設計に包括的セキュリティを組み込んだ Dell EMC VxRail

2020 年 10 月

ホワイト ペーパー

要約

IT インフラストラクチャとセキュリティのトランスフォーメーションに理想的なプラットフォームである VxRail なら、データやビジネス アプリケーションのセキュリティを守る保護レイヤーを手に入れられます。絶え間なく進化する昨今の脅威のランドスケープに対処するのに必要な完全なエンドツーエンドのソリューションを提供できるのは、デル・テクノロジーズ ファミリーの企業をおいて他にありません。本書では統合されたセキュリティ機能やオプションの機能、ベスト プラクティス、実証済みの手法を用いてコアからエッジ、クラウドまで VxRail のセキュリティを守る方法について説明します。

デル・テクノロジーズのソリューション

DELL Technologies

著作権

目次

はじめに

あらゆる業界の企業が運用のあり方をモダナイズし、差別化された製品やサービスの提供方法を変革しようという動きを見せています。データのある場所、そのデータへのアクセス方法、デバイスの数、そしてコアからエッジ、クラウドまで、検討すべきことは多岐にわたります。セキュリティは常に IT の一部として、切り離せない関係にあります。とりわけ認証、ファイアウォール、コンプライアンス、サイバー犯罪の領域ではセキュリティが重視されます。セキュリティは今やプロジェクトの一部などではなく、絶えず評価し分析を重ねなければならない継続的なライフサイクルなのです。デル・テクノロジーズは、セキュリティが決して足かせとなるものではなく、むしろイノベーションを加速させ、新たな戦略的視点を提示し、チャンスを引き寄せてくれるものだと考えています。

Dell EMC の VxRail ならコアからエッジ、クラウドまでセキュリティ トランスフォーメーションをもたらす最短かつ最もシンプルな道筋を提示できます。VxRail にはフルスタックの整合性があり、エンドツーエンドのライフサイクル管理が可能な機敏なインフラストラクチャによって、運用効率を高め、リスクを軽減し、チームがビジネスに集中できる環境を整えてくれます。運用上のサイロを解体しワークロードの迅速なプロビジョニングと導入によって継続的なイノベーションを実現する VxRail システムなら、大幅なコストの節約と運用効率の向上が見込めます。ひいては IT 部門を、業務をサポートするだけの裏方ではなく、ビジネス チャンスを後押しできる存在へと変えることができます。VMware を強化するために、VMware によって開発された、VMware のための VxRail は、VxRail ハイパーコンバージド インフラストラクチャでの導入、プロビジョニング、管理、監視、更新にまつわる運用の複雑さを解消するべく VMware と共同で設計された、初めてにして唯一の HCI システムです。

VxRail には統合されたテクノロジー スタックのあらゆるレベルにセキュリティが組み込まれています。個々のプロセッサーから PowerEdge サーバーをはじめ、VxRail HCI システム ソフトウェア（統合された VMware ソフトウェアも含む）に至るまで網羅的なセキュリティでコア、エッジ、クラウドを保護するとともに、従来のワークロードからクラウド ネイティブなワークロードまで隈なく可用性、整合性、信頼性を確保します。

デル・テクノロジーズと始めるセキュリティ トランスフォーメーション

デル・テクノロジーズという企業におけるセキュリティ トランスフォーメーションの目的はセキュリティの概念を根本から見直し、イノベーションを加速させることにあります。デル・テクノロジーズは関連企業との協業から製品が開発され、販売された段階に至るまで、あらゆる面のセキュリティを重視しています。VxRailも例外ではありません。最高レベルの製品セキュリティ アシュアランスを持ったVxRailなら、完全に統合されたセキュリティ機能によってサイバーセキュリティの耐久性をエッジからコア、クラウドまで最適化し、イノベーションを加速することができます。

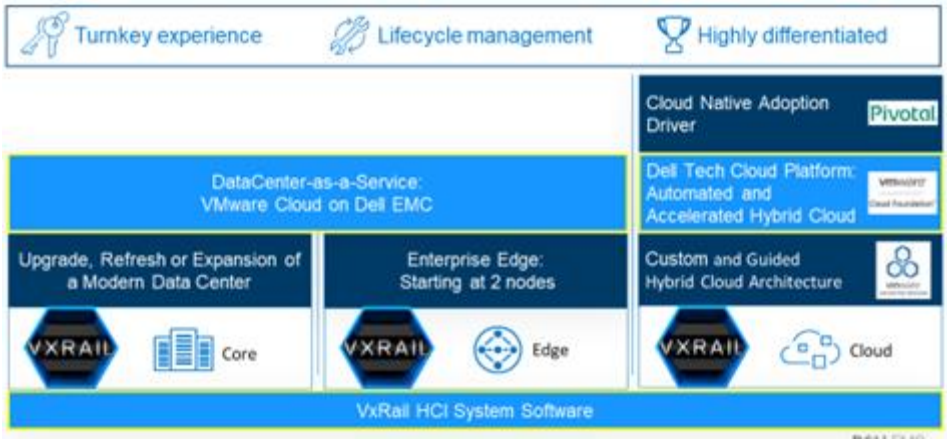


図 1： コアからエッジ、クラウドまで

新たに公開されたリスク ベースのセキュリティ調査『2019 MidYear QuickView Data Breach Report[i]』によれば、公表されたデータ侵害の件数は 2019 年の最初の 6 か月間で 3,800 件を超え、41 億件ものレコードが侵害され、流出していたという調査結果を Forbes が報じています。この数字を踏まえると、侵害の件数は 2018 年に公表された 6,515 件というデータ漏洩事故を上回る可能性があるということです。

デル・テクノロジーズならセキュリティ戦略とモダナイゼーションの取り組みの足並みを揃え、確実にビジネスリスクを軽減できます。

セキュリティ プログラムを総合的なビジネス リスクと一体的に扱うことで負うべきリスクを判断できます。

刻々と変化する脅威のランドスケープにも効果的に対応できるような高度なセキュリティ運用を実装できます。

耐障害性のあるモダン インフラストラクチャを構築してエンドポイント、ネットワーク、アプリケーション、データを守ります。

信頼できるアドバイザリー サービスを活かしてセキュリティ トランスフォーメーション プログラムの設計と実装を支援するデル・テクノロジーズは、独自の立場からあらゆる領域のセキュリティ対策を支援します。

複数のセキュリティ レベルからなる階層型の防御手段が必要ですが、それにはあらゆる要素が連動して機能する必要があります。セキュリティ トランスフォーメーションの第一歩は、セキュリティを考慮して設計、構築された VxRail などのサイバー レジリエンスを備えたモダン インフラストラクチャを導入することです。

昨今進化し続ける脅威のランドスケープによって、そうした脅威を防止、軽減するためのアプローチを変えることが求められています。旧式のインフラストラクチャを守るのは容易いことではなく、複数のベンダーの製品をバラバラに利用することで環境が複雑になり、脆弱性を悪用されるリスクを高めることになります。そうした複雑さを悪意を持って見れば、そこには複数の侵入経路があるということです。

セキュリティの基準とセキュリティ コンプライアンスについても検討が必要です。コンプライアンスに違反した場合、通常は重大な法的処分が下され罰金が科されます。罰金は軽くはありませんが、データ侵害が会社の評判に与える影響と比べれば軽微であるとも考えられます。というのも情報漏洩事故を起こした会社との取引は敬遠される傾向にあるからです。

- Payment Card Industry Data Security Standard（PCI DSS） - クレジット カード所有者の保護
- 一般データ保護規則（GDPR） - 欧州連合が定めるデータ プライバシー規制
- The German Bundesdatenschutzgesetz（BDSG） – 包括的なデータ保護法

- Sarbanes-Oxley Act（SOX） - 上場企業の財務報告に関する機密情報の保護
- Gramm-Leach-Bliley Act（GLBA） - 金融サービス業界における非公知の個人情報（NPPI）の保護
- Health Insurance Portability & Accountability Act（HIPAA） - 患者の電子的な医療データおよび情報の保護
- California Consumer Privacy Act（CCPA） - カリフォルニア州民のプライバシーの権利および消費者保護を強化する法律（2018 年 6 月 28 日制定）

デル・テクノロジーズは、セキュリティ トランスフォーメーションで重要なのは信頼できるパートナーを得ることだと考えています。デジタル リスクの管理を支援し、マネージド セキュリティ サービスや専門技術、インフラストラクチャからアプリケーションまでフル スタックを保護するサービス、ソリューション、製品を提供し、運用の効率化を支え、セキュリティをビジネス戦略にとって不可欠な要素に変える、そのようなパートナーの存在が重要なのです。

デル・テクノロジーズはその信頼できるセキュリティ パートナーとして、ユーザーのセキュリティ トランスフォーメーションを後押しします。エンドポイント、データ センター、開発者、アイデンティティ、セキュリティ運用、クラウドそして仮想化。そのいずれを重視するにしても、セキュリティはエンドツーエンドでなければなりません。デル・テクノロジーズはそうしたニーズに応え、セキュリティやビジネス リスクへの取り組み、セキュリティ侵害への対処、ランサムウェア攻撃による打撃からの回復、安全なアプリケーションの構築を支援します。セキュリティは人によって受け取り方が変わります。良い意味に取る人もいれば、悪い方に考える人もいます。それがどのようなものであれ、デル・テクノロジーズをパートナーとして選んでもらえることが当社の願いです。

デジタルの未来へとつなぐ

今の時代、ビジネスの問題を解決する手段としての IT 利用がかつてなく盛んになっています。データ分析、人工知能、新しいアプリケーション、スマート デバイスの導入という形で IT が利用され、膨大な量のデータが企業によって生成されています。そうしたデータが実用的な情報を生み、競争で優位に立つための独自性の獲得につながります。このようなメリットがあるにもかかわらず、いまだに明確なデジタル ビジョンと戦略を欠く企業は少なくありません。そうした企業では旧式のテクノロジーが制約を生み、変化を拒む企業文化を助長しています。適切に計画を立てなければリスクもセキュリティも後付けで考えることになり、広い視野から戦略的に論じることは到底かないません。このようなテクノロジーの重要な転換点において、受け身の経営姿勢ではもはや立ち行かないのです。イノベーションを加速させデジタルの未来の可能性を拓くには、セキュリティに対する現状把握を根本から変える必要があります。

IT の世界ではセキュリティは好ましい変化を促す存在ではなく、むしろ障害として捉えられます。セキュリティ業務は日常的でありながら感謝されにくい仕事であり、経営陣からは投資しても回収が難しいという目で見られることもあります。セキュリティ業務に携わる人員は高まる脅威や複雑なシステムを管理し、刻々と変化する脅威のランドスケープに対して有効な知識を日々蓄えなければなりません。毎日のようにニュースを賑わすサイバー攻撃の話題はストレスとなり、これまで会社が築き上げてきたものも一瞬で失われるかもしれないという想像に気持ちは滅入る一方です。ですがセキュリティにこのような恐れや不安は無用です。セキュリティはより積極的でプロアクティブであることを常に求めるものであり、そのためには適切なものの見方とテクノロジーが不可欠です。かつて私たちが持っていたセキュリティやリスクに対する考え方を変えることなく保ち続けるのは不可能です。その変化を正しく理解するために、車のブレーキについて考えてみてください。最初はスピードを緩めるだけの装置だと考えるかもしれませんが、実は速く走れるのもブレーキのおかげです。ブレーキがあるからこそ障害物や行く手に備えつつ、自信を持って加速できるのです。企業にとってのセキュリティとリスクも同じです。動きを加速させるものでこそあれ、鈍らせるものではないのです。

Dell EMC 製品のセキュリティ プログラムによる信頼の構築

2002 年、Dell EMC は製品のセキュリティ ポリシーの策定に着手していました。ちょうどストレージ ハードウェア ベンダーを主力とする会社から、エンタープライズ クラスのソフトウェア プロバイダーへと力点を移した頃のことです。その後 2004 年に脆弱性対応プログラムを公開し、2005 年になって全社規模の製品のセキュリティ ポリシーが策定されました。このポリシーには Dell EMC 製品を包括的に取り扱った、幅広く明確なセキュリティ基準が盛り込まれています。策定後も継続的に更新を行い、2007 年には新たなセキュリティ開発ライフサイクル（SDL）に統合されました。SDL では製品開発および導入のあらゆる段階に、測定可能で繰り返し実践できる一連のセキュリティ対策が取り入れられています。2012 年にはサプライ チェーン リスク管理プログラムを正式に開始し、Dell EMC の製品コンポーネントを提供しているサプライヤーにセキュリティ対策を広げています。このように、Dell EMC は今も製品のセキュリティ プログラムを進化させ、最先端の業界標準とプロセスを導入しています。

VxRail でも Dell EMC のセキュリティへの取り組みは健在です。VxRail の開発ライフサイクルは Dell EMC 製品セキュリティの開発プロセスに沿って進められ、セキュリティ開発ライフサイクルがそれを補強します。その Dell EMC セキュリティ開発ライフサイクルでは厳格なアプローチによって製品開発のセキュリティを守り、経営レベルでのリスク管理を行ったうえで製品を市場に投入しています。VxRail ハイパーコンバージド インフラストラクチャの構成要素として重要な位置を占める VMware vSphere も、同様のセキュリティ開発ライフサイクルをもとに開発されています。

セキュア開発ライフサイクル

Dell EMC のセキュア開発ライフサイクル（SDL）は、セキュリティ上の耐久性と一貫性のあるセキュリティ機能を製品に組み込み、公開されたセキュリティ脆弱性に迅速に対応するために必要な、製品のライフサイクル全体にわたる一連のアクティビティが定められています。SDL の基盤になっているのは、業界のベスト プラクティスに沿って製品の R&D 部門によって実施される一連の管理機能です。次の図は SDL の一環として実施される一般的な取り組みの一部を示したものです。

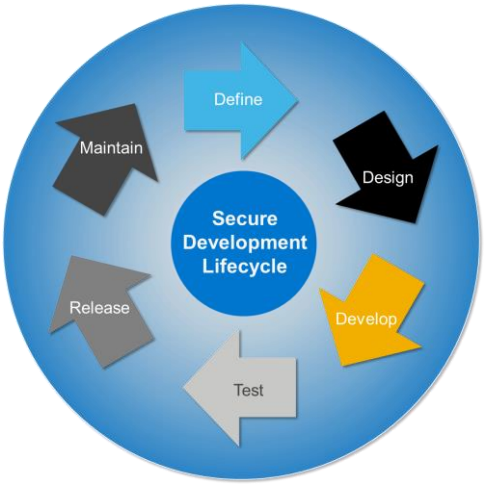


図 2： Dell EMC の SDL の取り組み

セキュリティ担当者は製品の R&D 部門の内部で関係者と密に連携し、製品およびアプリケーションのセキュリティ基準を踏まえて管理業務や検証作業を実施します。次の表は具体的な SDL のアクティビティを、一般的なアジャイル ライフサイクルに対応付けたものです。

Agile Development Activity		SDL Activity
High Level Planning	Requirements	• Formalize security requirements in PRD/PCD • Product Security Training
	Architecture	• **Threat Modeling** • **Security Testing** (test planning)
Sprint 1..*n*	Design	• Update **threat model**
	Develop	• **Static Analysis**
	Test	• **Security Testing**
	Release	• **Security Scanning** • **Security Configuration Guide** • Inventory of Embedded Components
General Availability	Assure	• Perform Code Signing
	Assess	• Finalize and **submit scorecard** • Have a plan for mitigating any "critical" and/or "high" issues
Post-GA	Respond	• Respond to vulnerabilities following EMC's vulnerability response policy

図 3： SDL と一般的なアジャイル ライフサイクルの対応関係

表にあるスコアカードとは Dell EMC のビジネス全体で採用されている仕組みの 1 つで、製品やソリューションが Directed Availability/General Availability（DA/GA）のリリース日を迎えたタイミングのセキュリティ体制を評価するものです。

