

Splunk Enterprise 向け Cisco HyperFlex システム

Splunk ワークロード向けにプライベート Cloud-in-a-Box ソリューションを実装します。

概要

Cisco HyperFlex™ システム:柔軟性、俊敏性、効率性、および拡張性を備えた次世代のハイパーコンバージド プラットフォームとして、Cisco Unified Computing System™ (Cisco UCS®) を搭載しています。ユニファイド ファブリック、ユニファイド マネジメント、および高度な監視機能を提供します。また、サービス プロファイルを使用して一貫性のある迅速な展開が可能のため、使用開始直後から優れたパフォーマンスを発揮します。

Cisco HyperFlex HX データ プラットフォーム:高性能のフラッシュドライブ向けに最適化された分散ファイル システムとして、データ管理、ストレージ効率、遅延などでパフォーマンスを犠牲にすることなく、幅広いエンタープライズクラスのデータ管理および最適化サービスを提供します。

Splunk Enterprise を使用した運用インテリジェンス:Splunk ソフトウェアはコンピューティング、ストレージ、ネットワーク アクティビティ、サービス正常性、ファイアウォールへのアクセス、顧客のクリック操作や通話の記録を含む、あらゆるソースからのデータを監視して分析します。これらのデータは貴重なビジネスの分析情報へと変換されます。

インテリジェントなプライベート Cloud-in-a-Box ソリューション:新しいアプリケーションや運用モデルでは、必要に応じて拡張できるソリューションが必要です。このソリューションでは、スケールアウト設計により高精度のスケーリングを簡素化することで、コストの発生を必要時のみに抑えられます。

Splunk Enterprise を使用した強力な検索、分析、および可視化機能:IT システム、セキュリティ デバイス、およびテクニカル インフラによって生成される膨大なデータ ストリームを、簡単、迅速、かつ安全に分析できます。

検証済みのソリューション:このソリューションは、幅広く展開されるコンバージド インフラ ソリューション ([ビッグデータ向け Cisco UCS 統合インフラでの Splunk](#)) を補完するために作成されました。本ソリューションは、模擬的なワークロードや現実の IT 運用ワークロードを含む、さまざまな仮想マシン構成についてテスト・検証されています。

Cisco HyperFlex システム: 高速かつ柔軟なハイパーコンバージド システム

Cisco Unified Computing System™ (Cisco UCS®) 向けに設計された Cisco HyperFlex™ システムは、ハイパーコンバージェンス ソリューションが持つ力を最大限に活用して、運用の簡素化に必要な俊敏性、拡張性、セキュリティ、およびライフサイクル管理機能を提供します。Cisco HyperFlex システムは、オンプレミス インフラストラクチャの利点を備えた、クラウドの成長に合わせた段階的な投資モデルをサポートします。

