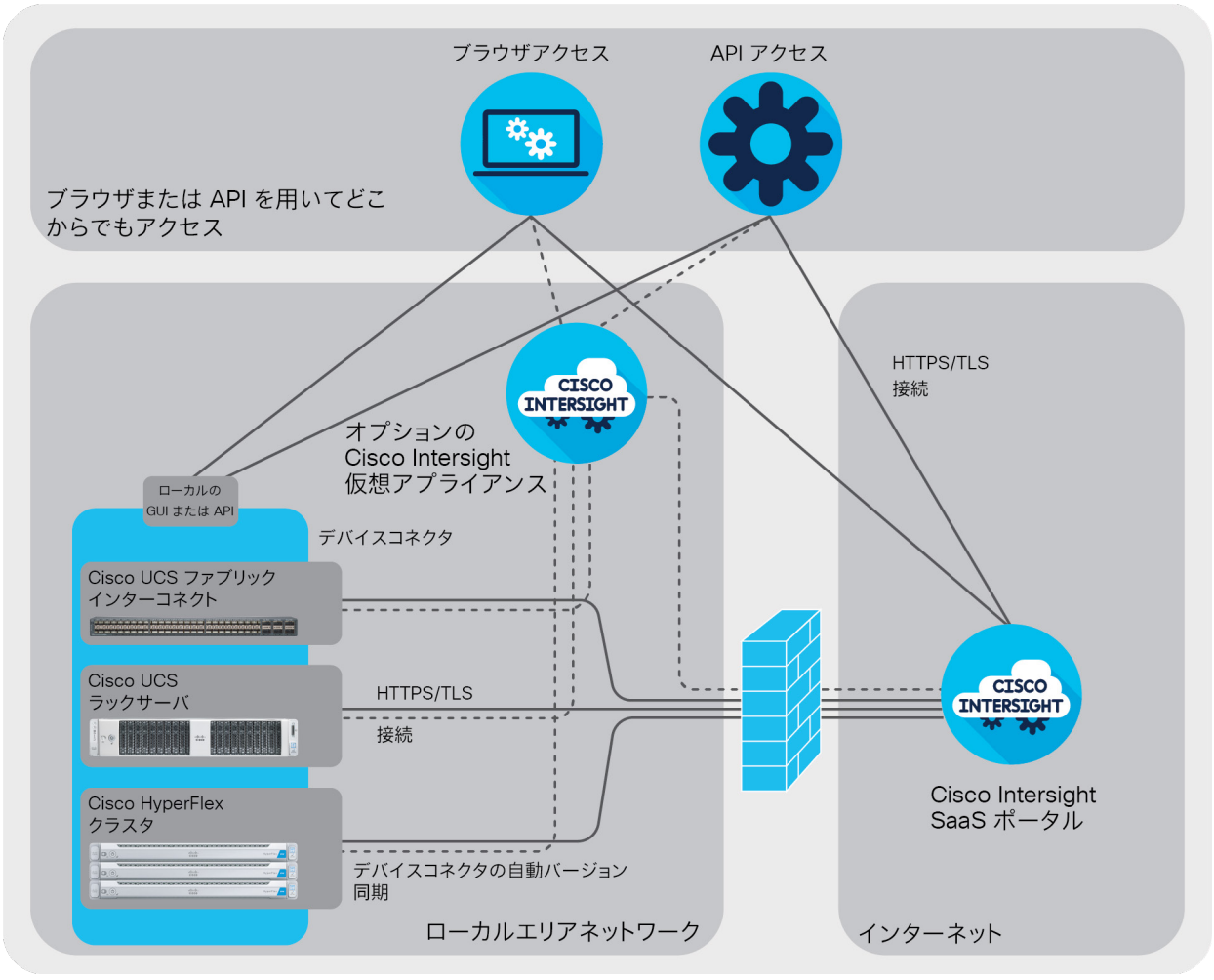

図 2.
Intersight プラットフォームは、ユーザーとデバイスのトラフィックを分離し、業界標準の HTTPS および TLS プロトコルを使用して通信

データ暗号化と接続セキュリティ

デバイスと 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。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と HTTPS を含む Transport Layer Security（TLS）を使用します。Intersight に送信されるデータはすべて、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が暗号トークンで認証されるため、正規のデバイスのみが管理可能となり、潜在的なトロイの木馬の攻撃ベクトルを閉じることができます。