セキュアな開発

Dell EMC のセキュアな開発に対する包括的なアプローチは、ソフトウェアの脆弱性リスクや製品設計上の欠点を最小限に抑えることに重点を置いています。

このセキュアなソフトウェア開発に対する包括的なアプローチが、ポリシー、スタッフ、プロセス、テクノロジーにまで一貫して採用されています。以下に具体例を紹介します。

- Dell EMC 製品セキュリティ ポリシーは、市場の期待や業界のベスト プラクティスを基準にして製品のセキュリティを評価するために、Dell EMC 製品に携わる企業の共通リファレンスとして使用されています。
- Dell EMC のエンジニアリング チームはセキュリティ意識の高いエンジニアリング コミュニティーを形成しています。すべてのエンジニアがロール ベースのセキュリティ エンジニアリング プログラムに参加して職種特有のセキュリティ ベスト プラクティスの訓練を受け、関連リソースの使用法について知見を深めています。Dell EMC ではこのようにエンジニアリング コミュニティー全体を巻き込んで、セキュリティ意識の高い文化の醸成に努めています。
- Dell EMC の開発プロセスは安全なだけでなく繰り返し実践できるようになっています。SDL は標準的な開発プロセスを補強し、Dell EMC 製品セキュリティ ポリシーに準拠した高度なコンプライアンスを実現します。
- Dell EMC の開発チームはクラス最高のセキュリティ テクノロジーを開発基盤に持ち、最先端のテクノロジーを駆使してソフトウェア セキュリティの共通の要素（認証、許可、監査、アカウンタビリティ、暗号、キー管理など）として使用されるソフトウェア一式や標準規格、仕様、設計を開発してきました。必要に応じてオープン インターフェイスを使用し、既存のお客様環境におけるセキュリティ アーキテクチャとの統合を可能にしています。

- Dell EMC の SDL は標準的な開発プロセスをセキュリティで補強し、Dell EMC 製品セキュリティ ポリシーに準拠した高度なコンプライアンスを実現します。Dell EMC の SDL では厳格なアプローチによって製品開発のセキュリティを守り、経営レベルでのリスク管理を行ったうえで製品を市場に投入しています。
- SDL はセキュアな設計基準に組み込まれている幅広い集合的プロセスの一要素です。このセキュアな設計基準は Dell EMC 製品のセキュリティを構築するうえでのベンチマークとなるものであり、すべての製品の機能のセキュリティに関わっています。この基準には必須のセキュリティ機能についても説明があり、お客様に提供される Dell EMC 製品には必ずその機能を実装することになっています。こうした基準を設けることで、Dell EMC 製品には次のような強みがあります。
  - 厳格なセキュリティ要件を持つお客様への対応
  - PCI や HIPPA などの規制条件への適合支援
  - Dell EMC 製品やお客様環境に対するセキュリティ脆弱性のリスクを最小限に抑制
  - ソース コードの保護機能により、ソース コードや製品関連の知的財産を含む Dell EMC エンジニアリング システムの適切な保護方法を把握し、お客様環境に導入されている製品の整合性を保証

Dell EMC における脆弱性対応

システム コンポーネントにセキュリティ脆弱性が存在した場合、そこから侵入を受けて IT インフラストラクチャ全体を侵害される可能性があります。脆弱性が初めて発見された瞬間から修正プログラムが提供されるまでの間は、攻撃する側とそれを防ぐ側との競争です。Dell EMC が最優先で取り組んでいるのは、この発見から対策までの時間をできる限り短くし、リスクを減らすことです。

Dell 製品セキュリティ インシデント対応チーム（PSIRT）は社外で発見された Dell EMC 製品のあらゆる脆弱性に対処し、情報公開の段取りをつける役割を担っています。PSIRT は脆弱性による脅威への対処に必要な情報やガイダンス、被害を軽減するための戦略を適宜お客様に提供します。

製品のセキュリティの潜在的な欠陥に関する情報は、Dell の Web サイトや電子メールを利用してどなたでもお寄せいただくことができます。ご提供いただいたすべての情報は調査から検証、修復、調査報告に至るまで業界のガイドラインに沿って実施されます。

Dell は製品の脆弱性に関するすべてのお客様にリアルタイムでお届けします。当社からのお知らせを通じて脆弱性の重大度を明確にするとともに、標準化されたレポート システムを複数併用して同情報を配信します。すべての Dell 製品のセキュリティ対策と同様に、当社の情報公開に関するポリシーも業界のベスト プラクティスを基に策定されています。

サプライ チェーン リスク管理

成果が期待できる製品セキュリティ プログラムとは、包括的であり、アウトソーシングによって調達したコンポーネントやソフトウェアにも適用されるものです。信頼を築き維持していくにはサプライ チェーンの中で整合性テストを実施することが不可欠です。デル・テクノロジーズには公式のサプライ チェーン リスク管理プログラムがあり、これによって社内製品で使用されるハードウェア コンポーネントが適切かつ入念な検査を経て調達されたものであることが確かめられています。

サプライ チェーンのセキュリティを決定付けるのは、物的資産、在庫管理、情報、知的財産、人材を保護する予防的および発見的コントロール手段の実践と応用です。サプライ チェーンにマルウェアや偽物のコンポーネントが紛れ込む可能性を減らすことで情報セキュリティや物的、人的なセキュリティに対処することが、確実なサプライ チェーンの提供を支えます。

Dell のサプライ チェーン リスク管理フレームワーク（次の図）には National Infrastructure Protection Plan（NIPP）の包括的なリスク管理フレームワークが反映されています。このフレームワークは、米国政府と民間部門の協働によっていかにリスクを軽減し、セキュリティ目標を達成するかがまとめられています。Dell のフレームワークは開かれたフィードバック ループを取り入れることで継続的な改善を可能にしています。リスク軽減計画の優先順位付けと実施は、ソリューションのライフサイクル全体を通じて妥当性のある適切なものになります。以下にサプライ チェーン リスク管理プロセスを図で示します。

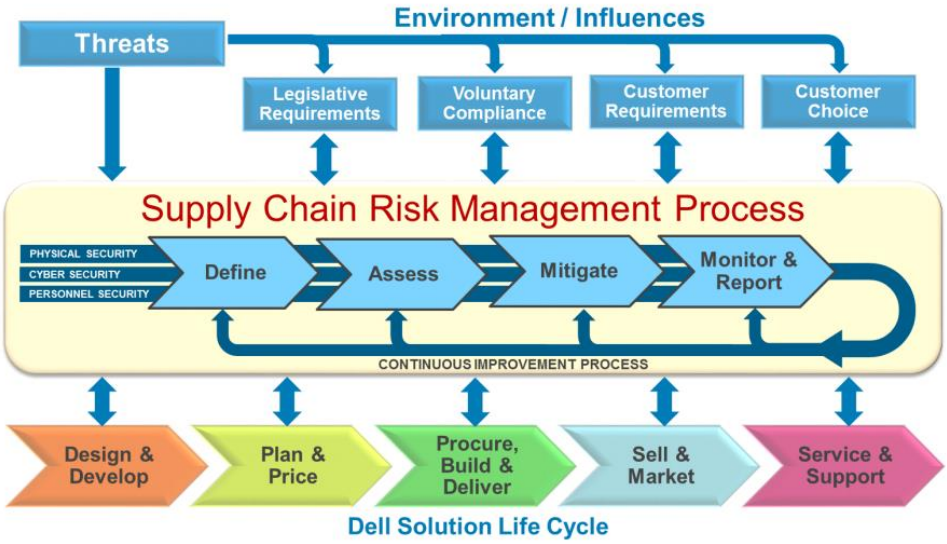


図 4： Dell のサプライ チェーン リスク管理プロセス

製品セキュリティを向上させる業界コラボレーション

セキュリティ上の脅威は絶え間なく現れては、密につながりあう今日のシステム環境を通じて瞬く間に社内に広がっていきます。その脅威に対処するには、他社との協業によるアプローチが最も効率的で効果的であるとデル・テクノロジーズは考えます。

リスクが高まっている現状を考慮するならば、こと製品のセキュリティに関してテクノロジー プロバイダーは市場での競争目標は脇に置くべきです。IT 製品のあらゆるセキュリティの問題を単独で解決しうるベンダーは存在しません。IT セキュリティとは共同での協調的な営為なのです。IT という市場が誰もが成功を収められる場所であり続けるためには、他社との協業が不可欠だというのがデル・テクノロジーズの考えです。

製品セキュリティとともに歩んだ数十年がデル・テクノロジーズの発展を支え、豊かな知見の礎となりました。そして今、そこから得たものをお客様や同業他社、パートナー企業と分かち合っています。もちろんお客様の IT システムはデル・テクノロジーズの製品だけで成り立っているわけではありません。そこで当社は製品が稼働しているエコシステムのセキュリティを向上させることに力を尽くします。つまり積極的な参加によって IT 業界全体に建設的に貢献するということです。

長年にわたって製品のセキュリティを高めるべく取り組んできた立場から、業界への新規参入者を支援し、後押しする責任も生まれました。デル・テクノロジーズの製品セキュリティを束ねるリーダーたちは会議での発言やブログ投稿のほか、公的な交流の場で自由な意見の交換を促しています。

業界の製品セキュリティ グループへの参加

デル・テクノロジーズは製品セキュリティを扱う複数のグループに参加しています。少しずつ進化しているベスト プラクティスを活動の中で学び、時に教えることで知見を深め、製品セキュリティに対する共同責任の感覚を養っています。当社が参加している業界団体は次のとおりです。

- **BSIMM** — Building Security in Maturity Model は業界のソフトウェア セキュリティに対する取り組みを評価するもので、企業向けにセキュリティ対策の現状と展望を提供しています。

- **The Open Group** — 400 を超える企業や組織の会員からなるコンソーシアムで、IT 担当者、製品、サービスを対象とした認定プログラムを運営し、IT に関わる標準化、向上に貢献しています。The Open Group は現在ある、および表面化しつつある IT の要件を把握し、それに適合するために必要なベスト プラクティスを確立ないし共有するべく活動しています。

- **SAFECode** — Dell EMC が共同設立に加わった SAFECode こと The Software Assurance Forum for Excellence in Code は、より安全で信頼できるソフトウェア、ハードウェア、サービスの提供に効果的なベスト プラクティスを見つけ、奨励するという業界の主導による取り組みです。

- **CSA** — The Cloud Security Alliance はベスト プラクティスの策定と意識向上を主とし、安全なクラウド コンピューティング環境の実現に貢献している世界有数の組織です。

- **FIRST** — The Forum of Incident Response and Security Teams はインシデント対応の分野で知られるグローバル リーダーです。DELL PSIRT は FIRST VxRail チームに参加しています。

VxRail：データ センターのモダナイゼーションと IT トランスフォーメーションの基盤

VxRail には絶えず進化を続けるセキュリティ上の脅威のランドスケープとの競争に勝利するために必要な、現在および将来の脅威に対抗できる適応力があります。最新世代の Dell PowerEdge サーバーと最新のプロセッサー テクノロジーをベースに構築された VxRail はセキュリティの高いプラットフォームで、柔軟な構成オプションも用意されています。vSphere によってストレージとサーバーが仮想化され、ワークロードに対する要件の高度化に応じて容易に拡張できます。規制の内容が変わっても VxRail なら柔軟な構成オプションを利用して速やかに適応できます。

VxRail はどのような産業分野にでも応用が利き、サイバー レジリエンスを最適化し、リスクを管理し、コンプライアンス要件を満たすことができます。VxRail は VMware vSAN を構成要素に持ち、完全に統合された唯一の事前構成済みかつテスト済みのハイパーコンバージド インフラストラクチャであり、導入場所を選びません。データ センターやエッジ、あるいはハイブリッド クラウド ソリューションの一部に組み込んでも、ビジネスクリティカルなアプリケーションや VDI、リモート インフラストラクチャの提供を一層シンプルでセキュアな優れたものにしてくれます。Dell EMC は、サイバー レジリエンスを最適化して導入環境全体をカバーするために必要な機能を、VxRail を通じてお客様に提供することができます。VxRail には次の図に示すようなセキュリティが組み込まれています。

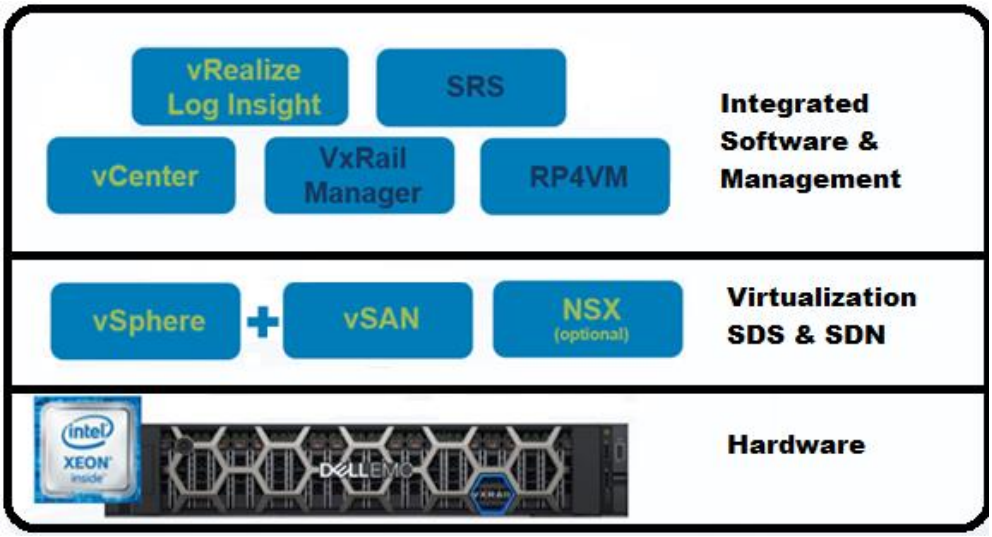


図 5： VxRail に組み込まれているセキュリティ

Dell EMC PowerEdge サーバー

VxRail は Dell PowerEdge サーバー プラットフォームを基盤にハードウェアおよびシステムレベルでのセキュリティ機能が実装されており、階層的な防御構造でインフラストラクチャを保護します。速やかに侵入を検知することでシステムを信頼できるベースラインに復旧させることができます。PowerEdge サーバーには次のような独自のセキュリティ機能が実装されています。

- システム ロックダウン機能が不慮や不正による変更を防止します。セキュリティの脆弱性を生じ機密データの流出につながるような構成上の変更を防ぐ、業界初の機能です。
- UEFI セキュア ブート、BIOS リカバリー機能、署名されたファームウェアなどの機能を備えたサイバーレジリエント アーキテクチャが攻撃に対する保護を強化します。
- サーバーの廃棄時にはサーバー レベルでの System Erase 機能で、ドライブからも不揮発性メモリーからもすべてのユーザー データを迅速かつ安全に消去でき、プライバシーを保護できます。

Dell EMC PowerEdge サーバーは VxRail クラスター内のノードを構成する極めて重要なハードウェアです。各ノードの CPU、メモリー、ディスク リソースはクラスターの資源としてプールされ、ネットワーク インターフェイスを介して接続されます。そのためセキュアな Dell EMC PowerEdge サーバーが VxRail セキュリティの基盤となっています。

PowerEdge サーバーには iDRAC と呼ばれる統合リモート アクセス コントローラーが用意されています。iDRAC を利用するとセキュアな通信、認証、ロールベースのアクセス制御によってリモートから物理システムを安全に管理、構成できます。アラートの設定を利用すれば、ハードウェアにアクセスを受けるか構成変更が発生するたびに iDRAC から Security Incident and Event Management（SIEM）システムにイベント情報を送信できます。こうした仕組みによって不正な変更を検知、報告することで VxRail の完全性を保つことができます。詳細については、『Cyber Resilient Security in 14th Generation of Dell EMC PowerEdge』を参照してください。