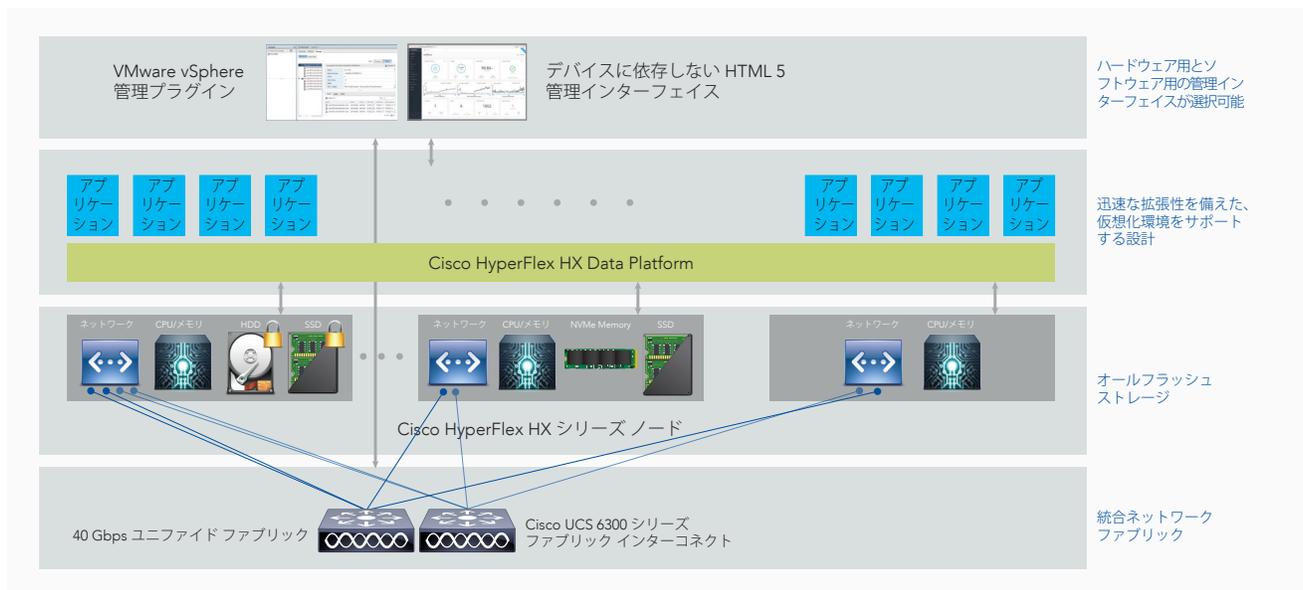


Cisco HyperFlex システムは、Cisco UCS サーバによるソフトウェア定義のコンピューティング、強力な Cisco HyperFlex HX データ プラットフォームを利用したソフトウェア定義ストレージ、そして Cisco® ユニファイド ファブリックによるソフトウェア定義ネットワーク (SDN) が一元化されています。

Cisco HyperFlex システムでは、データ プラットフォームが 3 台以上の Cisco HyperFlex HX-Series ノードにわたって構築されているため、可用性の高いクラスターを実現できます。各ノードには、内部フラッシュベ

スの SSD またはフラッシュベースの SSD の組み合わせを使用してデータを保管する、スケールアウト型の分散ファイル システムを実装した HX データ プラットフォーム コントローラが含まれています。コントローラは 40 ギガビット イーサネット で相互に通信し、クラスター内の複数のノードにわたる単一のストレージ プールを実現します (図 1)。ノードはファイル、ブロック、オブジェクト、API プラグインを使用し、データ レイヤを介してデータにアクセスします。ノードが追加されると、クラスターはそれに比例して拡張され、コンピューティング、ストレージ容量、I/O パフォーマンスを提供します。

