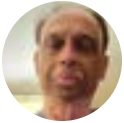


VMware Cloud Foundationの ネットワークングとラテラルセキュリティ におけるビジネス価値



Vijay Bhagavath
Research Vice President,
Cloud and Datacenter Networks, IDC



Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC



目次



各見出しをクリックすると、
該当ページへ直接移動します。

エグゼクティブサマリー	3
ビジネス価値のハイライト	3
概況	4
VMware Cloud Foundationのネットワーキングとラテラルセキュリティソリューション	5
VCFのネットワーキングとラテラルセキュリティにおけるビジネス価値	6
調査対象企業の市場特性	6
VCFのネットワーキングとラテラルセキュリティの選択と使用	7
VMware NSXとVMware vDefendのビジネス価値とベネフィットの数値化	9
ネットワーキングの効率性とコストベネフィット	11
セキュリティ上のベネフィットと効率化	14
アジリティと開発のベネフィット	16
運用リスク低減のベネフィット	18
ビジネスベネフィット	20
ROIの概要	20
課題と機会	21
結論	22
補遺1: 調査方法	23
補遺2: VMware NSXとVMware vDefendソリューションの使用に関するベネフィットの数値化	25
補遺3: 補足データ	26
IDCのアナリストについて	28

エグゼクティブサマリー

VMware NSX Network Virtualization (以下、NSX) とVMware vDefend Distributed Firewall (以下、vDefend) は、VCF (VMware Cloud Foundation) プライベートクラウドプラットフォームの重要なコンポーネントである。このプラットフォームは、Kubernetes/コンテナ、VM、API (Application Programming Interface)、マイクロサービスなどの最新のアプリケーションアーキテクチャ向けに、クラス最高水準のSDI (Software-Defined Infrastructure) を実装している。

VCFのVMware NSXとVMware vDefendは、迅速かつ効率的にビジネスアプリケーションを開発するための包括的なツールとリソース一式を提供している。

IDCは、VMware NSXとVMware vDefend (VCFのネットワーキングおよびラテラルセキュリティの総称) を使用することで得られる効果を、企業への使用経験に関するインタビューを通じて評価した。調査参加企業は、ネットワークやセキュリティ担当者の効率化、コスト削減、機能の向上を通じて、大きな価値を得たと報告している。

これらの直接的なベネフィットに加え、インタビュー対象のVMwareの顧客は、事業運営に対するサポートのアジリティ、拡張性、パフォーマンスの向上によるベネフィットについても報告している。

IDCは、VCFのネットワーキングとラテラルセキュリティを現在利用しているユーザーへのインタビューを分析し、以下のような効果によって、1データセンター当たり年間平均124万ドル (1組織当たり1,600万ドル) 相当のベネフィットを実現できると予測している。

- プライベートクラウド環境におけるより効率的でコスト効率の高いネットワーキングの提供
- プライベートクラウドのセキュリティ機能の向上とセキュリティ関連のリスク低減
- 開発チームによるビジネスニーズへのより迅速な対応の実現
- ネットワークやその他のIT機能の停止に伴う運用リスクの低減
- より迅速なビジネス機会への対応と顧客への高品質なサービスおよび製品の提供による、より多くのビジネス成果の達成



各項目をクリックすると、本書内の該当箇所へ移動します。

ビジネス価値のハイライト

610%
3年間の投資収益率

6か月
投資回収期間

25%
ITネットワーク管理の効率化

70%
インフラストラクチャおよび直接的なコストの削減

35%
ITセキュリティチームの効率化

11倍以上
East-Westネットワークトラフィックの安全性向上

6%
開発者の生産性向上

196万ドル
1企業当たりの年間収益増加額

概況

ネットワークのモダナイゼーションは、企業のデジタルトランスフォーメーションの一環としてプライベートクラウド環境を実現する上で極めて重要である。これを実施するには、大規模で複雑な、世界規模で展開している企業向けデータセンターの設計方法とライフサイクルの管理方法を考え直す必要がある。

最新のSoftware-Definedインフラストラクチャへの移行は、セキュリティ、レジリエンシー、管理性、ピーク時のアプリケーションパフォーマンス、コスト効率の確保に関する課題が伴う。これは、フルスタックのエンタープライズアプリケーションが、社内とサードパーティのクラウドデータセンターにまたがるプライベートクラウド環境に分散する、仮想化およびコンテナ化した一連のワークロードとして実装されている場合に発生する。

