Cisco HyperFlex Security の優位性

保管データの保護

- 自己暗号化ドライブにより保管データを暗号化します。
- エンタープライズ キー管理ソフトウェアと統合することにより暗号キーを管理します。
- Cisco HyperFlex™ Connect インターフェイスでセキュリティ ライフサイクル全体を管理します。

規制への準拠

- 保管データを暗号化することでデータの機密性を確保し、データプライバシー規制にも準拠できます。

セキュア プラットフォームを使用

- シスコは脆弱性アセスメントを継続的に実施しており、脅威に対する保護を支援します。
- 製品開発プロセスの一環として、すべてのコンポーネントのセキュリティを維持・強化しています。

機密データの損失は重大なビジネス リスクを招きます。シスコはデータのプライバシーと整合性の維持を支援します。

Cisco HyperFlex™ クラスタでは、シンプルな保管インターフェイスとデータ暗号化により、保管データの安全を確保します。シスコのポリシー ベースの管理アプローチによって、セキュリティに対してクラスタ全体で統一性と一貫性を確保し、規制に準拠したセキュアな暗号化管理と導入を実現します。

企業にとって重要なアプリケーションを Cisco HyperFlex システムに移行する際、セキュリティをプラットフォーム全体に統合させる包括的なアプローチを提供します。保管データ暗号化によって、セキュリティのベスト プラクティスの採用が求められる規制に準拠できます。さらに、脆弱性や脅威から保護するセキュアな開発ライフサイクルに基づいて強化されたプラットフォームを提供します。これらすべての機能を備えた Cisco HyperFlex システムは、最も重要なビジネス アプリケーションに対する信頼性の高いソリューションになります。

保管データの保護

Cisco HyperFlex ノードに保管されるデータセキュリティは、次のコンポーネントを統合し、高度なセキュリティ機能によってデータが保護されます。

- 自己暗号化ドライブ（SED）により、パフォーマンスを犠牲にすることなく暗号化できます。
- エンタープライズ キー管理により、暗号化キーが保護されます。
- Cisco HyperFlex Connect インターフェイスでは、簡単にデータ セキュリティを設定・管理できます。

ハイグレードのセキュリティ コンポーネント

自己暗号化対応のハードディスク ドライブ（HDD）とソリッドステート ディスク（SSD）ドライブを各ノードに統合することから始めます。データ ストリーム内のハードウェア アクセラレーションの暗号化モジュールにより、データがドライブ間で転送される際のパフォーマンス上の影響が最小限に抑えられています。ハイブリッド（HDD および SSD ドライブ）ノードとオールフラッシュ ノードの両方で SED がサポートされています。

鍵を玄関マットの下に隠していては、データは安全であるとは言えません。エンタープライズ キー管理システムと統合したのはそのためです。お客様のディスクの暗号化キーは、次のような業界をリードするキー管理ソリューションによってセキュアに保たれます。

- Gemalto SafeNet KeySecure
- Thales Vormetric Data Security Manager

これらのソリューションを利用したキー管理プロセスがシスコのプラットフォームと統合されたことで、セキュアでシンプルな暗号化を実現しています。このソリューションには、レポート、コンプライアンス追跡、および監査機能も含まれています。Cisco HyperFlex システムは、KMIP（暗号化ドライブのキー管理プロトコル）1.1 に準拠しているため、今後その他の互換性のあるキー管理システムとも簡単に統合できます。

Cisco UCS® Manager に組み込まれたオプションによって、ローカル キーまたはパスフレーズを使用することもできます。

シンプルな管理

エンタープライズ キー管理またはローカル キー管理のどちらを使用する場合でも、Cisco HyperFlex Connect インターフェイスで暗号キー設定処理を制御できます（図 1）。この使いやすい HTML 5 インターフェイスにより、クラスタ内の SED で、有効化、設定、キー再生成、セキュアなデータ消去のプロセスが簡単になります。