図 1: Cisco HyperFlex システムは、シスコ独自の機能セットを搭載した次世代のハイパーコンバージド ソリューションを実現します

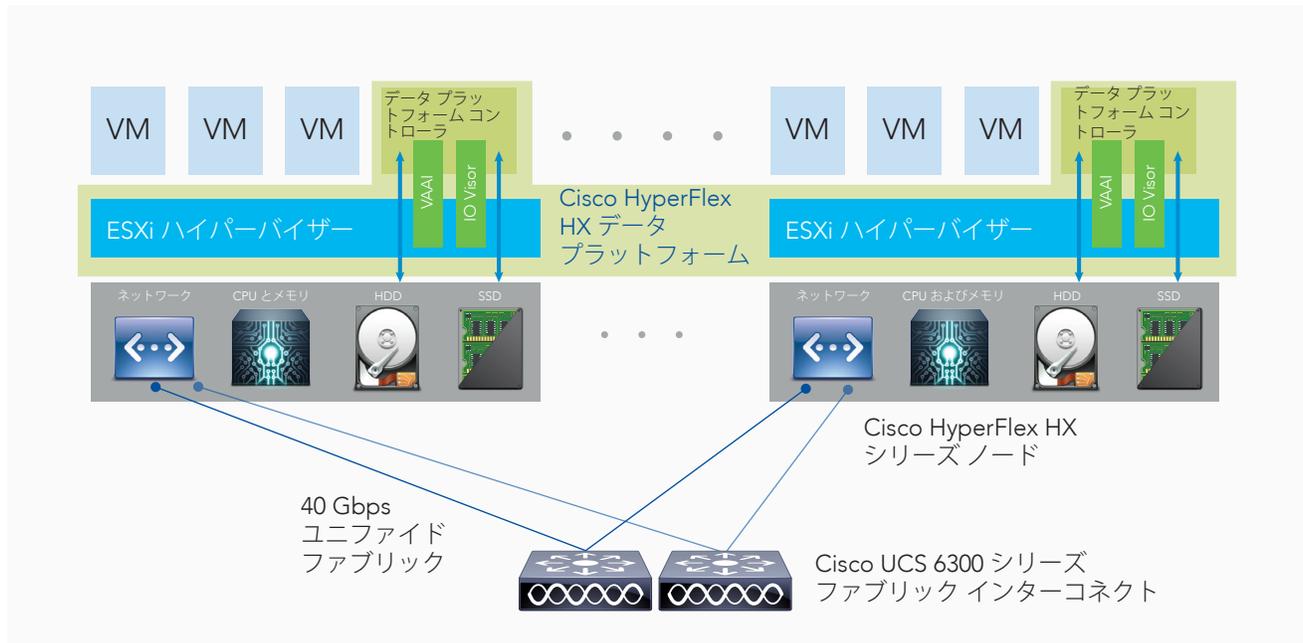


Cisco HyperFlex HX データ プラットフォーム

仮想マシン上のアプリケーションによる固有のデータ要求は、多くのストレージをサイロ化させてきました。Cisco HyperFlex システムの基盤である HX データ プラットフォーム (図 2) は、ハイパーコンバージド環境用に設計された、専用の高性能なログ構造を持つスケールアウト型ファイル システムです。

スケールアウト型の分散ストレージ技術を再定義するデータ プラットフォームの技術革新により、第一世代のハイパーコンバージド インフラストラクチャの限界を超えて、幅広いエンタープライズクラスのデータ管理 サービスを提供します。

図 2: Cisco HyperFlex HX データ プラットフォーム アーキテクチャ



Cisco HyperFlex HX データ プラットフォームは、ハイパーコンバージェンスを実現する業界最先端のプラットフォームとして実績をあげてきました。これは、仮想デスクトップ インフラストラクチャ (VDI)、仮想サーバー インフラストラクチャ (VSI) およびデータベースなどのアプリケーションに最適なプラットフォームです。実稼働環境、テスト環境、および開発環境で使用でき、複数のアプリケーション インスタンスを共存させて、一元化された管理ウィンドウから管理できます。詳細については、[Cisco HyperFlex システムのホワイト ペーパー](#)を参照してください。

エンド ユーザにとって、データ プラットフォームの主な利点は次のとおりです。

- インテリジェントなストレージ管理と、平衡化されたストレージ利用を実現する動的データ分布機能により、一貫したパフォーマンスを保証
- インライン重複排除、圧縮、スナップショット、およびワンボタン操作の無停止のローリング アップグレードなどの、エンタープライズクラスのストレージおよびメンテナンス機能

- Cisco UCS Director を使用した堅牢なレポート作成と分析、自動化、およびオーケストレーション
- 実稼働、開発、テスト、およびリモート拠点/分散事業所など (ROBO) の展開のために成長に応じて効率を拡張できる適応型インフラストラクチャ
- 展開とスケーリングの容易さ。1 時間以内で展開できるため、価値実現の時間を短縮
- 複数のアプリケーションを 1 つの高性能のオールフラッシュ ハイパーコンバージド インフラストラクチャにホストする能力
 - 複数のアプリケーション インスタンス (Splunk、データベース アプリケーション、VDI) をホストできる単一クラスター インフラストラクチャ
 - リソースを複数のプールに論理的に分割し、それによりシームレスなマルチテナンシーを可能にする能力
- 3 ウェイ レプリケーションによるネイティブ データの可用性

機械データ: デジタル インフラストラクチャの原動力

社内のデジタル データ インフラストラクチャを支える相互接続システムは、システムの状況、運用、結果、および侵入のステータスについて膨大な詳細情報を常にもたらします。これらの機械データを運用分析することは、現代のデジタル機器を高効率で稼働し続けるのに不可欠です。複数レベルにまたがる各種の IT システム（ネットワーク スイッチ、ルータ、ファイアウォール、IoT デバイス、仮想マシン、コンテナ、アプリケーション、クラウド）の動作を可視化することは、現在の企業にとって最も重要です。

各システムによって生成されたデータは、それぞれ本質的に異なります。従来のアプローチでは、カスタムビルドのツールを使用して、それぞれの固有のシステム（またはシステム グループ）単位で分析していました。しかし、この分析アプローチではデータのサイロ化が発生するため、意思決定者に対して分析情報を提供するに

は、多くの調整と手作業による関連付けが必要でした。同時に反復的で、手作業を伴うことから、俊敏性、拡張性、および焦点となる範囲も制限されます。

IT 運用インテリジェンスおよびセキュリティ分析のための Splunk Enterprise

Splunk Enterprise は、IT 運用分析向けの主要なプラットフォームです。さまざまな機械データを監視して、デジタル インフラ全体からの運用データの監視、分析、および関連付けを支援します。そのため、競争力と生産性の高い分析情報を意思決定者やビジネス リーダーに提供できます。主要なビジネス意思決定者向けの分析情報に富んだカスタム ダッシュボードは、短期間でビジネス成果を生み出します。また、機械データを詳細分析し、対象を絞った追加の自動臨時検索を実行できるようにするため、複数層の機械データにまたがる相関関係を特定できます。