このような場合は、VMware Cloud Foundationのような本番環境に対応したSDIプラットフォームの出番となる。VMware Cloud Foundationは、コンピューティング、ストレージ、ネットワーク、セキュリティのSoftware-Definedサービス一式に加え、Day 0からDay 2以降のクラウド管理機能を提供する、Broadcomのソフトウェアポートフォリオの主力プラットフォームである。

IDCがインタビューした企業のIT部門やビジネスリーダーは、プライベートクラウドを構築するために、本番環境に対応したSoftware-Definedインフラストラクチャプラットフォームを使用する必要性を指摘し、それには、複数のベンダーの製品を寄せ集めた煩雑な構成ではなく、単一ベンダーの製品が理想的であると指摘している。統一された最新のインフラストラクチャをベースにしたプライベートクラウドは、真のクラウド運用モデルで稼働し、開発者にクラウドエクスペリエンスを提供し、強力なセキュリティとレジリエンシーで保護されている。

仮想化されたネットワーキングとコンピューティングは、プライベートクラウドとハイブリッドクラウドのデータセンターを柔軟に拡張できるようにするのに対し、仮想化および分散化されたセキュリティ機能やフルスタックオペラビリティ機能は、脅威に対する脆弱性を軽減し、損害が大きいアプリケーションの停止時間を低減し、業界特有の要件や規制要件へのコンプライアンスを確保するのに役立つ。

つまり、IDCはSoftware-Definedインフラストラクチャを、企業のデジタルトランスフォーメーションとデータセンターモダナイゼーションへの取り組みを加速するために不可欠なものとみている。これによって、ITチームはクラウド規模のアプリケーションを効果的に構築および管理し、優れたビジネス成果を上げられる。

VMware Cloud Foundationの ネットワーキングとラテラルセキュリティ ソリューション

本IDC Business Valueレポートでは、VCFプライベートクラウドソフトウェアの2つの重要なコンポーネントであるVMware NSX Network VirtualizationとVMware vDefend Distributed Firewallに着目している。これらのテクノロジーは、VCFのネットワーキングとラテラルセキュリティの基盤となるテクノロジー機能を主に提供する。

NSXはVCFソフトウェアスタックのコアコンポーネントであり、VCF SKUを通じてのみ購入できる。vDefendは、vDefend Firewall SKUまたはvDefend Firewall with Advanced Threat Prevention SKUによってVCFに提供されるアドオン機能である。

NSX Network Virtualizationは、企業のITバイヤーに以下の主要な価値を提案する、VCFにおける業界独自のSDN (Software-Defined Networking) テクノロジーである。

- プライベートクラウドとハイブリッドクラウドのデータセンターで実行される従来のアプリケーションと最新アプリケーションのためのクラウド運用モデルの簡便さと拡張性のベネフィット
- エンドツーエンドの自動化と詳細な可視化によるネットワーク運用および最適化の簡素化と高速化
- 信頼性の高いランサムウェア対策と簡素化された障害復旧機能によって、サイバー攻撃やデータセンター停止の場合でもアプリケーションの可用性を確保
- データセンターのフットプリントの大幅な削減による、コンピューティングインフラストラクチャの利用率向上、二酸化炭素 (CO2) 排出量の削減、コスト削減 (スペース、HVAC、電力、インフラ)
- 高性能のGenerative AI (生成系AI: 以下、GenAI) クラスター向けにデータセンターのネットワークスループットを高速化するネットワークアクセラレーション機能によって、AIトラフィックとワークロードのプロファイルに特化したネットワーク性能の調整が可能

VMware vDefend Distributed Firewallは、VM、コンテナ、ベアメタルのワークロードを保護するSoftware-Definedのレイヤー7ファイアウォールである。

主な機能を以下に挙げる。

- **IDS/IPS、サンドボックス、NTA/NDRを備えたステートフルファイアウォール**をソフトウェアによって分散化し各ホスト上で提供
- **アプリケーションとフローに対する全体的な可視性とインサイト**。ワークロードのライフサイクルにポリシーの自動化を組み合わせ、規模に応じたマイクロセグメンテーションを実現
- セキュリティ運用チームが攻撃ベクトルのラテラルムーブメントをブロックし、フォレンジックを迅速化し、よりシンプルな運用モデルでITセキュリティポリシーの自動化を実現するために**セキュリティアーキテクチャのスケールアウトを実現可能な各ホスト上で動作する分散ファイアウォール機能**
- **ボットネットマスターのようなインターネット上の既知の悪意あるIPアドレスから企業ネットワーク上のアプリケーションを保護**（悪意のあるIPアドレスのリストは、VMwareのグローバル脅威インテリジェンスネットワークから逐次更新される）
- **Threat Preventionまたはフルスタックセキュリティを提供可能なAdvanced Threat Preventionアドオンによる、既知および未知の脅威に対する防御**—ファイアウォール、IDS/IPS、サンドボックス、NTA、NDR、暗号化トラフィック監視など