PowerEdge サーバーは暗号化形式で署名され検証されたファームウェアを利用することで信頼できるシステムを構築しています。つまりハードウェアと一体化したセキュリティ テクノロジーを活用しているということです。たとえば Intel 社の Trusted Execution Technology（TXT）のような機能によってサーバーが意図したバージョンのファームウェア、BIOS、ハイパーバイザーだけが実行されていることを確認し、検出を免れたマルウェアが紛れ込むのを防止しています。次の図はハードウェアの信頼の起点を示したものです。

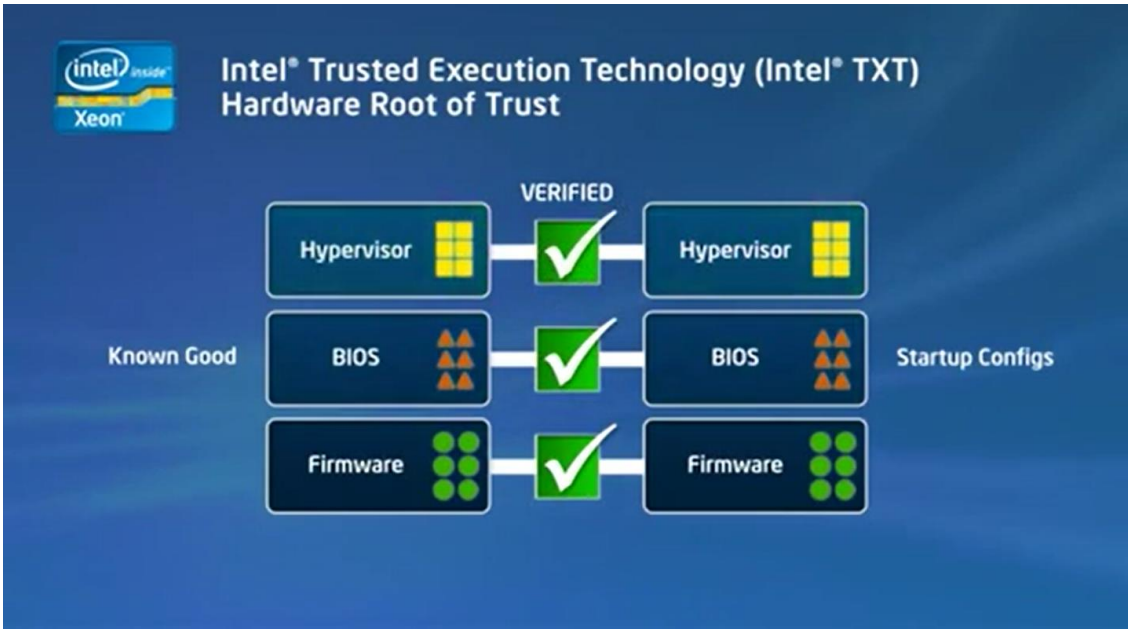


図 6： ハードウェアの信頼の起点

VxRail では Trusted Platform Management（TPM）モジュール（TPM バージョン 1.2 およびバージョン 2.0）を使用してノードを構成することで、サーバーの整合性をさらに高いレベルで保護できるというオプションがあります。TPM とはセキュアな暗号プロセッサーの国際標準で、暗号キーのセキュリティ強化を目的に設計された専用のマイクロコントローラーです。すべての VxRail ノードに任意で使用できます。

Dell EMC VxRail HCI システム ソフトウェア

VxRail の機能に独自性を与えている価値は、VxRail HCI システム ソフトウェアという基盤から生まれたものです。インフラストラクチャ スタックの観点から見れば、管理ソフトウェアは VMware ソフトウェアと PowerEdge サーバー上で実行され、VxRail を単一の統合システムとして機能することを可能にしています。

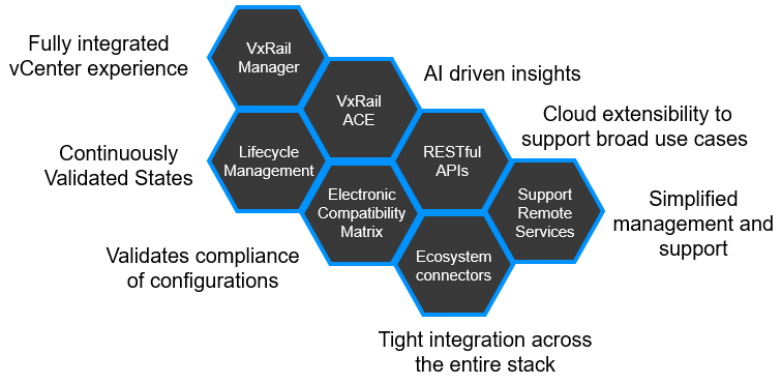


図 7： VxRail HCI システム ソフトウェア

継続的に検証された状態 — VxRail は、VMware ソフトウェアや PowerEdge サーバー コンポーネントを始めとする VxRail スタック全体との相性が事前にテストされ、検証済みのソフトウェアおよびファームウェア上で実行されます。VxRail のライフサイクル管理機能のおかげで、VxRail クラスターはライフサイクルの初めから終わりまで既知の正常な状態で稼働し続けるという安定性と、継続的な変更によって VMware ソフトウェアの最新の革新的機能やセキュリティ修正プログラム、バグ修正を利用するという柔軟性を両立しています。「継続的に検証された状態」という言葉は、VxRail クラスターの核である構成の安定性を表しています。

電子互換性マトリックス — ユーザーが VMware の互換性マトリックスから望ましいと判断した状態が、「継続的に検証された状態」として検証済みの状態になるように、VxRail チームは継続的にスタック内のさまざまなソフトウェアおよびハードウェア コンポーネントをすべて取り上げてスタック全体をテストし、正常性を確認することに取り組んでいます。また、VxRail はクラスターの構成に違反がないことをこのマトリックスを参照して確認します。こうしたメリットによりお客様の負担となるテスト作業およびリソースの投資が大幅に軽減されると同時に、アプリケーション ワークロードに影響を与えることなく想定どおりに安全に VxRail クラスターを進化させられるという安心感を与えます。

エコシステム コネクター — 広範囲に及ぶ電子互換性マトリックスを構築するには、VxRail とスタック内のエコシステムの構成要素である vSphere、vSAN、vCenter、PowerEdge サーバー、それらに搭載された複数のハードウェア コンポーネントと通信ができる必要があります。コネクターには VxRail が各コンポーネントで実行されているソフトウェア/ファームウェアのバージョンを把握し、それらのコンポーネントのライフサイクルを管理できるようにする役割があります。さらにオートメーションとオーケストレーションの機能が、VxRail をひとつの統合システムとして管理できるようにしています。

VxRail Manager — VxRail の主な管理ユーザー インターフェイスは、VxRail Manager と呼ばれる vCenter プラグインです。VxRail ユーザーはこのインターフェイスを介してさまざまな VxRail での作業を実行できます。具体的には初回のクラスター構成、ハードウェア コンポーネントの監視、クラスターの正常なシャットダウンの実行、ノードの追加によるクラスターの拡張、VxRail HCI システム ソフトウェアの更新などです。これによって完全に統合された vCenter の使用感を得られます。

VxRail Manager FIPS 140-2 レベル 1 — FIPS 140-2 レベル 1 コンプライアンスの一環として、VxRail 7.0.010 のリリースで VxRail Manager 仮想アプライアンスに次のアップデートが加えられました。

- VxRail Manager - VxRail Manager に転送中データを保護する FIPS 適合済みの暗号化モジュールを実装
- VxRail Manager - VxRail Manager OS での FIPS モードの有効化

- VxRail Manager – FIPS 証明書アルゴリズムで暗号化されたストレージのキーと認証情報を使用したロックボックス

SaaS マルチクラスター管理 — VxRail のライフサイクル管理を向上させる機能拡張が行われると、その多くは SaaS マルチクラスター管理におけるグローバル オーケストレーションの分析コンピューティング機能に依存します。HCI システム ソフトウェアによって収集された VxRail クラスターに関する高度なテレメトリーを通じて、SaaS マルチクラスター管理による人工知能を利用した分析情報が提供されます。ユーザーはこの情報を活用してプロアクティブにクラスターを管理し、パフォーマンスと可用性を向上させることができます。人工知能を利用した分析情報はよりアクティブなマルチクラスター管理機能の発展も促します。この分野は HCI 環境の普及に伴って大規模な管理が欠かせなくなれば、ますます HCI ユーザーの関心を集めていくことになると予想されます。

REST API — VxRail のライフサイクル管理にはユーザーに選ばれるインフラストラクチャ プラットフォームとして理想的なメリットがあります。IT 運用をシンプルにすることに重点を置いているというのがそれで、IT チームがクラウドベースの IT サービス提供モデルに注力するうえで重要な役割を果たしています。API を介して VxRail プラットフォームを拡張できるため、サービスとしてのインフラストラクチャ ソリューションを基盤に構築できます。API は大規模な管理にも都合がよく、いくつもの VxRail クラスターをさまざまな拠点に展開し、スクリプト化した内製ソリューションで大規模な管理を行っているお客様にとってメリットがあります。

リモート サービスのサポート — サポート体制も適切な HCI ソリューションを選択する際の重要な要素になります。VxRail では Dell テクニカル サポートによる単独ベンダーでのサポートを VMware ソフトウェア、PowerEdge サーバー、VxRail ソフトウェアに対して提供します。VxRail のサポートには Dell EMC Secure Remote Services によるオートコールや、ライフサイクル プロセスの全体を通じてリモートでの監視、診断、修復に対応するプロアクティブな双方向のリモート接続があり、最大限の可用性を確保できます。

VMware vSphere

VMware vSphere ソフトウェア スイートは VxRail に高可用性、耐障害性、オンデマンドの仮想化インフラストラクチャを提供します。ESXi、vSAN、vCenter Server が vSphere のコア コンポーネントです。ESXi は工場の段階で物理的な VxRail サーバー ノードにインストールされるハイパーバイザーで、その機能によって単一の物理サーバーに複数の論理サーバーないし VM をホストすることができます。vSAN は VM によって使用されるソフトウェアデファインド ストレージ、VMware vCenter Server は ESXi ホスト、vSAN、VM の管理アプリケーションです。

VM 上で実行中のアプリケーションを保護するために使用されるのが AppDefense です。AppDefense はアプリケーションおよびマシンの意図した状態と挙動を把握して脅威を検出し、防止する手段として機械学習を活用し、vSphere で実行されているアプリケーションの整合性を保護しています（vSphere Enterprise-Plus が実行されている VxRail）。

Dell EMC と同様に、VMware でも厳格なセキュア ソフトウェア開発ライフサイクルが守られており、Security Response Center による管理体制もあります。VMware との共同開発で生まれた VxRail はサポートでも VMware の支援を受けることができ、ソリューションに実装されるあらゆるコンポーネントの設計、構築、テスト、導入においてセキュリティが最優先として扱われています。詳細については、「VMware 製品セキュリティ」を参照してください。

VMware vCenter Server

vCenter Server はサーバー仮想化と vSAN ストレージのどちらにとっても重要な管理拠点となります。1 つの vCenter インスタンスをエンタープライズ レベルに拡張すれば、数百の VxRail ノードと数千の VM をサポートできます。VxRail は VxRail クラスター内に導入されている vCenter インスタンスを使用するか、既存の vCenter インスタンスを使用できます。

vCenter を利用すればデータセンター、クラスター、ホストを論理的に階層化できます。これによってユース ケースや基幹ビジネスごとにリソースをセグメント化し、必要に応じてリソースを動的に移動させることができます。この操作は単一のインターフェイスから直感的に実行できます。

vCenter Server はインベントリ サービス、タスクのスケジュール設定、統計情報のログ、アラームおよびイベントの管理、VM のプロビジョニングおよび構成などの VM サービスとリソース サービスを提供します。vCenter Server には次のような先進的な可用性機能もあります。

- **vSphere vMotion** — ダウンタイムが生じないライブ VM ワークロード移行を実現します。
- **vSphere Distributed Resource Scheduler（DRS）** — クラスター内のノード間で常に負荷の平衡が取れるように VM コンピューティング リソースを割り当て、最適化します。
- **vSphere High Availability（HA）** — VM のフェールオーバーと再開機能を提供します。

VMware ESXi ハイパーバイザー

VxRail では、ESXi ハイパーバイザーによってクラスター ノードに VM がホストされます。VM は安全で可搬性があり、それぞれがプロセッサー、メモリー、ネットワーク、ストレージ、BIOS を搭載した独立したシステムです。VM 同士は隔離されているため、VM で実行されているゲスト オペレーティング システムに障害が発生しても同じ物理ホスト上の他の VM は影響を受けずに実行をし続けることができます。VM は CPU へのアクセスを共有しています。ESXi は CPU のスケジュール設定を担当するほか、VM に利用可能なメモリーの領域を割り当て、物理ホストに関連付けられている物理ネットワーク カードとディスク コントローラーへの共有アクセスを管理します。X86 ベースのオペレーティング システムであればすべてサポート対象となり、同じ物理サーバー ハードウェア上の VM で異なるオペレーティング システムとアプリケーションを実行できます。

VMware の仮想ネットワーキング

ネットワーク トラフィックの分離は基本的なセキュリティ要件です。VxRail においては vSphere の仮想ネットワーク機能が柔軟な接続および分離を可能にしています。VxRail の VM は、VMware Virtual Distributed Switch（VDS）を利用することで相互通信を行います。VDS は同じクラスター内の複数のノードにまたがる単一の論理スイッチとして機能します。VDS は標準のネットワーク プロトコルと VLAN の実装を使用し、データリンク層でフレームを転送します。

vCenter Server を使用してデータセンター レベルで構成され、VM を複数のホストに移行しても安全で一貫性のあるネットワーク構成を維持できます。VxRail はその内部ネットワーク トラフィックを VDS に依存し、vSAN もそれ自体のネットワーク アクセスを VDS に依存しています。

また VxRail は、NSX と組み合わせることでソフトウェア デファインド型のネットワーク セキュリティを実現し、マイクロセグメンテーションによる粒度の高いアクセス制御が可能です。

VMware vSAN

vSAN は vSphere クラスター内のホストに接続されているローカル ディスクを集約して、分散共有ストレージのプールを作成します。容量のスケールアップはクラスターへのディスク追加で、スケールアウトは VxRail ノードの追加によって行います。vSAN は vSphere と完全に統合されているため、vSphere の他の機能ともシームレスに連動します。

vSAN で特筆すべきはその効率性とパフォーマンスです。ワークロード、使用率、リソースの空き状況を基に割り当ての自己最適化とバランス調整を行います。vSAN はパフォーマンスに優れフラッシュに最適化された HCI を提供し、多様なワークロードに対応できます。エンタープライズ クラスのストレージ機能には次のものがあります。

- 重複排除、圧縮、消失訂正符号などの効率的なデータ削減テクノロジー
- ユーザー定義の制限に基づいてワークロードの使用を制御する QoS ポリシー
- ソフトウェア チェックサム、フォールト ドメインなどのデータの整合性とデータ保護のテクノロジー
- vSAN の静止データ暗号化によるセキュリティの強化

vSAN では各 VxRail ノード上のディスクは、キャッシュ ドライブ 1 台と、1 台以上の容量ドライブが割り当てられた複数のディスク グループに自動編成されます。これらのディスク グループから単一の vSAN データストアが形成され、VxRail クラスター内のすべてのノードからアクセスできるようになっています。