すべての接続はデバイス側から開始されます。したがって、ファイアウォールで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、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。デバイスは、HTTPS プロキシサーバを使用して接続を仲介することでセキュリティのレイヤを追加するように設定できます。

接続のセキュリティを確保して中間者攻撃を阻止できるようにするため、Intersight プラットフォームに直接接続する Cisco UCS および Cisco HyperFlex デバイスは、単一宛先の HTTPS URL を使用します。このプラットフォームは認証局（CA）によって署名された証明書を提示し、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されません。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 Intersight ソフトウェアを最新の接続セキュリティ更新と同期させておくことも可能です。

二要素認証によるセキュアなデバイス登録

Intersight プラットフォームでデバイスを監視および管理するには、まず、Intersight アカウントからデバイスを登録する必要があります。ブラウザを使用してデバイスを登録するには、SaaS または仮想アプライアンスポータルに移動し、[**デバイスの申請（Claim Devices）**] タブをクリックします。デバイス ID と登録コードは、どちらもデバイス固有の情報であり、そのデバイスから取得できます。デバイスのローカル管理インターフェイスからデバイス ID と登録コードを確認できます。追加の予防手段として、登録コードは 10 分ごとに更新され、デバイスを登録する管理者が物理的にデバイスにアクセス可能であることを保証します。

二要素認証を使用して、登録する各デバイスの ID と真正性を認証します。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。デバイスへのアクセスだけでなく、Intersight アカウントと照らし合わせて認証されるデバイス 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。

デバイスの登録プロセスで、ユーザはデバイスを読み取り専用に設定したり、Intersight プラットフォームから制御可能にしたりできます。読み取り専用として設定されたデバイスは、Intersight アカウント内のユーザ権限に関係なく、Intersight ソフトウェアで変更できません。また、デバイスの登録解除や Cisco Intersight アカウントからの削除も、ポータルを通じて行えます。

業界のセキュリティ標準への準拠

Intersight プラットフォームは、次のような多くの業界標準に適用されている InfoSec の要件に合致するか上回っています。

- **連邦情報処理標準（FIPS）140-2：**Intersight は FIPS 140-2 準拠の暗号化モジュールを使用しています。認定は現在計画中です。

このプラットフォームのアウトオブバンド管理アーキテクチャにより、以下の標準あるいは監査の対象外となります。

- **クレジットカードデータ保護基準（PCI DSS）：**お客様のトラフィック（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。
- **医療保険の相互運用性と説明責任に関する法律（HIPAA）：**ネットワーク上の個人を特定できる医療情報（IIHI）は、Intersight ポータルに送信されません。

収集されたデータと保管時の暗号化

Intersight プラットフォームは、ローカル API アクセスと同様に、管理対象システムに対する完全な可視性と制御を備えています。管理対象システムのデバイスコネクタから収集されるデータには、次のものがあります。

- ファブリック インターコネクトと（ストレージコントローラ、ネットワークアダプタ、I / O モジュール、CPU を含む）すべてのサーバおよびノード**のインベントリと設定に関するデータ。**
- Intersight プラットフォームが推奨を自動化するために使用できる（障害などの）**サーバ運用データ。**
- Cisco Technical Assistance Center（Cisco TAC）から要求された場合に作成できる**テクニカルサポートファイル。**

デバイスコネクタは、接続されているシステムに保存されているパスワードなどのセンシティブデータは収集しないことに留意してください。

Cisco Intersight 仮想アプライアンスを使用する場合は、上記のデータをクラウドベースのポータルに渡すかどうかを制御できます。追加のデータ収集をオプトアウトすると、上記の情報はローカルに保持されます。Intersight のヘルプページには、オンプレミスの Cisco Intersight 仮想アプライアンスによって収集されるデータの詳細が記載されています。