VCFのネットワーキングとラテラルセキュリティにおけるビジネス価値

調査対象企業の市場特性

IDCは、企業8社に対し、VCFのVMware NSXとVMware vDefendソリューションに関する使用経験について詳細なインタビューを実施した。インタビューに際し、NSXおよびvDefendのソリューション独自のベネフィットと、両方のソリューションを利用することによる複合的な価値を把握しようと努めた。

Table 1 (次ページ) に示すように、調査参加企業のプロフィールは、平均従業員数5万2,900人、年間平均収益322億5,000万ドル（中央値は、従業員数5,500人、年間収益14億3,000万ドル）で大企業レベルのプロファイルであった。北米および欧州の両方、中東、アフリカを拠点とする高等教育（2）、公共部門、医療、法律、製造、ソフトウェア、通信などのさまざまな業種の企業が、VCFソリューション向けのネットワーキングとラテラルセキュリティに関する経験について情報提供をしている。

TABLE 1

インタビュー対象企業の市場特性

	平均	中央値
従業員数	5万2,900	5,500
ITスタッフ数	5,621	275
ビジネスアプリケーション数	1,817	850
年間収益	322億5,000万ドル	14億3,000万ドル
国	米国 (4)、英国、ドイツ、スウェーデン、スイス	
業種	公共部門、医療、高等教育 (2)、法律、製造、ソフトウェア、通信	

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

VCFのネットワーキングとラテラルセキュリティの選択と使用

調査参加企業は、VMware NSXおよびVMware vDefendソリューションを選択した理由を詳細に述べる中で、強力なネットワーキング機能とセキュリティ機能とより広範なVMware環境の継続性を維持できることに重点を置いていることを明らかにしている。ネットワークとセキュリティの機能を組織に提供するには、コスト効率良く拡張し、全体的な機能を向上させるアプローチが必要であると気づいたのである。調査参加企業はVMware NSXとVMware vDefendの導入を、ネットワーキングとセキュリティ環境のそれぞれの目的を達成し、ネットワーキングとセキュリティのソリューションを使用することで得られる有益な相乗効果を生かす機会と捉えていた。

インタビュー対象のVMwareの顧客は、自社の検討項目について説明している。

セキュリティとネットワーキングへの統合的なアプローチ：

「VMware Cloud Foundationは、実際のサーバーをユーザーに近い位置に配置する独自のアプローチを提供しているため、セキュリティ機能は、エッジに置くのではなく実際のサーバーを取り囲むようにしています。つまり、深く統合されているのです」

データセンター内のマイクロセグメントが可能：

「VMware Cloud Foundationを選択したのは、vSANとすべてのVCFソリューションを利用したいと考え、データセンターをマイクロセグメント化し、多数のセキュリティを追加導入したかったからです。＜中略＞境界防御だけに頼ることはできません。また、データセンターのセキュリティも確保する必要があり、現在は1つのソフトウェアスタックで、すべてのニーズに応えることができます」

SDDC (Software-Defined Datacenter) で制御を維持しながら、デプロイのスピードアップを実現：

「ソフトウェア開発者に対して迅速なデプロイを行うためにVMware Cloud Foundationを選択しました。最新かつ最高のサービスを彼らに提供することで、外部のクラウド環境に放り出すことはせず、自社のデータセンターに留まることができます。＜中略＞SDDCを使用することで、パブリッククラウドに資金を投じることをせず、コストを削減しています」

価格と熟練した人材の確保：

「VMware Cloud Foundationを選んだ主な理由は価格と経験豊富な人材の確保の2点です。当社はグローバルに事業展開していますが、主要な事業拠点は1つです。少なくとも中程度のスキルを持つ人材を確保できる製品を選ぶ必要があり、VMwareはそれを叶えてくれました」

Table 2は、調査参加企業によるVMware NSXとVMware vDefendソリューションの広範な利用に関する情報を示している。インタビュー対象のVMwareの顧客は、平均13のデータセンターと332拠点をサポートしていると回答しており、分散するITやビジネスの運用を行うためにどのようにVMware NSXとVMware vDefendを利用しているかを明らかにした。また、平均で4万4,986人の従業員がITサービスに依存していることや、VCFのネットワーキングとラテラルセキュリティを実行している部分の売上高が平均61%であることから、その利用規模の大きさがうかがえる。