VxRail には 2 種類の vSAN ノード ストレージ構成オプションが用意されています。1 つはフラッシュ SSD とメカニカル HDD を併用するハイブリッド構成、もう 1 つはオールフラッシュ SSD 構成です。ハイブリッド構成ではキャッシュ用としてフラッシュ SSD を、容量ドライブおよび永続データ ストレージとしてメカニカル HDD を使用します。一方オールフラッシュ構成ではキャッシュと容量ドライブの両方にフラッシュ SSD を使用します。次の図に vSAN の基本概念を示します。

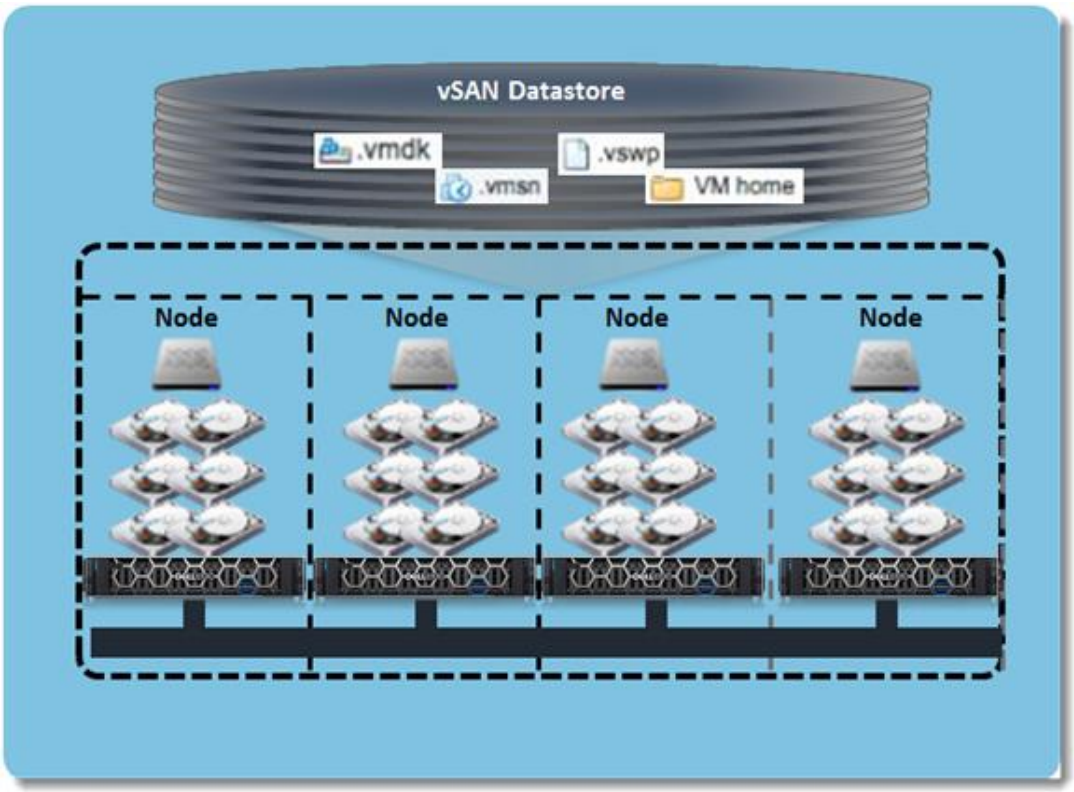


図 8： vSAN の基本概念

vSAN は VxRail クラスターが最初に初期化されるときに構成され、その後 vCenter を介して管理されます。VxRail の初期化プロセス中に vSAN は各 ESXi ノードにローカル接続されたディスクを基に分散共有データストアを作成します。データストアのストレージ容量は、クラスター内の全容量ドライブを合計した量になります。使用できるストレージ容量は適用されている保護レベルによって異なります。システム初期化の一環で構成と検証が行われたオーケストレーション済みの vSAN によって、一貫性のある予測可能なパフォーマンスとベスト プラクティスを踏襲したシステム構成が実現します。

vSAN セキュア ディスク ワイプ

vSAN セキュア ディスク ワイプは vSAN 環境で使用したディスクを安全に廃棄ないし流用するための機能で、NIST 標準規格に準拠しています。この機能を使用するには、vSAN のディスク グループからドライブを解除する必要があります。この機能は 1 つまたは複数のディスクに対して同時に実行できますが、磁気ディスクはサポート対象外です（フラッシュおよび NVMe のみ対象）。

ストレージ ポリシーベースの管理（SPBM）

vSAN はポリシー駆動型の仕組みを持ち、ストレージのプロビジョニングと管理をシンプルにすることを目標に設計されています。vSAN ストレージ ポリシーは VM のストレージ要件を定義するルール セットが基盤となっています。管理者は VM ストレージ ポリシーを必要に応じて柔軟に変更できます。SPBM ルールの例としては、許容する障害の数、使用するデータ保護技法、ストレージレベルのチェックサムの可否などがあります。

VMware vRealize Log Insight

VxRail にバンドルされている VMware vRealize Log Insight はシステム イベントを監視して、仮想環境とハードウェアの状態に関する進行形の総合的な通知を可能にします。ログ監視、インテリジェントなグループ化、分析機能を備えた VxRail のリアルタイムの自動ログ管理によって、VxRail の物理、仮想、クラウドの各環境にまたがる大規模なトラブルシューティングをシンプルにします。ログの一元化はインフラストラクチャが安全であるための基本的な要件です。ログ機能や SIEM を導入済みのお客様についても、VxRail なら業界標準の Syslog プロトコルを使用して簡単に統合できます。

VMware Cloud Foundation（および NSX）

VMware Cloud Foundation on VxRail は Dell EMC と VMware の共同設計による統合ソリューションで、ソフトウェアデファインド データセンター（SDDC）の運用を、Day 0 から Day 2 の段階に至るまで全面的にシンプルで効率的に変え、自動化する機能を備えています。この新しいプラットフォームは、プライベートとパブリックの両方の環境において、コンピューティング（vSphere および vCenter を使用）、ストレージ（vSAN を使用）、ネットワーキング（NSX を使用）、セキュリティ、クラウド管理（vRealize Suite を使用）向けの一連のソフトウェアデファインド サービスを提供し、ハイブリッド クラウド用の運用ハブにします。

VMware Cloud Foundation on VxRail はネイティブの VxRail ハードウェアおよびソフトウェアの機能と VxRail の他の独自の統合（vCenter プラグインや Dell EMC のネットワーキングなど）を活用する完全に統合されたハイブリッド クラウド プラットフォームによって、最もシンプルにハイブリッド クラウドを導入する手段となります。これらのコンポーネントが連携することで、フルスタック統合によるターンキー ハイブリッド クラウドの新しいユーザー エクスペリエンスを提供します。フルスタック統合とは、HCI インフラストラクチャ レイヤーとクラウド ソフトウェア スタックの両方を、ライフサイクルが自動化された完全なターンキー エクスペリエンス 1 つで手に入れられることを意味します。

VMware NSX Data Center は仮想クラウド ネットワークを実現するネットワーク仮想化とセキュリティのためのプラットフォームであり、ソフトウェアデファインドの手法によるネットワーキングをデータ センター、クラウド、エンドポイント、エッジにまで横断的に広げたものです。NSX データ センターではスイッチング、ルーティング、ファイアウォール、ロード バランシングなどのネットワーク機能がアプリケーションの近くにあり、環境全体に分散しています。VM の運用モデルと同様にネットワークをプロビジョニングし、基盤となるハードウェアとは別に管理できます。

NSX データ センターはソフトウェア上でネットワーク モデル全体を再現し、単純なネットワークから複雑な複数階層型ネットワークまで、あらゆるネットワーク トポロジーに対応できます。しかも作成、プロビジョニングにかかる時間はわずか数秒です。ユーザーはさまざまな要件を持つ複数の仮想ネットワークを作成できます。その際に NSX のサービスに含まれるマイクロセグメンテーションや次世代のファイアウォールからパフォーマンス管理ソリューションまで多岐にわたるサード パーティー統合のエコシステムを組み合わせて利用し、本質的により機敏で安全性の高い環境を構築できます。こうして組み込まれたサービスはクラウド内およびクラウドをまたいで多くのエンドポイントに適用できます。詳細については、『VMware Cloud Foundation on VxRail Architecture Guide』を参照してください。

VxRail のセキュリティ機能

セキュリティに関する機能は、データ セキュリティとシステム セキュリティの 2 つに分けることができます。これから説明する VxRail の安全なシステム構成と管理は、機密性-整合性-可用性（CIA）の 3 原則に基づいています。

VxRail はすべてのセキュリティ機能について事前構成済みかつテスト済みのスタックを提供します。これらのセキュリティ機能は統合により VxRail に組み込まれています。

データ セキュリティ

許可されたアカウントまたは特定のアカウントだけがデータを利用できること、またコンプライアンスを満たし仕様に適合することを確実にするために、データ セキュリティは CIA の 3 原則に基づいて構築されています。これはデータへの物理的なアクセスとユーザー レベルでのアクセス両方の視点が対象となります。

機密性

機密情報が意図しないユーザーにアクセスされるのを防ぎつつ、許可がありそれが適切な場合には会社のデータにアクセスできるようすることは、機密性やプライバシーと呼ばれる根本的な問題です。VxRail は使用中データ、移動中データ、静止データの機密性の問題に対処します。

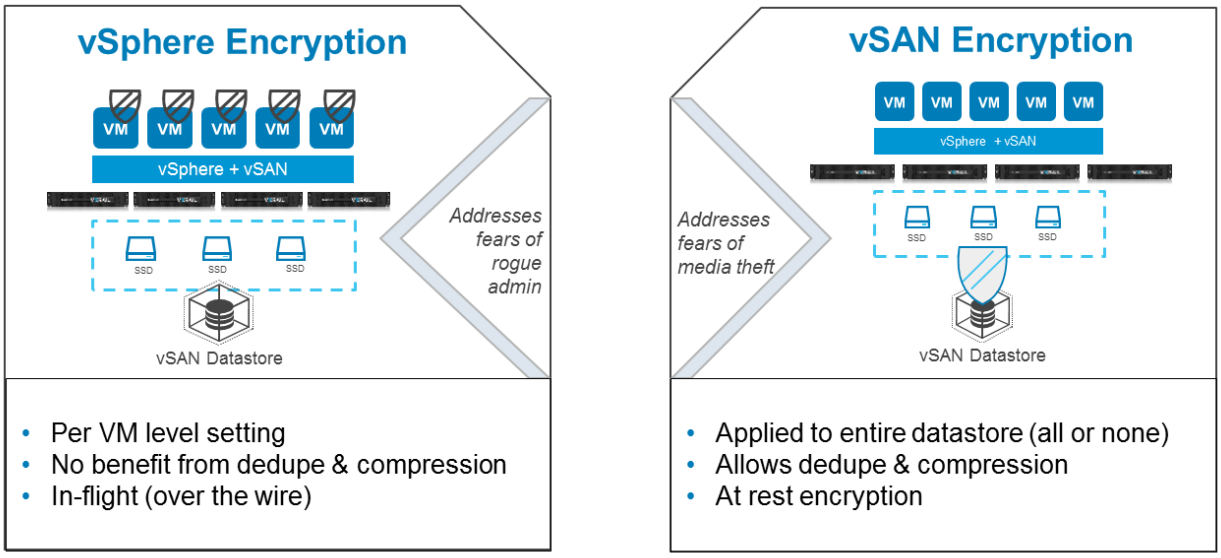
暗号

暗号化は許可されていない相手にデータが渡っても中身を読み取られないようにすることで情報の機密性を守る技術です。VxRail では vSAN の静止データ暗号化（D@RE）によってデータストアを暗号化できます。これにより FIPS 140-2 に適合したデータ保護が可能です。vSAN 暗号化が D@RE で保護するのはワークロードだけではありません。vCenter（同一クラスターでホストされている場合）や VxRail Manager も保護対象となります。個々の VM は vSphere 暗号化によって、動作中の VM は vMotion 暗号化によってそれぞれ暗号化されます。こうした暗号化に加えて、アプリケーションの要件に応じて暗号化レベルを高く構成することもできます。

vSAN 暗号化は単一の設定で vSAN データストア全体が暗号化されるため、静止データを暗号化するには最もシンプルかつ柔軟に利用できる方法です。この暗号化はデータストアを使用するすべての VM を対象に、クラスター全体に適用されます。通常、暗号化されたデータに対しては、重複排除や圧縮などの空き容量削減技法を使用することで得られるメリットはありません。しかし vSAN では重複排除と圧縮が行われた後に暗号化が実行されるため、そうした技法のメリットを損なうことなく享受できます。

VM 暗号化には VM 単位で暗号化できる柔軟性があります。つまり、1 つのクラスターに暗号化された VM とそうでない VM が混在する場合があるということです。VM 暗号化は VM に追従し、ホストされる場所には影響を受けません。したがって VM が VxRail 外のデータストアに移動されても、その VM の暗号化はそのまま維持されます。

また、VM の暗号化の有無は切り替えられますが、暗号化されている VM を vSphere vMotion を使用して移行する場合、必ず暗号化された vSphere vMotion が使用されます。暗号化されていない VM の移行で vMotion を使用する場合は、「無効」、「便宜的」、「必須」の暗号化オプションから選択できます。暗号化されていない VM で vMotion を使用する場合のデフォルトには、「便宜的」オプションが適用されます。次の図は、VM 暗号化と vSAN 暗号化の違いをまとめたものです。



Both require use of a supported external key management server (KMS)

図 9： VM 暗号化と vSAN 暗号化の違い

VxRail は暗号化されている VM のホスト間移動における、暗号化された vMotion をサポートします。同じ VxRail 内での vMotion 移行だけでなく、vCenter インスタンス内の VxRail クラスター間での vMotion 移行も対象となります。暗号化された vMotion は、vSAN 暗号化と併用して静止データ暗号化と転送データ暗号化の両方に対応できます。暗号化された vMotion は、vSphere 暗号化が有効になっている VM に対して適用されます。

移動中データの暗号化で使用される一時キーが vSphere から提供される場合、暗号化キーの安全な生成、保管、配信にはキー管理サーバー（KMS）が必要です。ただし vMotion 暗号化が使用される場合はこの限りではありません。暗号化が有効になっている場合、vCenter は KMS との信頼関係が確立されてから KMS の接続情報を ESXi ホストに渡します。情報を受け取った ESXi ホストは暗号化キーを KMS に直接要求し、データの暗号化と復号を実行します。初期セットアップのときにだけ vCenter との接続が必要です。

KMS はセキュリティ インフラストラクチャの核となる重要なコンポーネントであるため、通常は DNS や NTP、Active Directory などの他の重要なインフラストラクチャ コンポーネントに適用されるのと同等の冗長性と保護が必要です。留意点として、KMS は暗号化の対象となる要素とは物理的に離しておく必要があります。起動中に ESXi ホストは KMS からキーを要求します。KMS を使用できない場合はシステムを起動できません。

VxRail および VMware は、Key Management Interoperability Protocol（KMIP）v1.1 以降に対応する Dell EMC CloudLink などの KMS をサポートしています。VMware では vSphere で検証済みの KMS に関する互換性ガイドを整備しています。

vSphere 内では FIPS 140-2 で検証済みの共通モジュール セットによって暗号化が処理されます。これらの共通モジュールは VMware セキュア開発ライフサイクルによって設計、実装、検証されます。暗号化用の共通モジュールのセットを使用することで、VxRail での暗号化の実装、管理、サポートを容易にしています。

VxRail での暗号化は、vCenter でのシンプルな構成設定によって有効になっています。アクセス制御により、許可されたユーザーだけが暗号化の有無を切り替えられます。「非暗号管理者」というロールを管理者に設定した場合、通常の管理タスクは実行できますが、暗号化の設定を変更する権限はありません。