収集されたすべてのデータについて、次の追加のセキュリティ対策が実施されます。

- **顧客データ**は、仮想的なデータ分離によって他の顧客データから分離されます。Cisco Intersight サービスによるデータ要求では、お客様のアカウントに固有のデータのみが返され、お客様ごとの暗号化キーがアクセスに使用されます。
- **長期の永続データ**は保管時に暗号化されます。すべてのデータおよびテナントファイルに対して、ブロックストレージまたは同様のボリューム暗号化が有効になっています。
- **サードパーティによる**データへのアクセスは許可されていません。

シスコのセキュリティおよびデータ処理標準へ準拠

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 & トラスト部門（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。セキュリティに関する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。

- シスコのセキュアな開発ライフサイクルのガイドラインに従って Intersight の開発、統合、テストを行っています。
- 設計と開発に関する固有のプラクティスから、実装のテスト、展開に関する一連の推奨事項の作成にいたるまで、最大限のセキュリティを確保する製品開発と展開のコンポーネントをシスコの方法論に組み込んでいます。
- 攻撃対象領域を減らし堅牢なセキュリティ態勢を実現するために、セキュリティ意識の高い文化を育成しています。
- セキュリティに焦点を当てたポリシーとプロセスを導入しています。
- 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んでいます。

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次のような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ーアクセスと管理者アクセスの管理について、要求事項を遵守します。
- **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ー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：**サービスはクラウドベースであり、使用するサービスはセキュリティ要件に準拠する必要があります。
- **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、可用性を保護します。
- **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施行します。
- **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ーおよびデバイスを特定します。

管理ネットワークの分離

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 実稼動データや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 Intersight ポータルに送られます（図 3）。IT 実稼働およびアプリケーションデータは、実稼働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ってデバイスが Intersight ソフトウェア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、ローカルの管理ネットワーク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 の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。

セキュリティ上のメリット

Cisco Intersight プラットフォームの管理アプローチは、典型的な監視ツールや管理ツールと比較して、多くのセキュリティ上の優位性があります。

- **効率性：**Intersight プラットフォームにより、プラットフォーム管理の負担が軽減されるため、IT スタッフがその他のタスクや優先事項に集中できるようになります。
- **デバイスの接続性：**Intersight によって管理されるデバイスは、自動的に接続し、設定や動作ステータス（ファームウェアとソフトウェアの現行バージョンを含む）を報告します。
- **自律性：**最初の接続以降は、デバイスで人が操作する必要はありません。エージェントやその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：**自動更新デバイスコネクタにより、各デバイスが自動的に Intersight プラットフォームと同期します。ユーザが操作しなくても、必要なときに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の更新について、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。