キー管理ワークフローは、Cisco HyperFlex と管理システムとの間で証明書ベースの信頼性を持った接続を形成します。

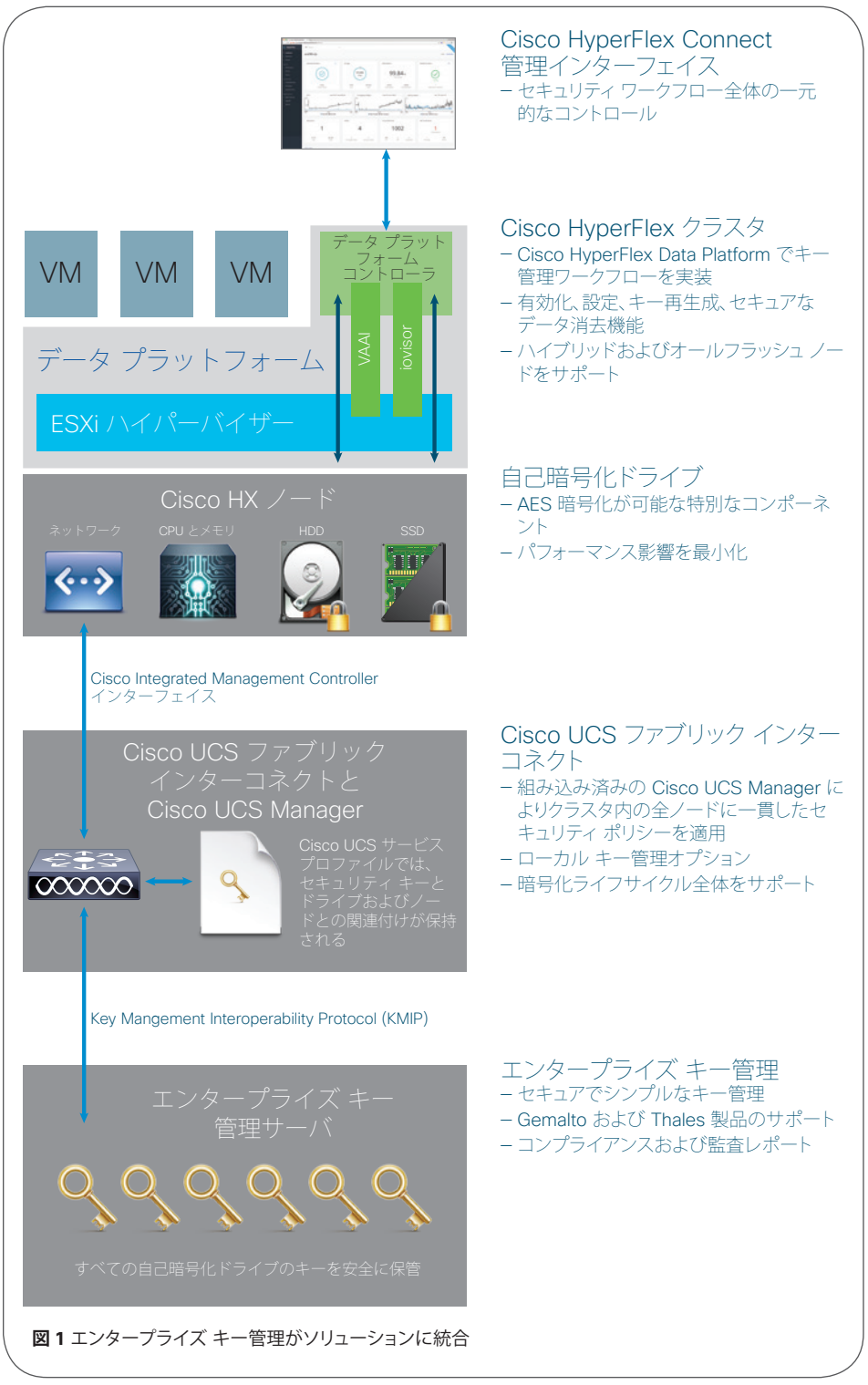

図 1 エンタープライズ キー管理がソリューションに統合

保管データの保護

- 自己暗号化ドライブにより保管データを暗号化します。
- エンタープライズ キー管理ソフトウェアと統合することにより暗号キーを管理します。
- Cisco HyperFlex Connect インターフェイスでセキュリティ ライフサイクル全体を管理します。

HX データ プラットフォームとキー管理サーバの間で証明書ベースの信頼チェーンを確立します。各ノードではこの接続を使用して、ドライブのロック解除に必要な暗号化キーを安全に転送できます。

運用セキュリティ

セキュリティに対するシスコのアプローチでは、暗号化とキー管理がクラスタ全体に同じ方法で一貫性をもって導入されるようにポリシーが確立され、適用されます。このアプローチにより、セキュリティを損なう一貫性が欠けたセキュリティが実装される心配がなくなります。ポリシー実装が自動化されているため、クラスタ内の多数のノードとその SED に設定を繰り返し適用できます。

Cisco UCS Manager では Cisco Unified Computing System™（Cisco UCS）サービス プロファイルを使用して、セキュリティ ポリシー、データ プラットフォーム、キー管理ソフトウェア間の設定、処理が指定できます。それらのプロファイルと、各サーバに対して Cisco UCS Manager が設定する 100 を超える ID、設定、および変数により、すべてのノードで、規制に準拠した一貫性のある導入を行うことができます。設定と導入が自動化できる（個別の手作業設定をなくせる）ため、新しいノードを追加してクラスタを拡張するプロセスはシンプルで簡単です。

規制への準拠

データ プライバシー

規制への準拠にはプライバシーが不可欠であり、データのプライバシーは暗号化によって実現します。保管データの暗号化機能を備えた Cisco HyperFlex システムにより、業界固有の多数の規制に対するコンプライアンスが確保できます。このような規制は、次に示すもの（アメリカのケース）を始め多数あります。