TABLE 2

インタビュー対象企業によるVMware NSXとVMware vDefendの利用状況

	平均	中央値
データセンター数	13	3
拠点数	332	5
物理サーバー数	586	132
VM/クラウドVM数	15,094	1,775
アプリケーション数	1,377	700
アプリケーションのユーザー数	44,986	2,000
サポートされている収益の割合	61%	80%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

VMware NSXとVMware vDefendのビジネス価値と ベネフィットの数値化

調査対象企業はVMware NSX Network VirtualizationとvDefend Distributed Firewallソリューションを使用することで大きな価値を得ていると報告している。これらのソリューションを単独で使用した場合でも、調査参加企業はネットワークとセキュリティの運用の効率、堅牢性、コスト効率を高められている。また、VMware NSXとVMware vDefendのソリューションを組み合わせることで、ビジネス運用に適したアジリティと安全性を高めた高性能なIT基盤を確立している。

インタビュー対象のVMwareの顧客は、セキュリティ、開発、ビジネスのアジリティと 成果などの分野における重要な影響について具体的な例を挙げている。

データのセキュリティ、開発チームへの支援：

「VMware NSXとVMware vDefendの最大の価値は、安全なデータとその評価の維持です。次は、2,000人の開発者のためのデプロイの迅速化でしょう。以前は、開発者にリソースを提供するために、ネットワークインフラストラクチャの場合は2〜3週間かかっていましたが、今では数分で提供できます」

セキュリティの強化と管理の容易さ：

「VMware vDefendの主なベネフィットはセキュリティですが、管理がしやすいというベネフィットもあります。さまざまなスイッチやファイアウォールをすべて手動で設定することはなくなりました。＜中略＞また、さまざまなパイプラインをすべて自動化するために、システムを仮想化ベースに構築しているため、今後の自動化にも役立ちます」

トラフィックとセキュリティの可視性の大幅な向上：

「VMware NSXとVMware vDefendのITに関連する最大のベネフィットは可視性です。あらゆるものの動きが見え、トラフィックの流れ、パターン、不規則性を把握するのがはるかに簡単になりました。これはセキュリティ面では素晴らしいことで、非常に役立っています。＜中略＞劇的な変化です」

顧客主導のセキュリティ要件への適合：

「今はセキュリティに大きな関心があります。我々の顧客は、非常に具体的なトピックについてたずねるアンケートを含め、当社がどのようにセキュリティを確保しているかについてたずねてきます。VCFのネットワーキングとラテラルセキュリティのおかげで、当社はこれらの目標を達成し、他のソリューションに比べて効率的な方法で実施できるため、セキュリティ確保が簡略化されました」

VMware NSXとVMware vDefendを使用している顧客へのインタビューに基づき、IDCは、それらの顧客が以下の分野で、1データセンター当たり年間平均124万ドル（1企業当たり1,600万ドル）相当のベネフィットを実現すると算出している。

・ ITスタッフの生産性ベネフィット：

調査参加企業は、開発、ネットワーク、セキュリティなどのコアITチームの効率を大幅に向上させている。ネットワークとセキュリティのチームは、日常業務の処理に要する時間を大幅に短縮し、開発チームは事業運営の支援において大きな価値をもたらしている。IDCは、スタッフの効率化と生産性向上の価値を1データセンター当たり年間平均88万3,800ドル（1企業当たり1,138万ドル）と算出している。