表 1 は、主な関連性のある業種市場における Splunk Enterprise のユースケースを示します。

表 1: ユースケース

産業界	ユースケース
航空宇宙および防衛産業	<ul style="list-style-type: none">資産の状況、信頼性、およびシステムの整合性を監視するサイバーセキュリティの脅威から重要なインフラを保護するコア IT インフラストラクチャとともにセンサーおよびデバイスからリアルタイムの分析情報を得る
サービス プロバイダー	<ul style="list-style-type: none">サービス プロビジョニングと新製品の提供を迅速化する総合的なセキュリティ ポスチャを改善し、不正行為を削減するカスタマー エクスペリエンスを向上させる
エネルギー/公益事業	<ul style="list-style-type: none">資産の状況、信頼性、およびシステムの整合性を監視するサイバーセキュリティの脅威から重要なインフラを保護する
金融サービス	<ul style="list-style-type: none">サイバー脅威や不正行為から保護するIT 運用効率を向上させる非構造化データを整理する機械学習と高度な分析を使用して、顧客に関する詳細な分析情報を取得する
医療	<ul style="list-style-type: none">システム パフォーマンスを把握し、より広範な医療エコシステムと連携する患者記録を保護し、規制要件に準拠する患者、支払者、およびプロバイダーへの情報アクセスを向上させる

産業界	ユースケース
高等教育機関	<ul style="list-style-type: none"> エンドツーエンドの状況把握を行う IT の運用、規制、および要件を可視化する セキュリティ、コンプライアンス、およびセキュリティ インシデントのリアルタイム監視と問題緩和を向上させる
製造業	<ul style="list-style-type: none"> IT および製造作業を可視化する システムおよびアプリケーションのパフォーマンスと稼働時間を向上させる セキュリティ体制を改善する デバイス、センサー、および機器のパフォーマンスを把握する
オンライン サービス	<ul style="list-style-type: none"> Web サイトのパフォーマンスと稼働時間を向上させ、セキュリティ体制を強化し、カスタマー エクスペリエンスを改善する クラウド、オンプレミス、およびハイブリッド環境を管理する DevOps を監視する
公的機関	<ul style="list-style-type: none"> 3 つの政府部門と 4 つの軍事部門にけるユースケースすべてに対応する サイバーセキュリティを強化する
小売業	<ul style="list-style-type: none"> 販売チャネル全体でシステムおよびアプリケーションでの運用状況を把握する 注文、在庫、および追跡プロセスの状況を把握する クロスチャネルの顧客の行動をリアルタイムで把握する

Splunk Enterprise 向けの参照アーキテクチャ

実績のあるコンバージド インフラストラクチャ ソリューション、[Splunk Enterprise 向け Cisco UCS Integrated Infrastructure](#) は、大規模で可用性の高い、分散化された Splunk の導入に推奨されます。表 2 に要約されている Cisco HyperFlex ハイパーコンバージド オールフラッシュ構成は、Splunk ワークロードの仮想化を希

望するお客様や、社内でのクラウド型アーキテクチャに興味を持つお客様を対象とした補完サービスとして開発されました。このソリューションは、さまざまな仮想マシン仕様の Splunk ワークロードでテスト・検証されています。

表 2: 構成の詳細

サーバノード	<p>Cisco HyperFlex 240c M4 オールフラッシュ ノード x 4。それぞれに以下を搭載。</p> <ul style="list-style-type: none"> Cisco UCS 仮想インターフェイス カード (VIC) 1387 モジュール型 LAN on Motherboard (mLOM) x 1 Intel Xeon プロセッサ E5-2680 v4 CPU x 2 384 GB の DDR4 RAM 800-GB SSD Enterprise Performance (SSD-EP) キャッシュ ドライブ x 1 960-GB SSD Enterprise Value (SSD-EV) オールフラッシュ (キャパシティ) SSD ドライブ x 23
接続性	<p>32 x 40 ギガビット イーサネット ポートを備えた Cisco UCS 6332 ファブリック インターコネクト x 2</p>