転送中データの暗号化

転送中データの暗号化によって VxRail に総合的なセキュリティ体制が加わります。転送中データの暗号化はデフォルトでは無効化されていますが、vSAN ディスク グループのローリング フォーマットは不要なため、いつでも有効にできます。転送中データの暗号化にはキー管理サーバー（KMS）は必要ありません。FIPS 2 準拠のアルゴリズム（AES-GCM-256）暗号化キーは自動的に生成され、デフォルトで 24 時間ごとに再生成されるようになっています。

転送中データの暗号化は、重複排除や圧縮、静止データ暗号化などの他の vSAN 機能と併用できます。ハイブリッドおよびオールフラッシュ環境のノードでは転送中データの暗号化を有効（デフォルトでは無効）にできます。

オプションの NSX を使用した VxRail ソフトウェア デファインド ネットワーク

VxRail などの動的な仮想環境は、大抵ソフトウェア デファインド ネットワーク（SDN）サービスによる柔軟性のメリットを得られます。VxRail に SDN を導入する方法として最もシンプルなのは、VMware NSX です。オプションのソフトウェア ライセンスのため、VxRail には付属していません。NSX は完全なネットワーク仮想化とセキュリティのためのプラットフォームです。NSX ならルーター、ファイアウォール、ロード バランサーなどの仮想ネットワーク全体をソフトウェアだけで作成できます。このソフトウェアデファインド ネットワークは基盤となる物理ネットワーク インフラストラクチャとは切り離されているため、特定のスイッチ ベンダーに接続された VxRail に依存するということがありません。

VxRail と NSX の組み合わせは統合セキュリティ ソリューションとして、セキュリティ用ハードウェアやソフトウェアのコンポーネントを追加する必要性を軽減してくれます。VxRail 管理者は NSX を使用してマイクロセグメンテーションを構成することで、さまざまなテナント ワークロードの保護と分離、入口および出口の制御を実現し、従来の複数階層型アプリケーションや汎用型 VM、VDI 環境を含めたすべてのワークロードのセキュリティを強化できます。VxRail と NSX を併用するメリットの一例を次に挙げます。

- ワークロードに即したセキュリティ ポリシーを適用できます。セキュリティ ポリシーはソフトウェアに適用され、セキュリティ制御はワークロードとともにクラスター内のホスト間を移動します。
- セキュリティを備えたシンプルな管理が vSphere スタックと統合され、vSphere HTML5 Web Client と NSX Manager プラグインを介して vSphere で一元管理されます。
- グループとポリシーにより自動化された、一貫性のあるセキュリティ制御が特徴です。ワークロードは自動的に識別され、適切なセキュリティ体制に収まるように動的に配置されます。
- ハイパーバイザー レベルでの効率的なセキュリティ制御の実装により、外部的なセキュリティ制御や境界ベースのセキュリティ制御と比較してアプリケーションのレイテンシーと帯域幅の消費が緩和されます。
- トラフィックを制御する適切な許可/拒否ルールによって、内部および外部クライアントのインターネットからの入出力を制御する DMZ レベルの分離が可能です。
- VM のなりすまし IP アドレスを SpoofGuard 機能で検出し、ブロックします（この機能の詳細については、VMware の「SpoofGuard の使用」に関するマニュアルを参照してください）。
- NSX 管理者が Active Directory のユーザーベースで DFW ルールを作成できる ID ファイアウォール（この機能の詳細については、VMware NSX のマニュアルを参照してください）。
- 侵入検出と侵入防止（IDS/IDP）などのサード パーティー製セキュリティ サービスと統合できます。

環境のセキュリティ体制を強化する NSX は以下の認定と標準に準拠しています。

- Common Criteria 認定 − EAL 2+
- ICSA Labs 認定ファイアウォール
- FIPS 140-2 レベル 1
- 仮想化されたワークロードの保護に関する NIST のサイバーセキュリティ勧告の全項目に適合

VMware NSX プラットフォームのセキュリティ オプションを VxRail で利用すると、ファイアウォールとセキュリティ ポリシーが VxRail の内部に組み込まれ、外側に境界を設置するセキュリティとは異なる真の統合環境を整えることができます。VxRail と NSX を組み合わせて導入することで、ハードウェアやソフトウェアコンポーネントの追加増設によらず VxRail の一部としてセキュリティを制御できるようになるため、新たなアプリケーション施策の導入に要する時間が短縮されます。

ロックダウン モード

セキュリティのさらなる強化と柔軟性の両立を求められる環境では、ESXi にロックダウン モードを構成できます。ロックダウン モードでは個々のホストに対する管理操作が制限され、vCenter を介して管理タスクを完了させなければならない状態が強制的に適用されます。

「通常（Normal）」モードのロックダウンでは、任意のユーザー グループを許可リストに追加して、vCenter を使わずにローカルでサーバーを管理させることができます。この許可リストには特定の VxRail 管理アカウントを含める必要があります。

厳格なロックダウン モードではいかなるユーザーもローカルでサーバーを管理することはできません。なお、「厳格（Strict）」モードでのロックダウンは VxRail ではサポートされていません。

HTTPS を使用したセキュアな管理

セキュリティで保護されていない管理トラフィックは重大なセキュリティ リスクです。そのため VxRail では、Transport Layer Security「TLS 1.2」vCenter、iDRAC、HCI システム ソフトウェアすべてで保護された管理インターフェイスを使用して平文による HTTP インターフェイスを無効にし、TLS 1.2 を使用する HTTPS の使用を必須にしています。また、ESXi サーバーのコマンド ラインにアクセスする際は SSH を使用する必要があります。SSH と HTTPS の使用は、VxRail で利用するコマンドの安全性と制御にとって非常に重要な要素となっています。

完全性

会社のデータの整合性は、事業経営にとって基本的な要件です。VxRail ではデータのライフサイクルを通してその整合性、正確性、信頼性を維持することで、データの完全性を確保します。その具体的手段として、ユーザー アクセスの制御やデータ チェックサムなどの整合性に関連する組み込みの機能を用います。

ネットワークの区分化

ネットワークの区分化はプライベート ネットワークのトラフィックをパブリック トラフィックから分離し、攻撃対象領域を狭める手法として使用されます。このセキュリティ制御の手法は、攻撃者がネットワークを渡って移動するのを制限するうえでも効果的です。

VxRail の設計にはさまざまなレベルのネットワークの区分化（ハードウェア管理ネットワークの物理的な区分化、アプリケーションとインフラストラクチャ ネットワークの仮想的な区分化、VMware のオプション NSX ソフトウェアによる VM およびアプリケーション レベルのマイクロセグメンテーションなど）が盛り込まれています。区分化を適用すると重要な管理ツールに対する可視性が制限され、攻撃者がそれらをシステムに悪用するのを防ぐことができます。デフォルトでは、適切なネットワークの区分化がシステム初期化の

一環で自動的に構成されるようになっています。管理者はその初期構成に加えて、アプリケーション環境に必要なレベルの区分化を柔軟に定義できます。ネットワーク構成に関するベスト プラクティスについては Dell EMC VxRail ネットワーク ガイドに記載されています。

VxRail では VMware 分散仮想スイッチによって管理、vSAN、vMotion、アプリケーションの各トラフィック用に異なる VLAN を使用し、デフォルトでトラフィックを区分しています。vSAN ネットワークと vMotion ネットワークはルーティング不可能なプライベート ネットワークです。VxRail ネットワークでサポートされるアプリケーションによって異なりますが、トラフィックは、アプリケーションの種類や本番環境のトラフィックか非本番環境のトラフィックかなどの要件に基づいて、さらにセグメント化される場合があります。

VxRail 上の分散仮想スイッチは、デフォルトで vSphere Network I/O Control（NIOC）を使用して構成されます。NIOC により異なる VLAN に物理的な帯域幅を割り当てることができます。サービス拒否攻撃やワームなどの一部のサイバー攻撃はリソースの過剰使用を引き起こす恐れがあり、それが原因で直接攻撃にさらされていない他のサービスに対してリソースの拒否が発生する可能性があります。NIOC はあるサービスに対して攻撃が行われた際に、他のサービスが整合性を維持するために必要となるネットワーク帯域幅を確保する仕組みです。システムが初期化されると、推奨のベスト プラクティスに従って NIOC の設定が自動的に構成されます。VxRail のデフォルト VLAN に適用される NIOC 設定について、Dell EMC ネットワーク ガイドで説明しています。

各 VxRail ノードには iDRAC ハードウェア管理インターフェイス用の物理 Ethernet ポートが別に搭載されています。そのネットワークを物理的にセグメント化することで、攻撃者がハードウェアの管理機能にアクセスすることが困難になります。これにより分散型サービス拒否攻撃が発生しても物理的にセグメント化されたネットワークは影響を受けず、攻撃が及ぶ恐れのある範囲を限定できます。

UEFI セキュア ブート

UEFI セキュア ブートはオペレーティング システムの破損を防ぎ、ルートキットによる攻撃から保護する機能です。仕組みとしてはファームウェア、ブート ローダー、VMkernel のいずれもが信頼できる認証局の UEFI セキュア ブートによってデジタル署名されていること、また ESXi に対しては VMware インストール バンドル（VIB）が暗号で署名されていることをそれぞれ検証するものです。これによりサーバーのブート スタックで正規のソフトウェアがすべて実行され、それらが変更されていないことを確実に確認します。

ソフトウェア チェックサム

データの整合性で重要なのは、ストレージから取得したデータが書き込み後に変更されていないことを検証することです。VxRail はブロック レベルのエンドツーエンドのデータ整合性チェックサムをデフォルトで使用します。このチェックサムはデータが書き込まれる際に作成されます。作成されたチェックサムは読み取りの際に検証され、書き込み時のデータから変更されていることが示された場合は、RAID グループの他のメンバーからデータを再構築します。vSAN にもプロアクティブなスクラバー メカニズムがあり、アクセス頻度の低いデータであってもデータ破損の可能性を検出して修正できます。

可用性

IT システムを最新の状態に保ち、ハードウェアを正常に機能させ、十分な帯域幅を提供することは、いずれも会社のデータの可用性を確保し許可されたユーザーに提供するうえで重要な点です。VxRail のソフトウェア ライフサイクル管理、vSphere の可用性機能、プロアクティブな監視、組み込みのリカバリー機能に加えてハードウェアによる物理的なセキュリティと安全なシステム構成があれば、システムの可用性を最大限に引き出せます。

VxRail のソフトウェア ライフサイクル管理

IT インフラストラクチャの安全確保にあたって企業が取れる最も重要な措置の 1 つは、最新のソフトウェア アップデートとパッチを欠かさず適用することです。ただしアップデートとパッチではダウンタイムやパフォーマンスの改善につながる可能性のある問題が修正されることはありません。それらは普通、セキュリティの

脆弱性を修正するものであるからです。セキュリティのコミュニティーでは多大なコラボレーションが実現しています。VMware と共同で設計された VxRail では、セキュリティ修正プログラムの計画初期から投稿内容が読まれているおかげで、VxRail チームは認定前のセキュリティ パッチの検証と準備を速やかに進めることができています。とはいえ、誰もが味方というわけではありません。そこには脅威を緩和し修復すべく取り組む守り手の側と、脆弱性の悪用を目的とする攻撃者との間の競争があります。VMware と共同で設計された VxRail では、セキュリティ修正プログラムの計画初期から投稿内容が読まれているおかげで、VxRail チームは認定前のセキュリティ パッチの検証と準備を速やかに進めることができています。

VxRail のソフトウェア ライフサイクル管理では複雑でリスクの高いアップデート作業も、容易にインストールして安全に実装できるものに変わります。VxRail HCI システムはすべてのソフトウェア コンポーネントがバンドルとして設計、テスト、リリースされている唯一のシステムです。VxRail ソフトウェア バンドルには BIOS、ファームウェア、ハイパーバイザー、vSphere、付属の管理コンポーネントのアップデートが含まれる場合があります。脆弱性が検出された場合はそれがどこで発見されたものであれ、脅威を緩和するためのパッチが速やかに開発されます。アップデート バンドルは VxRail の幅広いハードウェア プラットフォームと、ソフトウェア スタック全体に対してテストを実施したうえでお客様にリリースされます。

アップデートの提供が開始されると HCI システム ソフトウェアを通じて管理者向けにその旨が通知されます。通知を受けた後はアップデート バンドルを直接ダウンロードしてプロセスを開始するか、アップデート プロセスのスケジュールを調整するかを選べます。システムがオンライン状態のときにローリング プロセスでアップデートが実行されます。再起動が必要な場合は、VM が自動的にクラスター内の他のノードに移行された後で続きが行われます。

HCI システム ソフトウェアのライフサイクル管理は複雑さの軽減効果があるだけでなく、システムにパッチを適用する際の所要時間と困難を軽減することでインフラストラクチャのセキュリティを高め、リスクを取り除いてくれます。

VxRail と vSphere の可用性機能

VxRail は VMware High Availability（HA）、VMware Distributed Resource Scheduler（DRS）、VMware 拡張クラスターなどの vSphere に実装されている可用性機能を利用しています。これらの機能によって VxRail の自動化されたソフトウェアがサポートされ、VxRail でホストされているサービスに継続的な可用性が提供されます。そのためこれらの機能が実装されたバージョンの vSphere を使用することをお勧めします。

VMware HA は VxRail クラスターで実行されている VM を監視する機能です。VM またはノードに障害が発生した場合、クラスター内の別のノードで HA が再起動します。VM の障害はさまざまな理由で起こります。サイバー攻撃、基盤となるハードウェアの障害、ソフトウェアの破損などがその一因として考えられます。VMware HA はアウテージを防止するわけではありませんが、サービスの回復にかかる時間を最小限に抑えることができます。

VMware DRS はクラスター内のすべてのホストに VM ワークロードを分散する機能です。DRS は VM リソースのニーズの変化に合わせ、vSphere vMotion を利用してクラスター内の他のホストに VM ワークロードを移行させます。サイバー攻撃は攻撃対象になっていない VM でもリソースの問題を引き起こす可能性があります。これは大抵、攻撃を受ける VM によってリソースが大量に消費されることが原因です。したがってホスト レベルでリソースの使用率が高いと同一ホスト上の他の VM が使用できるリソースにも影響が出ます。DRS はリソースが限られたホストから VM を移行させることで対象の VM を保護し、サービス提供を継続できるようにします。

VMware 拡張クラスターは VxRail クラスターを単一サイトから 2 つのサイト間へと拡張することで可用性レベルを向上させます。1 台の VM に対応するインスタンスは、1 つだけ存在します。ただしデータについては完全なコピーが両方のサイトで保持されます。万一 VM が実行されている方のサイトが使用できなくなっても、VM はもう一方のサイトで再開されます。

データ保護

強固なセキュリティによる防御は重要ですが、堅牢で信頼できるリカバリー計画も同じくらい重要です。侵害を受けた後のリカバリーにおいて要となるのがバックアップとレプリケーションです。リカバリーによる回復を容易にする手段として、HCI システム ソフトウェアにはファイルベースのバックアップとリストアが付属しています。すべての VxRail にはクラス最高のローカルおよびリモート レプリケーションを実現し、きめ細かなリカバリーに対応できる Dell EMC RecoverPoint for VM（RP4VM）のスターター パックが組み込まれています。

HCI システム ソフトウェアのファイルベースのバックアップとリストアは、VM の誤削除や内部的な破損に対する保護を提供します。バックアップは定期的に実施されるように構成することも、必要に応じて実施することもできます。vSAN データストア内のファイルをバックアップするオールインワンの機能であるため、ハードウェアやソフトウェアを別途用意する必要はありません。