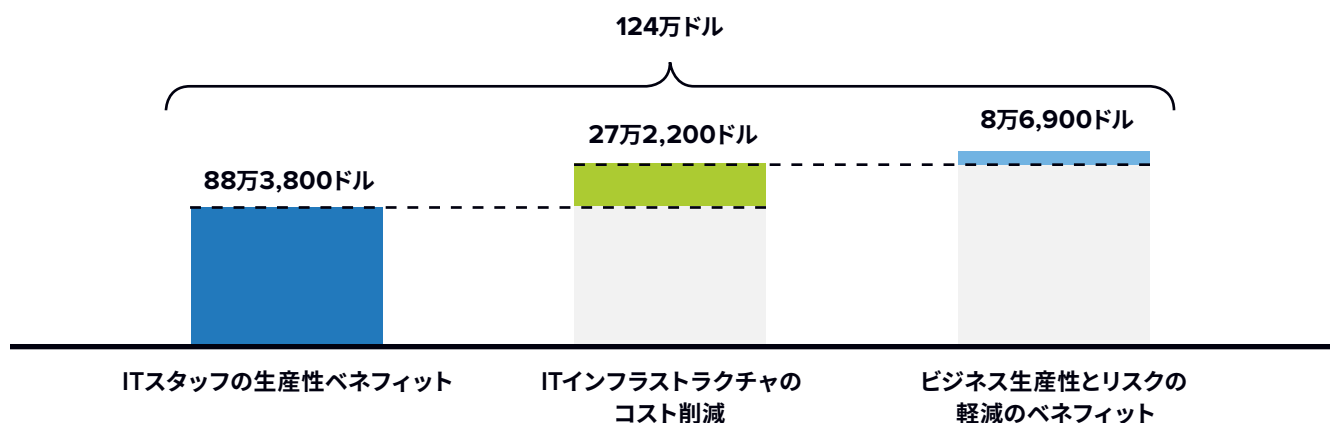
・ ITインフラストラクチャのコスト削減：

調査参加企業は、仮想化の拡大によってネットワークインフラストラクチャの要件を最小限に抑え、セキュリティのポイントソリューションを統合することで、直接的なコストを大幅に削減できている。IDCは、1データセンター当たり平均27万2,200ドル（1企業当たり350万ドル）の年間コストを削減できると推定している。

・ ビジネスの生産性とリスク軽減のベネフィット：

調査参加企業は、計画外停止が業務に与える影響を最小限に抑え、事業部門がビジネス機会によりうまく対処できるように、タイムリーで高品質なサービスやソリューションを提供している。IDCは、1データセンター当たり年間平均8万6,900ドル（1企業当たり112万ドル）に相当する実際の生産性と収益が得られると算出している。

FIGURE 1
1データセンター当たりの年間平均ベネフィット
(ドル)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

本図におけるデータを分かりやすくした表を見る場合は、補遺3のFigure 1 補足データを参照のこと。

ネットワーキングの効率性とコストベネフィット

調査参加企業は、VMware NSX Network Virtualizationソリューションを使用して、高度な仮想化を特徴とするSDDCを構築することで、ネットワーク関連のスタッフとコストで大きなベネフィットを得られたと報告している。最も多かったのは、VMware NSXによって、従来のネットワーキング環境と比べて可視性、アジリティ、自動化が明らかに強化されているという指摘である。プロビジョニングやトラブルシューティングなどの業務が自動化されたことで、ネットワーク環境の運用に日々割かれていたスタッフの作業時間が削減された。これによって、ネットワーク環境がよりシンプルになり、複雑さが軽減されたのである。

インタビュー対象のVMwareの顧客は、VMware NSXを使用することで、ネットワークインフラストラクチャチームが、より効率的に業務を遂行できるようになったとコメントしている。

自動化によりIT関連の作業がスピードアップ：

「VMware NSXを使用することで、技術者が行わなければならない低レベルのタスクのほとんどを排除できました。＜中略＞この自動化によってネットワークチームやサーバーチームは多くの時間を節約しています」

統合されたITチームをサポートするためのプラットフォーム：

「VMware NSX環境では、コンピューティング、ネットワーク、セキュリティなどのすべての構築作業を単一チームに任せ、その過程でコンプライアンスや変更管理などに対応することで、非常に迅速かつ容易に目的を達成できます」

チーム全体の大幅な効率化：

「VMware NSXを導入したことで、より少ない人員でより多くのサーバーを扱えるようになりました。＜中略＞現在はすべてが自動化されているため、以前はネットワークチームに14人必要でしたが、現在は2人で済んでいます。余ったチームメンバーを他の業務に割り当てました」

スタッフの注力を日常業務から他へ移行：

「VMware NSXの最大の価値は、時間の節約です。スタッフは運用に関する業務に注力する代わりに、将来のテクノロジーや、他のことについて学べるようになりました」

Table 3 (次ページ) は、VMware NSX Network Virtualizationの利用が、ネットワークインフラストラクチャチームの日常業務に与える影響に関するIDCの調査結果を示している。調査参加企業は、これらのチームの効率が平均25%向上したと報告している。その結果、より複雑なネットワーク管理業務や他のITやビジネスの取り組みに関するサポートに費やせるスタッフの作業時間が大幅に増加した。