図 3 に構成済みのソリューションを示します。

図 3: 構成済みのソリューション



Cisco HyperFlex HX データ プラットフォーム ソリューションは Cisco UCS プラットフォーム上に構築されます。より迅速な導入、より優れた柔軟性、そしてより高い効率性を魅力的な価格で提供しながら、お客様のリスクも軽減します。このアプローチでは、お客様のワークロード ニーズに対応する上で必要なカスタマイズを可能にしながら、計画立案や構成に関する意思決定の必要性を排除または低減します。採用されたプラットフォームと管理モデルは、確立された Cisco UCS データセンター戦略を発展させたものです。この中では、Cisco UCS Manager によるポリシーベースのフレームワークを使用することで、使い慣れたコンポーネントが一貫した方法で管理されています。

Cisco HyperFlex オールフラッシュ システム上の Splunk Enterprise

Splunk の導入は一般に小規模から始まりますが、追加用途に対応する際は迅速に拡張できます。このように迅速に拡張できるインフラストラクチャはきわめて重要です。Cisco HyperFlex オールフラッシュ システムは、次のいずれかの Splunk ソフトウェア ロールをサポートする多くの仮想マシンをホストする際に使用できます。

- **Splunk インデクサ:** インデクサは、データを分散して解析、変換、インデックス作成、および保管する Splunk Enterprise のインスタンスです。検索ヘッドからの検索要求に応じて、インデックス付きのデータを検索します。また、フォワーダがない場合はデータ入力を許可します。

- **Splunk 検索ヘッド:** 検索ヘッドは、分散した Splunk 構成での検索操作のみ実行するように特別に構成された Splunk インスタンスです。検索要求をインデクサの適切なセットに送信して、結果をマージします。高可用性を実現するために、1 つのクラスタに複数の検索ヘッドを構成できます。
- **Splunk ヘビー フォワーダ:** ヘビー フォワーダは、複数のソースからデータを収集し、Splunk インデクサにそれらを転送するように特別に構成された Splunk Enterprise のインスタンスです。
- **複数の Splunk のスタンドアロン Splunk インスタンス:** スタンドアロン インスタンスは、1 日あたり 5 GB よりも少ないデータのインデックスを作成することを意図した Splunk インデクサです。データのインデックス作成と検索を実行し、完全なダッシュボード機能を提供します。

HX データ プラットフォームは、コンピューティング リソースとストレージ リソースを非常に正確なレベルで管理できるようにします。表 3 は、汎用の IT 運用分析、エンタープライズ セキュリティ、および IT サービス インテリジェンスにおけるユースケースで推奨される仮想マシン構成です。

表 3: 汎用のユースケースにおける仮想マシン構成

仮想マシンの仕様 ¹ 構成要素	IT 運用分析 (ITOA) 用の Splunk Enterprise
CPU: 仮想 CPU (vCPU) x 12 ²	1 日あたりのインデックス容量: 最大 250 GB ³
メモリ: 32 GB	
ストレージ: 必要に応じて	

注:

1. 仮想マシンは、インデクサ、検索ヘッド、またはヘビー フォワーダとして機能させることができます。[Splunk 導入の仮想化を実現する Splunk 向けの参照アーキテクチャ](#)を参照してください。
2. Splunk Enterprise Security (ES) や Splunk IT Services Intelligence (ITSI) などのプレミアム ソリューションでは、必要に応じて vCPU やメモリを増やすことを計画してください。
3. インデクサ ノードあたりの推奨最大インデックス容量は、ES ソリューションで ITOA の場合 1 日あたり 250 GB、ITSI の場合は最大 100 GB です。

- ITOA のユースケースの場合、最大 2 TB (日単位のインデックス作成)
- システムが ES または ITSI のユースケースで使用されている場合、800 GB (日単位のインデックス作成)

このソリューションは、次のようなメリットを Splunk ワークロードにもたらします。

- **ハイパーコンバージドプラットフォーム:** Cisco UCS 上に構築された Cisco HyperFlex システムは、ネットワークワーキング、ストレージ、および仮想化リソースを単一のコンバージドシステムに結合します。
 - 高性能のオールフラッシュ システムは、運用開始時から一貫したパフォーマンスを発揮します。
 - インテリジェントなデータ分布は、クラスタ全体で Splunk インデックスを最適なバランスで増加させるため、すべてのインデックスがピーク時のパフォーマンスで動作できる環境を維持します。
 - ネイティブ レプリケーションは、Splunk ソフトウェアへの負荷を軽減させ、Splunk クラスタ管理の必要性を低減します。そのため、Splunk Enterprise は、インデックス作成、検索、およびダッシュボードの表示という中核的機能を実行して、貴重なビジネスの分析情報を提供できます。