RP4VM なら、たとえば VM が侵害された、データが破損した、あるいはランサムウェアに感染したという場合でも、VM とデータセットが攻撃を受ける前の時点にポイント イン タイムで即座にロールバックされるため、事業を速やかに立ち直らせることができます。VxRail Manager から直接インストールできる RP4VM を導入すると、使い慣れた vCenter プラグインを介して日常的なモニタリングを行えます。リカバリーについても vSphere インターフェイスから簡単に実行できます。

強力かつ包括的なデータ保護機能を求めている企業向けとして、VxRail では Dell EMC Data Protection Suite for VMware、Dell EMC Power Protect、Dell EMC Data Domain Virtual Edition が付属するオプションをサポートしています。

VxRail VM を再構築しなければならないような稀な事態が起きても、VxRail HCI システム ソフトウェアのファイルベースのバックアップ機能であればビジネス継続性の確保に役立ちます。

システム セキュリティ

VxRail の認証、許可、アカウンティング

認証（Authentication）、許可（Authorization）、アカウンティング（Accounting）の 3 つの頭文字を取った AAA フレームワークが組み込まれています。AAA はアクセスを制御して適切なユーザーにシステムを使用させ、ユーザーに応じたレベルのアクセスを提供し、どのような操作が誰によって実行されたかをログとして記録するように設計されています。

認証

HCI システム ソフトウェアとの認証は vCenter プラグインを介して SSO によって処理されます。VxRail vCenter は認証セキュリティ ポリシーに即して、組織の一元化された ID 管理システムをサポートします。

企業では多くの場合、LDAP を使用する Microsoft Active Directory（AD）などのディレクトリー サービスによって ID 管理を一元化しています。もし VxRail がスタンドアロン環境で、ドメインの一部でない場合は、ユーザーとパスワードを vSphere と iDRAC でローカル管理することができます。ベスト プラクティスの立場からは一元化した認証手段を使用することをお勧めします。

よくある環境ではユーザー名とパスワードに加えて、証明書、スマートカード、セキュリティ トークンのような追加の ID 検証を必要とする多要素認証によって、ID 管理を強化しています。VxRail はドメイン管理のユーザーとローカル管理のユーザーの両方に対して、多要素認証を全面的にサポートしています。

物理サーバー、VxRail のライフサイクル管理、そしてサーバー、ストレージ、ネットワークの仮想化環境の管理は、それぞれで担当者が異なるのが普通です。そのため VxRail では iDRAC、HCI システム ソフトウェア、vSphere のそれぞれにきめ細かなロールベースのアクセス制御が採用されています。

許可

「最小権限の原則」（POLP）を取り入れると、ユーザーには各自の役割を全うするのに必要なだけの権限が付与されます。vSphere には適切な権限を付与するために使用する、あらかじめ定義されたロールが複数用意されています。たとえば、「vSphere 管理者」や「HCIA 管理」というロールをユーザーに付与できます。両方のロールを付与することもできます。HCIA 管理は、vCenter 内の VxRail 管理プラグインから VxRail のライフサイクル管理タスクを実行できるユーザー権限を付与するロールです。一方 vSphere 管理者は、vCenter で管理者タスクを実行できる権限を付与するロールです。vSphere でカスタム ロールを作成すれば、さらに細かいレベルのアクセス制御も可能です。たとえば特権ユーザーはアラームを確認したりストレージ プロファイルを作成したりできますが、VM を導入することはできません。

ロールはユーザーとグループ、特定のオブジェクトに関連付けられます。オブジェクトとはモノまたはモノのグループです。たとえばあるユーザーまたはグループは、特定の VM やポートのアラートを確認する権限を持てますが、他のオブジェクトは確認できません。また、ユーザーに「アクセス不可」などの制限付きロールを割り当てれば、vCenter 内の特定の領域が表示されないようにできます。複数のユーザーまたはグループに同じオブジェクトに対するアクセスを付与しつつ、アクセスのレベルは揃えることも変えることもできます。親オブジェクトから継承した権限は、子オブジェクトに付与されたアクセス権でオーバーライドできます。

vSphere のロールベースのアクセス制御では「最小権限」と「責任の分離」というきめ細かいセキュリティ原則がサポートされています。このアクセス制御を活用すれば、セキュリティ管理者は企業におけるシステムの管理構造に基づいて厳密な権限を定義し、セキュリティを強化できます。

アカウンティング

システムを安全に保ったまま使用に供するには、構成とコンポーネントのステータスに対する変更を把握することが非常に重要です。変更は、一時的な修正により構成が変わったことで生じる場合がありますが、そうではなく侵入された徴候という可能性もあります。プロアクティブにインフラストラクチャを監視することは重要なセキュリティ アクティビティです。

然るべきタイミングで侵入を検出することは、攻撃者が重要なシステムを悪用できない程度のわずかな侵入に留められるか、それとも数か月もの間侵入を許し複数の重要システムを悪用の危険にさらしてしまうかという程の差にもなりえます。監査ログのシステムのメンテナンスを怠ると、攻撃の重大さを判断できるほど十分な情報が得られない場合があります。『2019 Trustwave Global Security Report』（閲覧するには登録が必要）によれば、調査したインシデントの 57%に企業および社内ネットワーク（2017 年の 50%から増加）が関わっているとのことです。[ii]

構成の変化はすべてのシステムに影響を与える難問です。システムの起動時点では安全な構成ベースラインを保っていても、時間の経過とともにシステムを脆弱にする変更が生じる可能性があります。そうした変更はさまざまな理由で発生します。トラブルシューティング中の一時的な変更、ベースライン構成の一部になる承認済みの変更などもこれに該当します。監視の仕組みがなければそうした変更を検出するのは非常に困難です。

情報を監視するにあたっての課題は、情報源が多種多様であることです。個々の VM、物理サーバー、仮想化インフラストラクチャ、ネットワーク、セキュリティ コンポーネント、アプリケーション自体など実に多岐にわたります。この情報から意味を見出すには、アクティビティと変更が一体となった統合的なビューが必要です。VxRail には vRealize Log Insight があります。Log Insight はサーバー、ネットワーク機器、ストレージ、アプリケーションなどの VMware ログを 1 つにまとめることができ、後掲の画像のように、ログデータから作成したグラフ付きの図をダッシュボードに表示できます。これは問題の根本原因を迅速かつ簡単に追跡できる、管理者にとって便利な機能です。次の画像が vRealize Log Insight のダッシュボードです。

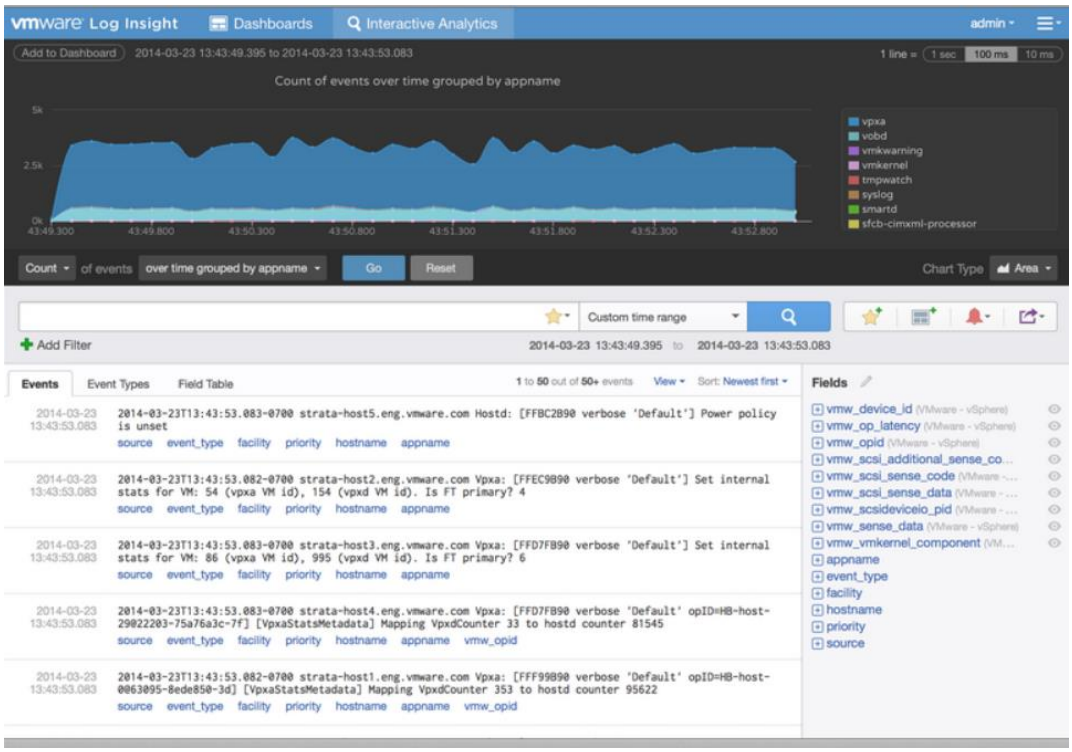


図 10： vRealize Log Insight

VxRail が業界標準の Network Time Protocol（NTP）を利用してすべてのコンポーネントのクロックを同期している数多くある理由のうちの 1 つは、これらすべての情報の関連付けにあります。

ログ管理システムや Security Incident and Event Management（SIEM）システムを導入済みの企業では、標準の Syslog プロトコルを使用して簡単に VxRail と統合できます。

VxRail の物理拠点におけるセキュリティ

物理的なセキュリティは包括的なセキュリティ ソリューションの不可欠な要素です。VxRail は従来のデータ センターの外に導入される可能性があるため、物理的なセキュリティは一層重要になりえます。USB ドライブを介してマルウェアや感染しているソフトウェアが入り込まないよう防ぐには、VxRail の USB ポートを無効にしておき、必要なときにだけ有効にする方法があります。

VxRail ノードはシャーシが開いたイベントやパーツの故障または交換、ファームウェアの変更、温度警告などのその他のイベントも監視します。この情報は iDRAC のライフサイクル ログに記録されます。大抵の場合、本番環境に移行した後にシャーシを開ける必要はありません。このようなアクティビティを追跡すればシステムの悪用を試みた徴候をつかめる可能性があります。

自動化

セキュリティを維持するうえで重要な点は、関連するすべてのセキュリティ構成要素を環境内のすべてのオブジェクトに確実に実装することです。個々の VxRail クラスターは最大 64 個の物理ノードを持つことができます。複数の VxRail クラスターを vCenter 1 つで管理できるため、対応可能な VM の数は数千台にもなります。単純な変更 1 つであっても、すべての VM に対して構成が必要であれば処理にかかる時間は膨大になります。また、反復的なタスクを実行しているときはミスを犯しやすいものです。そうした事情から自動化が重要性を帯びてきます。

自動化できれば環境の構成ミスが減り整合性が向上するだけでなく、効率が高まり、いつ意思決定を行いそれをいつ実施するのかという 2 つの決定がなされるまでの時間を短縮することができます。これにより、意思決定のタイム トゥ バリューが改善されます。

vRealize Automation などの互換性のあるツールは、vSphere と vSAN の自動化を可能にします。こうしたツールを活用することで VM やストレージ ポリシーの作成などの定常的な業務を自動化できます。vRealize Automation にはセキュリティ構成が適切な設定から変わっていないことを確認するという使い方もあります。構成が変更されると vRealize Automation は ESXi サーバー、vCenter、個々の VM を再構成して、求められるセキュリティ構成に再度準拠させることができます。VMware の標準ツールでもあるため、多くの IT 仮想化担当チームによって vRealize Automation の使用方法に関するノウハウが知られており、VxRail クラスターで機能するプロファイルが作成されています。

VxRail STIG 強化パッケージ

セキュリティの構成作業は複雑でミスを生じやすいプロセスであり、セキュリティによる軽減が求められる同様の多くのリスクが付き物です。VxRail インフラストラクチャを保護するプロセスは、3 つの要素によって簡略化されています。1 つ目は、vSphere の「デフォルトでセキュア」なアプローチによる構成です。2 つ目は、Defense Information Systems Agency Security Technical Implementation Guides（DISA STIG）が提示するセキュリティ強化の構想です。セキュリティ パラメーターを監視し必要に応じて確認および構成するという処理ができる自動化ツールは豊富に提供されています。そうしたツールを活用することで、ビジネス ニーズに応じて適切なリスク プロファイルを構成することができます。最後の 3 つ目として、予期しない変更が発生した場合に構成を既知のセキュアな状態に巻き戻す機能は、VxRail セキュリティの肝心な部分です。

vSphere 6.0 以降、VMware ではセキュリティを vSphere のデフォルト設定にするという取り組みに着手しました。これによって VxRail はそのまま使用しても安全性の高いソリューションとなっています。この取り組みの一環として、最も推奨されるセキュリティ設定をサイト固有の設定に分類するか、デフォルトのセキュアな設定にするという変更が加えられました。インストール後に変更が必要となっていた設定はアップデートを受けたことで、セキュアな設定がデフォルトになります。

サイト固有の設定に分類された構成は、デフォルトでは構成できません（たとえばリモート Syslog や NTP サーバーのホスト名）。VxRail では、VMware がサイト固有の設定に分類したものの多くは、インストールの一環で HCI システム ソフトウェアによって構成されます。

多くの組織ではシステムを強化するベースラインとして STIG を利用しています。この STIG では、人が読める形の PDF と自動化されたスクリプトの形式でチェックリストを利用できます。これにより自動化ツールに STIG を読み取らせ、手動操作を最小限に抑えて、推奨の構成と一致するように環境を構成できます。既存の VMware STIG は VxRail コンポーネント（vSphere、ESXi、vSAN など）をカバーし、実装が可能な限り簡単になっています。VxRail ソフトウェア バージョン 4.5.x、4.7.x、7.X を実行している Dell EMC VxRail は、関係のある DISA Security Technical Implementation Guidelines（STIG）の要件に準拠しています。

時間の経過とともに構成はセキュリティが低下した状態に変化する可能性があります。そのため構成を監視するだけでなく、初期のセキュアな状態に環境をリストアするという処理を自動化することも重要です。VxRail では必要な自動化レベルに応じて、複数のオプションがサポートされています。VxRail には現在の構成を STIG に照らし合わせてチェックする自動化された強化ツールがあり、構成に変更があった場合に既知のセキュアな状態に構成を巻き戻します。さらに対応範囲の広い自動化ツールが必要な場合、VMware vRealize Suite では VxRail 環境と連動してガバナンスと統制を維持したまま構成管理を自動化できます。VMware にはアプリケーションにさらに重点を置いたツールである AppDefense もあります。このツールでは機械学習を利用して VM と、VM がサポートするアプリケーションの既知の正常な状態に関する情報を収集し、その状態から変化したことを検知すると管理者に通知します。対処についてはインシデント対応ルーチンのライブラリを利用して自動化できます。

VxRail HCI システム ソフトウェアの SaaS マルチクラスター管理

セキュリティの概要

本質的なセキュリティを備えた SaaS マルチクラスター管理

VxRail HCI システム ソフトウェアの SaaS マルチクラスター管理は、VxRail クラスターが本質的に備えている運用のシンプルさを、運用のインテリジェンスによって補完します。SaaS マルチクラスター管理は、運用のシンプルさと運用インテリジェンスに本質的なセキュリティを組み合わせて提供することで、IT インフラストラクチャのトランスフォーメーションを目指す企業を支援します。

SaaS マルチクラスター管理は Dell EMC の IT 管理によるクラウド プラットフォームで実行されます。クラウドベースの SaaS ソリューションのため新しい機能を高頻度でシステムを停止することなく提供でき、優れたカスタマー エクスペリエンスを生み出す柔軟性があります。ディープ ラーニング向けのニューラル ネットワークは、VxRail がクラスターに関して収集できる膨大なメタデータを取得することで、予測機能を継続的に改善します。