TABLE 3

ネットワークチームの効率

1企業当たりの平均	VMware NSXおよび VMware vDefend 導入前／導入なし	VMware NSXおよび VMware vDefend 導入後	差	改善率
同じワークロードに必要な同等のFTE数	19.8	14.7	5.1	25%
必要なFTE時間に相当する価値 (1企業当たり年間ドル額)	198万ドル	147万ドル	50万1,700ドル	25%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

また、インタビュー対象のVMwareの顧客は、NSX Network Virtualizationソリューションの使用によって、ネットワークインフラストラクチャの直接コストを大幅に削減したと報告している。彼らはSDNオーバーレイを完全に構築することで、ネットワークハードウェアの追加購入と運用の必要性を抑えるというベネフィットを得ている。

さらに、100%のSDN環境を構築することで、ネットワーク環境の運用コストモデルを確立し、より高額で時間のかかる購入サイクルから脱却できる。インタビュー対象のVMwareの顧客は次のようなインフラストラクチャ効率化の例を挙げている。

ネットワークハードウェアコストの削減：

「VMware NSXを導入したことで、ネットワークスイッチにこれまでと同等の投資を行う必要がなくなり、ハードウェアのコストを削減できました。おそらく、年間100万ドルから200万ドルの節約になるため、これをVMware NSXの費用に充てています」

コスト削減に投資するベネフィット：

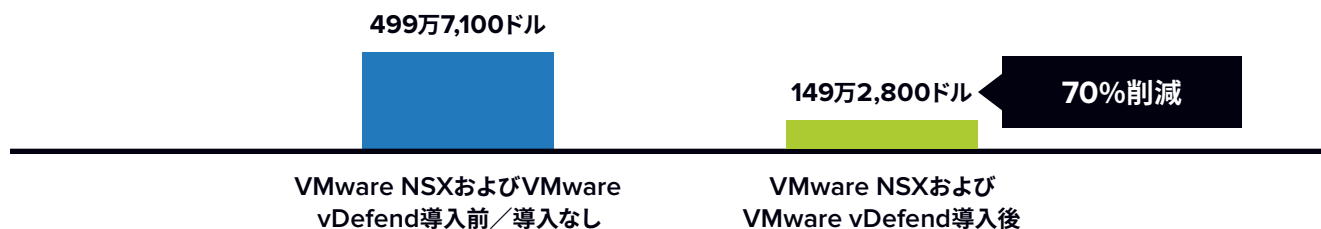
「他のクラウドプロバイダーに支払っていた費用を、ハードウェア、人材、サポート、サービスに投資できます。年間数百万ドルを節約し、今はそれを自社に投資しています」

電力使用量の大幅削減：

「VMware NSXによってフットプリントが大幅に削減されたため、持続可能性の目標達成に貢献しています。以前使用していた物理サーバーのセットに比べて、電力使用量が大幅に削減されました。少なくとも電力使用量を80%削減できました」

Figure 2に示すように、調査参加企業はVMware NSX Network Virtualizationを活用して、コスト効率のより高いネットワークインフラストラクチャ環境を構築している。直接的なコストを平均70%削減し、これによって1企業当たり年間平均約350万ドルを節約できたと報告している。

FIGURE 2
ネットワークインフラストラクチャの年間平均コスト
 (1企業当たりの年間コスト (ドル))

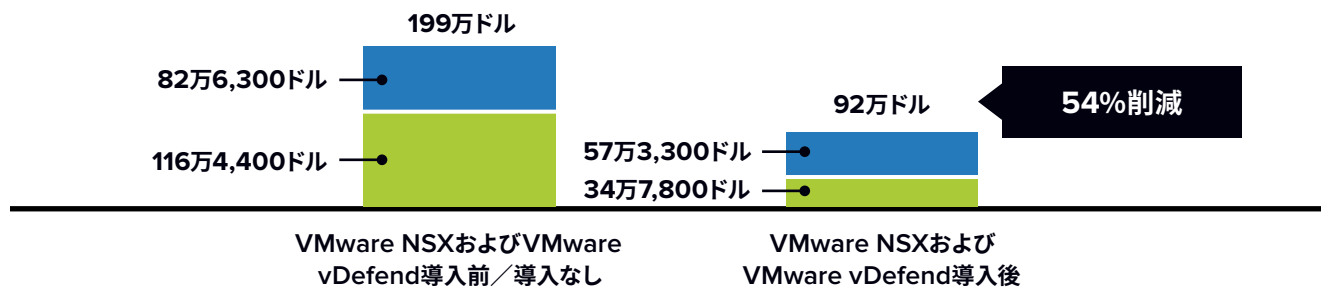


n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

このようなスタッフとインフラストラクチャの節約と効率化によって、調査参加企業は、よりコスト効率の高いネットワークとセキュリティサービスでビジネスをサポートできる。Figure 3に示すように、IDCは、調査参加企業がこれら2つの分野で3年間に平均54%のコストを削減し、1データセンター当たり年間平均100万ドル以上のコスト削減が可能になると算出している。