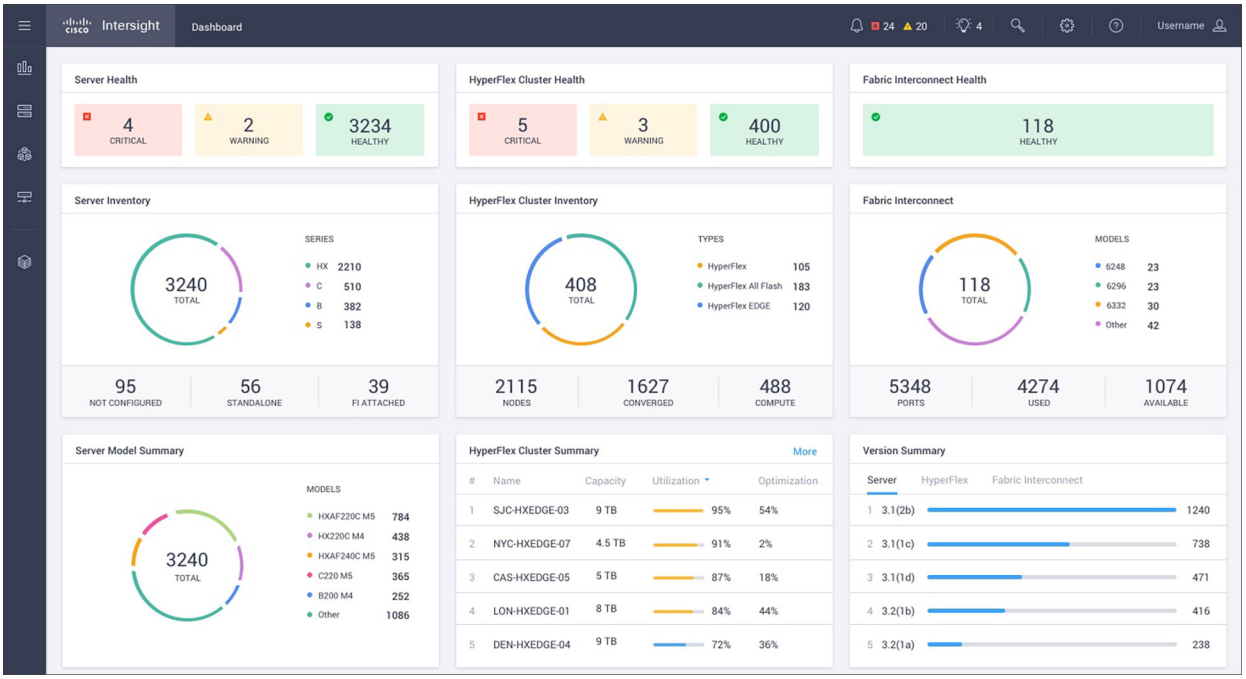

図 3.
Cisco Intersight ダッシュボード

ポータル インフラストラクチャ

Intersight はクラウドベースのポータルから管理できます。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、変更管理に関するサポートを提供しています。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、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、エンドユーザー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接続を維持。
- 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コンプライアンス

- データセンターの認定およびコンプライアンス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。

「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」

Michele Guel
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

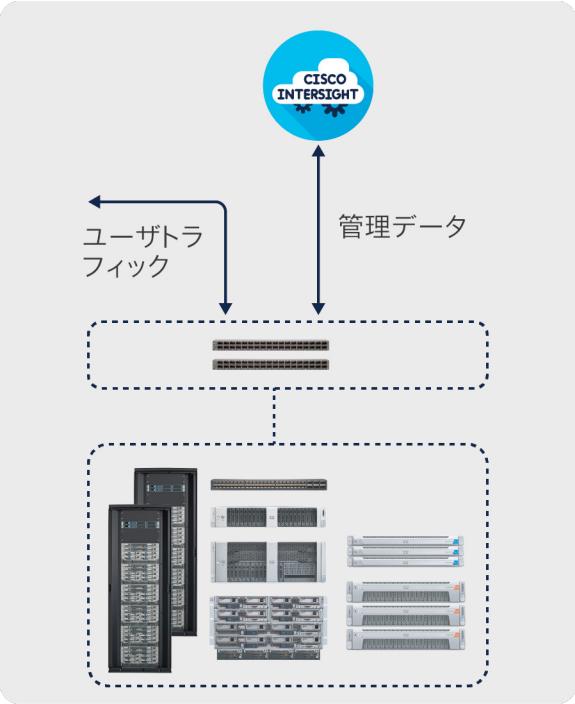

図 4.
トラフィックの分離

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、多くのセキュリティ上の優位性があります。

- **効率性：**Cisco Intersight ポータルにより、プラットフォーム管理の負担が軽減されるため、IT スタッフがその他のタスクや優先事項に集中できるようになります。

- **デバイスの接続性：**Cisco Intersight によって管理されるデバイスは、設定や動作ステータス（ファームウェアと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ー操作が不要になります。エージェントやその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：**自動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。ユーザが操作しなくても、必要なときに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の更新について、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。

詳細情報

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

運用上の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、https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/cs-sec-03232016-operational-security.html をご覧ください。

Cisco UCS の詳細については、https://www.cisco.com/go/ucs をご覧ください。

Cisco HyperFlex Systems の詳細については、https://www.cisco.com/go/hyperflex をご覧ください。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C22-744638-00JA 22.02