VxRailのユーザーはWebポータルやMyVxRail（https://myvxrail.dell.com）を介してSaaSマルチクラスター管理にアクセスできます。ログインにはDell EMCサポートの認証情報を使用します。

SaaS マルチクラスター管理は VxRail HCI システム ソフトウェアで実行されているデータ コレクター サービスを介して、組織全体の VxRail クラスターの VxRail ノードからテレメトリー データを収集します。収集したデータは次の図に示すように、Secure Remote Services（SRS）ゲートウェイを介して安全にクラウド プラットフォームに転送されます。

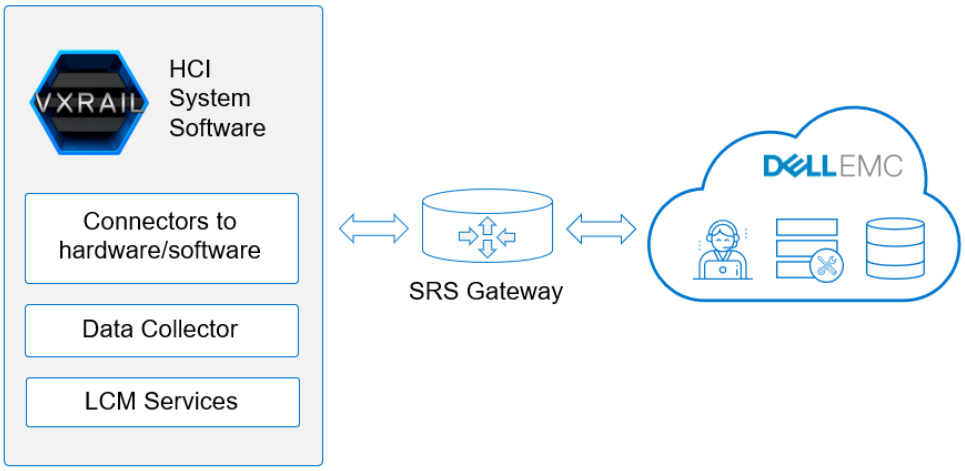


図 11： SaaS マルチクラスター管理の接続性

Dell EMC は、お客様がデータのセキュリティの維持に不安を抱えていることを理解しています。そこで SaaS マルチクラスター管理ではセキュリティを本質的なものとして設計に組み込み、転送データや静止データからのデータ コレクションもカバーしています。それだけでなく、Dell EMC の標準的なセキュリティ開発ライフサイクルの一部として、構造的な統制によって安全に開発されています。この標準には Dell EMC の製品チームが守るべきセキュリティに重点を置いた活動が定義されており、製品の開発からリリースの段階での、製品およびお客様環境に対するセキュリティ脆弱性のリスクを最小限に抑えられるよう取り組んでいます。

SaaS マルチクラスター管理のデータコレクション

各 VxRail クラスターでは Adaptive Data Collector（ADC）サービスが VxRail ハードウェアおよびソフトウェア コネクターを介して、HCI システム ソフトウェアからテレメトリー データを収集しています。個人識別情報（PII）については対象外です。次の表は ADC によって収集されるテレメトリー データの一覧です。

Table 1. SaaS マルチクラスター管理が収集する VxRail テレメトリー データ

基本テレメトリー（HW トポロジー：HCI、ドライブ、ファームウェア、PSU）	Performance Data	アラーム	ハードウェアのセンサーデータ
• クラスター情報 • HCI システム ソフトウェア	• クラスター（CPU、メモリー、ディスク） • VM（CPU、メモリー、ディスク） • vSAN（ディスク、ネットワーク）	• vCenter • VxRail	• センサーのタイプ • Health State • Name • 現在の計測値

ADC によって収集されるテレメトリー データはローカルには保存されず、Dell SRS ゲートウェイを介して安全に送信されます。

Dell に送信される SaaS マルチクラスター管理の転送データ

Adaptive Data Collector（ADC）によって収集されたデータのみが Dell EMC のバックエンドに送信されます。SaaS マルチクラスター管理は、SRS ゲートウェイ経由で HCI システム データの到着通知をサブスクライブします。 お客様はどのシステムから HCI システム データを送信するかをゲートウェイを介して制御できます。 Dell EMC SRS ゲートウェイ経由で送信されるすべてのデータは、転送時には業界標準のベスト プラクティスによって保護されます。SRS ゲートウェイは RSA®デジタル証明書に加えて、お客様制御のアクセス ポリシーと詳細な監査ログによって双方向に認証されます。Advanced Encryption Standard（AES）-256 ビット暗号化によってポイントツーポイントの通信を確立することで、Dell EMC IT 管理インフラストラクチャに転送されるすべてのデータをセキュリティで保護します。SRS では専用の VPN と多要素認証が使用されます。Dell にデータが到着すると SaaS マルチクラスター管理はデータを暗号化して、固有の Dell EMC IT 管理インフラストラクチャ内に保存します。

SaaS マルチクラスター管理の静止データ

テレメトリー データ コレクションが有効化されているクラスターから受け取った HCI システム データは暗号化され、Dell EMC IT 管理インフラストラクチャに保存されます。

Dell EMC IT インフラストラクチャには次の特徴があります。

- 各お客様のテレメトリー データを確実に分離するセキュアなプラットフォーム
- 高可用性、フォールト トレランス、ディザスター リカバリーに対応
- バックアップを含むお客様のテレメトリー データを検索（米国）
- SaaS マルチクラスター管理のアクティブな監視対象となっているシステムの履歴データ（SaaS マルチクラスター管理で生成された分析情報も含む）を無期限に保持
- 独立したセキュアなポータルへのアクセスを提供。このポータルで各ユーザーに表示されるのは、Dell EMC MyService360 で定義されたお客様のサイトへのアクセスを構成する、SaaS マルチクラスター管理内のシステムのみ

Dell の最高セキュリティ責任者が監督するデル・テクノロジーズの Security and Resiliency Office（SRO）は、SaaS マルチクラスター管理の SaaS ソリューションをホストする Dell EMC 情報技術インフラストラクチャのセキュリティと保護を担う組織です。その実現のために行われているのが、セキュリティ ポ

リシーや実施手順、情報セキュリティの管理を定評のある方法で統制することです。その具体的な方法として挙げられるのが階層型ファイアウォール、侵入検出システム、業界をリードするウイルス対策、マルウェア対策などです。 Dell EMC のサイバーセキュリティ チームはアプリケーションや基盤となる環境に対する脆弱性スキャンの継続的な実行に取り組んでいます。 修復が必要な場合はソフトウェアのアップグレード、パッチ、構成変更などによる現在進行形の脆弱性修復プログラムによって措置されます。

SaaS マルチクラスター管理に送信されるすべてのデータは、Dell EMC のデータ センターにホストされているインフラストラクチャに格納されています。情報セキュリティ ポリシーは Dell EMC のすべての情報とリソースに適切な保護を徹底するためのもので、情報の所有者はすべてのリソースに不明瞭な点がないようにし、各リソースに対して管理人を指定する必要があります。すべてのインフラストラクチャ コンポーネントは外部からのアクセスにさらされていない、専用の Dell EMC ファイアウォールで保護された隔離ネットワークの内部にあります。システム管理者とデータベース管理者のチームのメンバーを除けば、個人が直接データベース サーバーやデータベースにログインできない環境です。データベース アプリケーションのアカウントは標準的なデータベースのパスワード認証によって管理されます。 Dell EMC は業界のベスト プラクティスである変更管理プロセスを実装することで Dell EMC インフラストラクチャ ハードウェアの安定性を保ち、確実な制御と保護を図っています。変更管理には変更の管理に必要なポリシー、手順、ツールが用意されており、変更の評価と承認が適切に行われ、ユーザーに効果的に通知されるような仕組みが整備されています。

SaaS マルチクラスター管理のデータ アクセス制御

SaaS マルチクラスター管理のデータ アクセスは、次の 2 種類に大別できます。

- システム データや SaaS マルチクラスター管理から得られた分析情報の確認を目的とした、お客様による MyVxRail Web ポータルへのアクセス
- 社内の Dell EMC IT システム管理者およびデータベース管理者による、Dell EMC の管理下にある SaaS マルチクラスター管理インフラストラクチャへのアクセス

以下の小項目ではこの 2 種類のユーザーによるデータ アクセスの制御方法について説明します。

エンド ユーザーによる SaaS マルチクラスター管理へのアクセス

お客様は既存のサポート アカウントを使用して MyVxRail にログインします。MyVxRail から SaaS マルチクラスター管理データにアクセスするには、エンド ユーザー各自が有効な Dell EMC サポート アカウントを保有している必要があります。認証は Dell EMC のシングル サインオン（SSO）インフラストラクチャによって処理されます。 MyVxRail は Dell EMC MyService360 カスタマー ユーザー プロファイルを使用してアクセスを制御します。ユーザーが Dell EMC のアカウントに登録されると、ユーザー プロファイルが作成されて有効なカスタマー プロファイルに関連付けられます。 MyVxRail は各お客様に自社のシステムに関するビューを提供します。この安全かつ独立したビューによって、関係のあるデータだけが表示されます。MyVxRail で各ユーザーが見ることができるのは、Dell EMC MyService360 で構成されている自分のサイト アクセスの一部になっているシステムだけです。

Dell EMC IT の管理下にある SaaS マルチクラスター管理インフラストラクチャへの管理アクセス

お客様の専有情報や機密情報を保護することの重要性については、Dell EMC は細心の注意を払っています。その目的を果たすために、Dell EMC の全従業員は同意書に署名する必要があります。その内容には、すべてのお客様情報に対応する規定が盛り込まれています。同意書の義務は、いかなる方法あるいは形式のものであれ保守サービスに従事している期間に受領し、機械に保存されているデータに対して適用され、Dell EMC との雇用契約が終了した後も効力を持ちます。

互換性のある標準と認定

VxRail はコンプライアンス上の規制に対応できるように構成可能な、堅牢で柔軟なハイパーコンバージド インフラストラクチャです。中には互換性を謳っている HCI ベンダーもいますが、Dell EMC ではお客様にとって重要なセキュリティ標準の完全な認定の取得を積極的に進めています。極めて厳しいビジネス要件および規制条件に VxRail がどのように応えられるかについては、Dell EMC 担当者にお問い合わせください。VxRail で対応可能な標準および認定の一部を以下に説明します。

- **FIPS 140-2 の静止データ暗号化** — Federal Information Processing Standard Publication 140-2（FIPS PUB 140-2）には暗号化モジュールのハードウェアおよびソフトウェア コンポーネントの要件と基準が規定されています。米国政府および機密性が高いにも関わらず未分類の情報を収集、保管、移転、共有、普及するその他規制対象の業界（金融業界や医療機関など）では、FIPS 140-2 の認定が必要です。VxRail で使用される PowerEdge サーバーは認証済みです。

- **Common Criteria EAL 2+** — Common Criteria for Information Technology Security Evaluation は、コンピューター セキュリティ認定の国際標準（ISO/IEC 15408）です。Common Criteria の評価は、コンピューターのセキュリティ製品およびシステムを対象に行われます。システム セキュリティ機能を評価し、製品セキュリティ機能の信頼度レベルをセキュリティ保証要件（SAR）または評価保証レベル（EAL）で判定します。Common Criteria 認定ではセキュリティを保証できませんが、セキュリティの性質に関する主張を個別に検証することはできます。VxRail で使用している PowerEdge サーバーと vSphere コンポーネントは、現在完全な認定を有しています。

- **NIST Cybersecurity Framework** — NIST Framework for Improving Critical Infrastructure は企業がサイバーセキュリティやリスク管理、システムの耐障害性を改善するにあたっての指針として策定された、無償で公開されているガイドラインです。政府、業界、学識者などさまざまなパートナーと協議を重ね、合意に基づく確かなガイドラインおよび実践を集めたものとして、1 年以上をかけて作成されました。Special Publication 800-131A で規定されている暗号化キーの長さが推奨されています。

- **NSA Suite B** — Cryptographic Modernization Program の一環として National Security Agency が公布した暗号アルゴリズムのセットです。VxRail で使用されている ESXi および vCenter の現行バージョンは、NSA Suite B をサポートしています。

- **第 508 条 VPAT** — 米国のアクセス委員会第 508 条基準は米国政府が調達する電子および情報技術に適用される規定で、身体的、感覚的、認知的障害を持つユーザーに必要なアクセス要件を定義したものです。VxRail で使用する PowerEdge サーバーと vSphere ソフトウェア コンポーネントはどちらも第 508 条 VPAT に準拠しています。

- **Trade Adjustment Assistance（TAA）** — Trade Adjustment Assistance Program は貿易の影響で職を失った米国の失業者への支援を通じて雇用の拡大と促進を図る政府のプログラムです。VxRail がシステムとして販売される場合は TAA に準拠しています。

- **DISA-STIG** — 米国国防総省（DOD）の Defense Information Systems Agency（DISA）は、DOD の IT インフラストラクチャのセキュリティを維持する方法の 1 つとして策定された構成基準で、Security Technical Implementation Guides（STIGS）の名称で知られています。このガイドでは、そのままの状態では攻撃に対して脆弱な可能性のある情報システムやソフトウェアをロックダウンするにあたっての技術的なガイダンスが示されています。Dell EMC では VxRail の構成を手動または自動で実施して、DoD 情報ネットワーク（DISA）STIG の要件に準拠するための手順を提供しています。

- **IPv6** — IPv6 はインターネットの次世代のプロトコルです。IPv4 におけるアドレス数の制約を解決するだけでなく、セキュリティ面でもさまざまなメリットがあり多くの環境で IPv6 への移行が進められています。VxRail は USGv6 が定めるデュアル スタック モードの IPv6 対応と、高度な基準での IPv6 対応の相互運用性テストに合格しています。

- **Trusted Platform Module** — Trusted Platform Module（TPM）は Trusted Computing Group によって定義された仕様です。TPM 1.2 および 2.0 は VxRail でオプションとして使用できます。どちらのバージョンも FIPS 140-2、TCG、Common Criteria のセキュリティ要件に準拠しています。vSphere も TPM 1.2 および TPM 2.0 をサポートしています。

NIST Cybersecurity Framework と VxRail

NIST Cybersecurity Framework（NIST CSF）は民間企業のサイバー攻撃に対する防止、検出、対応能力を評価し、それを改善するためのコンピューター セキュリティに関するガイダンスとなる、ポリシー フレームワークです。この無償で提供されているフレームワークは、サイバーセキュリティに関連するリスクを管理するための標準、ガイドライン、ベスト プラクティスで構成されています。Cybersecurity Framework の優先度付けによる柔軟性で費用対効果に優れたアプローチは、核となるインフラストラクチャの保護と耐障害性の向上に効果的です。