- 医療保険の相互運用性と説明責任に関する法令（HIPAA）
- クレジットカード データ保護基準（PCI-DSS）
- 連邦情報セキュリティ マネジメント法（FISMA）
- 一般データ保護規制（GDPR）
- Sarbanes-Oxley 法

Cisco HyperFlex Connect 管理インターフェイスを利用して、保管データ暗号化の設定およびセキュリティ ライフサイクル全体の管理が簡単に実施できます。Cisco HyperFlex Connect では Cisco UCS サービス プロファイルを使用して、各ノードの設定とセキュリティ特性を指定できます。この機能により、ダウンタイムやセキュリティ上の脆弱性の原因となる、設定の不整合が発生するリスクが低減します。

認定

保管データのセキュリティのために、Cisco HyperFlex システムでは、自己暗号化ドライブを使用し、FIPS 140-2 に対して検証済みのエンタープライズ キー管理システムとの統合を図っています。

規制への準拠

- 保管データを暗号化することでデータの機密性を確保し、データ プライバシー規制にも準拠できます。

また Cisco HyperFlex システムは、情報技術セキュリティ評価（ITSEC）に関する評価保証レベル（EAL）2 に対するコモンクライテリア認証も取得しています。

シスコはセキュリティに関する広範な専門知識を全社的に備えており、グローバル認定および共通セキュリティ モジュール チームは、FIPS 認定に対する革新的なアプローチを確立しています。このグループは、信頼性の高い多様なシスコ製品に組み込み可能な、FIPS 検証済み暗号化モジュールを開発しています。コンプライアンス プロセスでは、基準に従った暗号化が製品に実装されていることが検証されます。Cisco HyperFlex システムで利用しているこのモジュール使用は、コンプライアンス レビューを経ています。

セキュア プラットフォームを使用

シスコはソフトウェア ライフサイクルの一環としてセキュリティを統合しているため、IT 部門の信頼を得ています。セキュリティは最初から製品に組み込まれ、シスコのソフトウェア開発チームが実装したシスコ セキュア開発ライフサイクルに従って、継続的に改善され強化されます。

プラットフォームの強化

Cisco UCS Manager や Cisco HyperFlex HX Data Platform、ハイパーバイザ自体など、Cisco HyperFlex システムに統合されているすべてのソフトウェアが大幅に強化されています。

この強化はセキュリティ技術導入ガイド（STIG）に従って行われ、認定基準の推奨事項が適用されています。たとえば、Cisco HyperFlex のベスト プラクティスと複数の VMware ESX Server のセキュリティ推奨事項を導入して、システムの検証が実施されています。

継続的な脆弱性アセスメント

強化されたシステムのセキュリティを長期にわたって維持するために、シスコでは Nessus スキャンを使用した定期的な脆弱性アセスメントを実施し、脆弱性データベースを高い頻度で更新しています。

管理セキュリティ

Cisco HyperFlex システムの管理は、最初からセキュリティが確保されています。Cisco HyperFlex Connect インターフェイスを使用することで、保管データの暗号化のエンドツーエンドのライフサイクルを含む、クラスタ運用のあらゆる側面を管理できます。クラスタ管理のセキュリティは、Microsoft Active Directory や Lightweight Directory Access Protocol（LDAP）を含め、vSphere シングル サインオン（SSO）に統合されたエンタープライズ認証および認可メカニズムによって確保されます。

セキュア プラットフォームを使用

- シスコは脆弱性アセスメントを継続的に実施しており、脅威に対する保護を支援します。
- 製品開発プロセスの一環として、すべてのコンポーネントのセキュリティを強化、維持しています。

詳細情報

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。

ロールベース アクセス コントロール（RBAC）により、設定変更できる管理者と、モニタリング目的の読み取り専用権限を持つ管理者を指定できます。Cisco HyperFlex Connect インターフェイス、Representational State Transfer（REST）API、コマンドライン インターフェイス（CLI）で行った変更を監査できるため、不正な変更はその発生元まで追跡できます。

管理インターフェイスを通して、Cisco UCS Manager が一貫性のある設定とキー管理をクラスタ全体に導入します。

まとめ

Cisco HyperFlex システムは、セキュリティに対する全体的なアプローチで、次のようにエンタープライズ アプリケーションをサポートします。

- 保管データを保護
- データ プライバシーが要求される規制への準拠に対応
- セキュアなプラットフォームによってアクティブな攻撃から防御

Cisco HyperFlex システムに組み込まれたセキュリティは、ソフトウェアのライフサイクルにセキュリティを統合してきた、シスコの長期にわたる取り組みの 1 つの成果です。Cisco HyperFlex システムのライフサイクルにセキュリティが組み込まれるため、お客様はこの優れたセキュリティ対応を利用できます。

LE-60301-00　07/17