FIGURE 3
3年間の運用コスト
 (1データセンター当たりの3年間のコスト (ドル))

- スタッフの作業時間のコスト (インフラストラクチャ、セキュリティ)
- インフラストラクチャ/VMware VCFのネットワーキングとラテラルセキュリティのコスト



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

本図におけるデータを分かりやすくした表を見る場合は、補遺3のFigure 3補足データを参照のこと。

セキュリティ上のベネフィットと効率化

調査参加企業は一律に、VMware vDefend Distributed Firewallソリューションによってセキュリティが大幅に向上したと報告している。組み込まれたセキュリティ機能によって、より迅速に脅威を特定でき、ネットワークやIT環境に流入し、移動するデータやトラフィックに対して、より包括的なセキュリティを提供できると説明している。

調査参加企業は、VMware vDefendソリューションによってセキュリティ機能がどのように強化されたかについて、具体的な例を挙げている。

大幅に強化されたEast-Westトラフィックのセキュリティ機能：

「VMware vDefendは、セキュリティ面、特にマイクロセグメンテーションによってEast-Westトラフィックに対するファイアウォール適用に大きな変革をもたらしました。〈中略〉現在は、VM単位で非常に細かく制御できるようになり、セキュリティが大幅に強化されました」

可視性の向上による、より強固なセキュリティの実現：

「VMware vDefend Distributed Firewallの導入によって、かつては見るのが難しかったことすべてが見えるようになったため、セキュリティが大幅に向上しています」

堅牢なセキュリティゾーン：

「VMware vDefendは、さまざまなセキュリティゾーンでのセキュリティ確保に大いに役立っています。以前は、さまざまなセキュリティゾーンがあり、そのセキュリティゾーン内では、すべての通信がオープンで、フローを追跡するのは困難でした」

既存のインフラストラクチャも含めた容易なセグメンテーション：

「VMware vDefendは、デバイスをセグメンテーションするスピードが速いため、セキュリティに役立っています。ハードウェアを追加せずに、より迅速にセグメント化できます」

すべてのワークロードのセキュリティを一画面表示：

「VMware vDefendでは、単一画面で10か所の環境をチェックできるため、問題がどこにあるかを正確に把握できます。現在はすべてのワークロードを見られるので、すべてを把握できます。また、セキュリティオペレーションセンターやオペレーションチームなど、セキュリティチームの人員もセグメント化できます」

高額な物理ハードウェアの廃止：

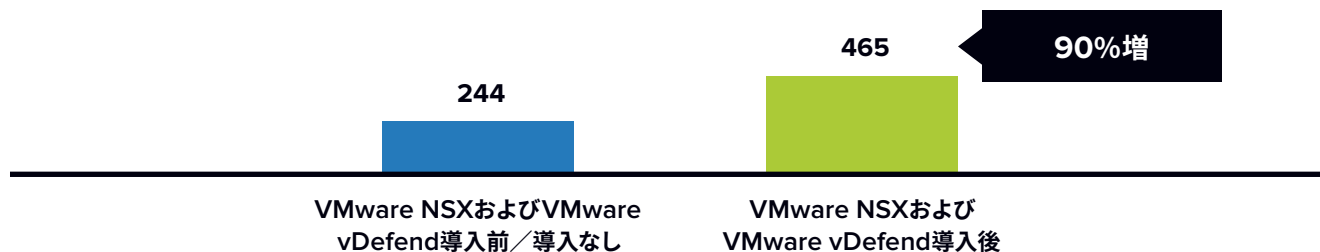
「物理的なファイアウォールの寿命が尽きたら、VMware NSXとVMware vDefendに交換する予定です。それらには現在、VMware NSXやVMware vDefendの数倍のコストがかかっています」

Figure 4 (次ページ) は、調査参加企業がVMware vDefendを使用して、ネットワークのセグメンテーションを進め、より優れたセキュリティの管理を確立および維持していることを示している。平均すると、維持するネットワークのセグメント数はほぼ2倍になったと報告しており、これは、プライベートクラウドネットワーク環境にアクセスする従業員、顧客、その他の関係者に対し、独自のよりきめ細やかなセキュリティポリシーを適用できるようになったことを反映している。