NIST CSF の要となる要素は次の図に示すように 5 つの機能に区分され、それらがさらに細分化されています。

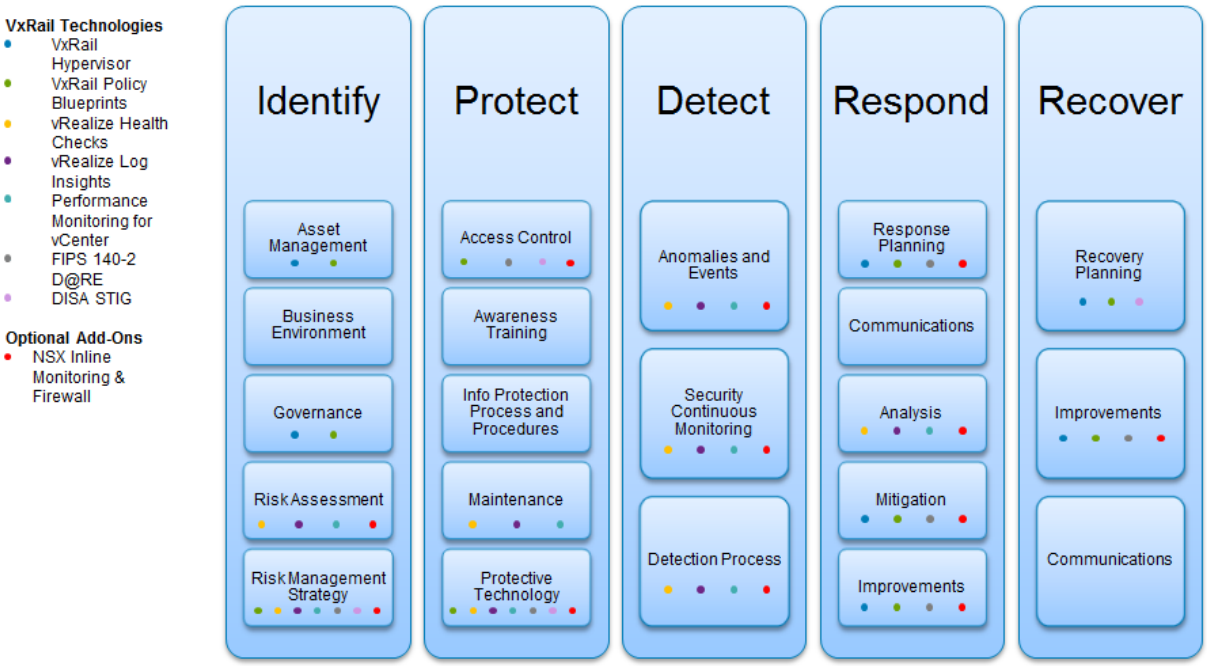


図 12： National Institute of Standards and Technology の Cybersecurity Framework

NIST CSF の詳細については、NIST の Web サイトを参照してください。

VxRail のセキュリティ ソリューションとパートナー

VxRail は設計段階でセキュリティが組み込まれ、セキュリティのベスト プラクティスに従って構築されたソリューションです。ユーザーの認証、許可は適切なアクセス レベルで行われます。VxRail クラスターは、静止データ暗号化を使用する簡単な構成でデフォルトのネットワーク構成セグメント トラフィックに含まれる情報の機密性を保護することができ、RecoverPoint for VM などのツールと合わせることでデータの整合性が損なわれた場合でもアプリケーションとサービスを速やかに復旧できます。このセキュリティ機能は VxRail の基礎であり、本質的に備わっている性質です。

しかしながら昨今の脅威から環境を保護するには、複数のセキュリティ レイヤーによる階層的な防御が欠かせません。VxRail で実行されているアプリケーションとサービスをその使用者となるユーザーに接続するためのネットワークは、必ず保護する必要があります。アプリケーションとサービス自体もやはり保護しなければなりません。ファイアウォール、侵入検出、予防システム、ウイルス/マルウェア対策、エンドポイント

保護、セキュリティ運用と管理は、そのすべてが多層防御の一部をなすものです。お客様の環境を完全に保護する広範なテクノロジーとサービスを持っている企業はデル・テクノロジーズだけです。

企業の規模と IT トランスフォーメーションの方向性によって適切なアプローチが定まります。既存のセキュリティ フレームワークでうまくいく環境もあれば、IT インフラストラクチャの変革に合わせてセキュリティ運用を変革する機会として利用できる環境もあります。企業の多くはセキュリティ プログラムの中でさまざまなベンダーを利用するため、それがもとで複雑さが増しリスクが高まります。デル・テクノロジーズ ファミリーである SecureWorks は、リスクの管理とデジタル資産の保護に有効なソリューションです。世界に通用するセキュリティの幅広い専門技術と、数千社規模のパートナーのエコシステムを単一ベンダーの関係性で提供できるのはデル・テクノロジーズをおいて他にありません。次の図は、リスクの管理やデータの保護を支援する Dell の総合力を示したものです。

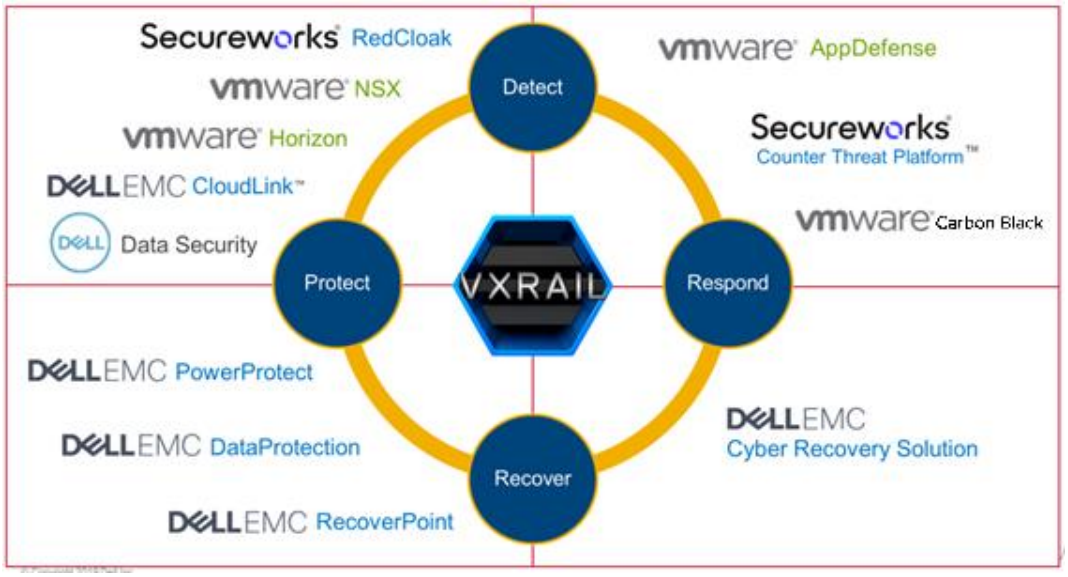


図 13： リスク管理やデータ保護を支援する Dell の総合力

ID およびアクセス管理

VxRail ではローカル ユーザー アカウント、LDAP 統合、シングル サインオンをサポートしています。スタンドアロンで VxRail を使用することもできますが、Microsoft Active Directory などのディレクトリー サービスを使用するエンタープライズ向けの ID およびアクセス管理（IAM）システムと統合することになるのが普通です。

Security Incident and Event Management

VxRail にはシステムのログ管理を一元化できる vRealize Log Insight が付属します。Splunk や Security Incident and Event Management（SIEM）システムなど、一元化された既存のログ管理機能を使用している企業であれば、業界標準の Syslog インターフェイスを使用して簡単に VxRail と統合できます。

セキュリティ イベント自体を管理したくないというお客様には、VxRailと、実質的にあらゆる情報資産やセキュリティ技術に対するログ管理サービスを提供するSecureWorksがあります。SecureWorksはビジネスの安全性を維持するのに必要なセキュリティ情報を収集し、それらを監視します。さらに重要なのは、SecureWorksの高度なスキルを持つセキュリティ エキスパートが、統合されたCounter Threat Operation Centerから24時間365日、あらゆる悪意のあるアクティビティを即座に調査、対応してくれる点です。

キー管理サーバー

暗号化は、情報の機密性を保護する強力なツールであり、VxRail には使用中データ、移動中データ、静止データを保護する暗号化機能が組み込まれています。しかしながら、暗号化によって提供されるデータのセキュリティは、暗号化プロセスで使用されるキーの生成、保護、管理に過ぎません。

暗号化キーは必要に応じて利用できる必要があると同時に、復号処理中のキーへのアクセスは、データの存続期間中保持される必要があります。したがって暗号化を効果的に利用するには、暗号化キーの適切な管理が不可欠です。多くの組織では企業全体でキーの管理を一元化することで管理の効率化、ポリシーの適用、コンプライアンスのためのレポート作成と監査に対応しています。

VxRail および vSphere は Key Management Interoperability Protocol（KMIP）をサポートするため、多くのエンタープライズ キー管理システムと連携できます。Dell EMC CloudLink は KMIP 対応のキー管理と、パブリック、プライベート、ハイブリッドの各クラウドに対応できる暗号化を提供します。既存のキー管理サービスを利用している企業であれば VxRail および vSphere と簡単に統合し、キーの管理を全社的に一元化できます。VMware では互換性のあるキー管理サーバーのリストを提供しています。

その他のセキュリティ パートナー

今日の IT インフラストラクチャとデジタル資産を安全に保護するという仕事は実に複雑です。単一のソリューションだけでは十分な堅牢性を備えた防御策は実現できません。それこそがデル・テクノロジーズがエコシステムのパートナーと共同でお客様環境に固有のリスクと脆弱性に対処する理由です。サイバーセキュリティに関するお客様目標を達成するには、業界全体が協調して対応にあたる必要があります。

Dell EMC の VxRail および VMware の vSphere はオープンなセキュリティ標準をサポートしており、お客様がセキュアな仮想のマルチクラウド IT 環境への移行を進めるにあたっては、パートナーが重要な役割を果たします。

付録 A でリンクされているホワイトペーパー『VMware Integrated Partner Solutions for Security and Compliance』には、VMware vSphere®、vCenter™、vShield Endpoint™、vCloud® Networking and Security™と統合されているネットワーキング、セキュリティ、コンプライアンスのパートナー ソリューションのリストと、vSphere でサポートされているアプリケーションとソフトウェアの完全なリストが掲載されています。VMware vCloud Ecosystem Framework では vShield Endpoint が提供するウイルス/マルウェア対策用の EPSEC API に加えて、vNIC および仮想エッジ レベルでのサービス挿入が可能です。VMware 互換性ガイドを利用すれば適切なコンポーネントを簡単に見つけられます。

まとめ

セキュリティ トランスフォーメーションの第一歩は安全な IT インフラストラクチャを導入することです。VxRail はコアからエッジ、クラウドまで安全なモダン インフラストラクチャを提供します。ハイパーコンバージド インフラストラクチャである VxRail は、インフラストラクチャに関わるコンポーネントの数を減らして単一の製品として設計、構築、管理することで潜在的な攻撃対象領域を狭めています。VxRail ソフトウェア ライフサイクル管理の VxRail 複合バンドルには BIOS、ファームウェア、ハイパーバイザー、vSphere、または実装されているあらゆる管理コンポーネントへのアップデートが含まれる場合があります。アップデートによってソフトウェア スタックはさらにシンプルになり、攻撃に対する脆弱性を低減できます。

昨今の脅威から環境を完全に保護するには、複数のセキュリティ レイヤーによる「階層的な防御」が欠かせません。VxRail で実行されているアプリケーションとサービスをその使用者となるユーザーに接続するためのネットワークは、必ず保護する必要があります。アプリケーションとサービス自体もやはり保護しなければなりません。ファイアウォール、侵入検出、予防システム、ウイルス/マルウェア対策、エンドポイント保護、セキュリティ運用と管理は、そのすべてが多層防御の一部をなすものです。

デル・テクノロジーズはセキュリティに対する理解があることはもちろん、世界各地のエキスパートがお客様の環境を評価し、固有の要件に適合したセキュリティ計画の設計を支援します。詳細については、デル・テクノロジーズ担当者にお問い合わせください。

参考情報

次の表は、本ホワイトペーパーの中で言及されているすべてのリンクや参考資料を一覧にまとめたものです。

資産	URL
リスク ベースのセキュリティ	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
EMC 製品のセキュリティ	https://www.dellemc.com/en-us/products/security/index.htm
Dell EMC セキュリティ開発ライフサイクル	https://www.dellemc.com/en-us/products/security/index.htm#tab0=2
Dell 製品セキュリティ インシデント対応チーム（PSIRT）	https://www.dell.com/support/contents/us/en/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
第 14 世代 Dell EMC PowerEdge サーバーのサイバー耐障害性セキュリティ	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense	https://www.vmware.com/products/appdefense.html
VMware Cloud Foundation on VxRail Architecture Guide	https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf
VMware 製品のセキュリティ	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf
Dell EMC VxRail Network Guide	https://infohub.delltechnologies.com/t/planning-guide-dell-emc-vxrail-network-planning/
VMware SpoofGuard 使用ガイド	https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
VMware NSX マニュアル	https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-B5C70003-8194-4EC3-AB36-54C848508818.html
ハイパーコンバージド ソリューションのセキュリティ	https://communities.vmware.com/servlet/JiveServlet/download/36084-3-183512/Security for Hyper-Converged Solutions_NSX.pdf
2019 Trustwave Global Security Report	https://www.trustwave.com/Resources/Library/Documents/2019-Trustwave-Global-Security-Report/
*1 2017 Data Breach Investigation Report	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 PWC『20th CEO Survey』（22 か国の 5,351 人のメンバー）	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
NIST Cyber Security Framework	https://www.nist.gov/cyberframework

資産	URL
互換性のあるキー管理サーバーのリスト	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc
VMware 互換性ガイド	https://www.vmware.com/resources/compatibility/search.php
VxRail Techbook	https://infohub.delltechnologies.com/t/techbook-dell-emc-vxrail-system-2/https://www.delltechnologies.com/asset/ja-jp/products/converged-infrastructure/technical-support/h15104-vxrail-appliance-techbook.pdf
Integrated Dell Remote Access Controller（iDRAC）のセキュリティ機能	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
vSAN マニュアル	https://docs.vmware.com/en/VMware-vSAN/index.html
Four business transformations	https://www.youtube.com/watch?v=TcKJ39_4Rwc
VMware の暗号化に関する認定	https://www.vmware.com/security/certifications/fips.html
VMware vRealize Log Insight	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
NIST の Dell EMC および VMware ベンダー別 FIPS 140-2 認定の検索	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
VMware セキュア開発ライフサイクル	https://www.vmware.com/security/sdl.html
VMware キー管理	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
vSphere 6.57.0 セキュリティ ガイド	https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-vcenter-server-70-security-guide.pdfhttps://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Dell EMC 製品のセキュリティ プログラムによる信頼の構築	https://www.emc.com/products/security/index.htm
SaaS マルチクラスター管理 ACE のリソース	
ACE の概要に関するデモ ビデオ	https://vxrail.is/acedemo
スマート アップデート バンドルのステージングに関するデモ ビデオ	https://vxrail.is/aceupdates
ソリューション概要 SaaS マルチクラスター管理のインフォグラフィック	https://www.dellemc.com/en-us/collaterals/unauth/infographic/products/converged-infrastructure/dell-emc-vxrail-hci-system-software-multi-cluster-management-infographic.pdfhttps://www.dellemc.com/resources/en-us/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf

資産	URL
Dell Technologies MyService360 の概要	https://www.delltechnologies.com/ja-jp/services/support-deployment-technologies/my-service-360.htm
『VxRail Comprehensive Security by Design』（ホワイトペーパー）	https://infohub.delltechnologies.com/t/dell-emc-vxrail-appliances-comprehensive-security-by-design/https://www.dellemc.com/resources/en-us/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
デル・テクノロジーズ製品のセキュリティ プラクティス	https://www.delltechnologies.com/ja-jp/products/security/index.htm
VMware vSAN 7 アップデート 1 に関するブログ記事 転送データの暗号化とセキュア ディスク ワイプ	https://blogs.vmware.com/virtualblocks/2020/10/12/vsan-a-secure-fortress-for-your-data/
YouTube - セキュリティ リソース	
Youtube - VxRail のセキュリティ強化とコンプライアンス	https://www.youtube.com/watch?v=ZjhfCE5nq6U
Youtube - VxRail のセキュリティの概要	https://www.youtube.com/watch?v=ZTNmYBgJv4s

[i] 2017 Data Breach Investigation Report
[ii] pwc-ceo-report-2017