- ハイパーコンバージドおよびコンバージド (Cisco UCS Integrated Infrastructure) な Splunk Enterprise の展開は同じ Cisco UCS ドメインでホストできるため、仮想、物理、スケールアップ、およびスケールアウトのニーズに単一の管理ウィンドウで対応します

- **シンプルな管理:** Cisco UCS Manager と VMware vCenter Web クライアントを使用すれば、1 人の管理者が Cisco UCS および Cisco HyperFlex システムを全面的に管理できるため、タスクを簡素化し、作業時間を節約できます
- **迅速な導入:** Cisco UCS Manager のプログラマビリティと使いやすさにより、Cisco HyperFlex システムを迅速かつ一貫して導入できます
 - この機能により Splunk を迅速に導入できます
 - Splunk はすぐに使用できるソリューションです
- **一貫したパフォーマンス:** 一貫したパフォーマンスを維持しつつ、Splunk ワークロードによるハードウェア/ソフトウェア プラットフォーム リソースの使用率を大幅に低減できます

表 4 は、Cisco HyperFlex HX データ プラットフォームに Splunk Enterprise を導入するためのガイドライン¹です。²

表 4: 導入のガイドライン

日単位のインデックス作成量					
ユーザ総数	100 GB 未満/日	100 ~ 300 GB/日	300 ~ 600 GB/日	600 GB ~ 1 TB/日	1 ~ 2 TB/日
最大 4 個	1 つの結合インスタンス	1 つの結合インスタンス	1 つの検索ヘッドと 2 つのインデックス	1 つの検索ヘッドと 3 つのインデックス	1 つの検索ヘッドと 7 つのインデックス
最大 8 個	1 つの結合インスタンス	1 つの検索ヘッドと 1 つのインデックス	1 つの検索ヘッドと 2 つのインデックス	1 つの検索ヘッドと 3 つのインデックス	1 つの検索ヘッドと 8 つのインデックス
最大 16 個	1 つの検索ヘッドと 1 つのインデックス	1 つの検索ヘッドと 1 つのインデックス	1 つの検索ヘッドと 3 つのインデックス	2 つの検索ヘッドと 4 つのインデックス	2 つの検索ヘッドと 10 つのインデックス
最大 24 個	1 つの検索ヘッドと 1 つのインデックス	1 つの検索ヘッドと 1 つのインデックス	2 つの検索ヘッドと 3 つのインデックス	2 つの検索ヘッドと 6 つのインデックス	2 つの検索ヘッドと 12 つのインデックス
最大 48 個	1 つの検索ヘッドと 2 つのインデックス	1 つの検索ヘッドと 2 つのインデックス	2 つの検索ヘッドと 4 つのインデックス	2 つの検索ヘッドと 7 つのインデックス	3 つの検索ヘッドと 14 つのインデックス

¹ これは単なるガイドラインです。ユースケースに基づいてこれらの数字を変更してください。

² 参照されているハードウェア要件を満たすインデックスは、検索の負荷をサポートしながら、1 日あたり最大 250 GB まで処理できます。

まとめ

機械データは豊富な分析情報を提供し、組織の成功と効率化を可能にします。しかし、適切なデータ分析プラットフォームを使用しなければ、それらのデータの分析は複雑化する可能性があります。Splunk Enterprise は、それらのデータからリアルタイムの分析情報を導出します。また、Cisco HyperFlex システムの俊敏性、一貫性、および復元力により、ハードウェア リソース管理の複雑さや迅速な展開の必要性、そして運用上のニーズに対処します。Splunk Enterprise および Cisco HyperFlex システムは、ビジネス成果をよりスマートに達成できる次世代のデジタル データセンターを、より迅速に構築・維持できるように支援します。

詳細情報

他の情報については、次の項目をご覧ください。

- www.cisco.com/c/ja_jp/solutions/data-center-virtualization/big-data/index.html
- www.cisco.com/go/bigdata_design
- www.cisco.com/c/ja_jp/products/servers-unified-computing/index.html
- www.cisco.com/c/ja_jp/products/hyperconverged-infrastructure/index.html



© 2017 Cisco and/or its affiliates. All rights reserved. Cisco およびシスコロゴは、シスコ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は、http://www.cisco.com/web/JP/trademark_statement.html でご確認ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2017 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, および SPL は、Splunk Inc. の米国およびその他の国における商標です。 C22-739511-00 08/17