FIGURE 4

ネットワークセグメンテーションへの影響

(1企業当たりのネットワークセグメント数)



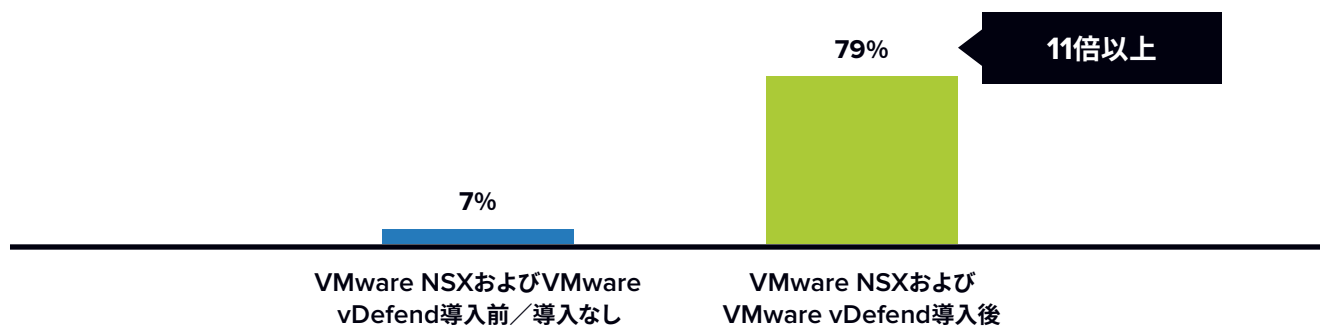
n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Figure 5は、VMware vDefendを使用することで、導入前にはほぼなかった重要なセキュリティ機能が、調査参加企業に提供された主な例を示している。多くの企業にとって、East-Westネットワークトラフィック、つまり、企業のネットワーク環境内のデータや情報の流れは、社外からの通信に比べ盲点になっていることがあまりにも多い。つまり、セキュリティの脅威が社外向けのファイアウォールを突破した場合、その脅威は社内のネットワーク環境内を移動するため、それを隔離して対処するのは困難であることを企業は分かっている。Figure 5に示すように、インタビュー対象のVMwareの顧客は、以前はほとんど保護していなかった(平均7%) East-Westネットワークトラフィックの大部分(平均79%)を保護するようになっている。この11倍以上の対応率の向上は、調査参加企業のセキュリティ機能に対し重要かつ影響力があることを反映したものである。これによって、社内ネットワークに流れるトラフィックに関連するリスクや潜在的な障害を抑えられる。

FIGURE 5

East-Westネットワークのセキュリティへの影響

(East-Westネットワークトラフィックの保護率)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

このようにVMware vDefend Distributed Firewallの強化されたセキュリティ機能と共に、自動化や仮想化のベネフィットも拡大したことで、セキュリティチームはより効率的かつ効果的に業務を遂行できるようになった。ある調査参加企業は、一元管理と単一画面によって、セキュリティ運用がいかに効率的になるかについて次のように述べている。「VMware vDefendではファイアウォールを一元管理できるため、個別ではなく、単一の画面でサーバーをまとめて管理できます。これによって管理が容易になり、管理に必要なスタッフの作業時間も削減されました。12人のスタッフそれぞれで約15%削減しています」Table 4に示すように、インタビュー対象のVMwareの顧客は、VMware vDefendを使用することで、セキュリティチームの効率が平均35%向上したと報告しており、この効率化によって、日常業務に割くスタッフの作業時間を抑えられるだけでなく、すでに説明した強化されたセキュリティ機能のベネフィットを確保し、適用することにも役立っている。

TABLE 4

セキュリティチームの効率

1企業当たりの平均	VMware NSX およびVMware vDefend導入前/ 導入なし	VMware NSX およびVMware vDefend導入後	差	改善率
同じワークロードに必要な 同等のFTE数	21.8	14.1	7.7	35%
必要なFTE時間に 相当する価値 (1企業当たり年間ドル額)	218万ドル	141万ドル	76万6,700ドル	35%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

アジリティと開発のベネフィット

調査参加企業は、VMware NSXとVMware vDefendソリューションを使用することで、アジリティや開発チームの能力の面で大きなベネフィットを得ている。従業員や顧客に新規のソフトウェア機能やアップデートした機能の提供は開発チームが担っている。そのため、開発プロセスを妨げる、ネットワーク、セキュリティ、その他のインフラストラクチャが生み出す摩擦を最小限に抑えるよう努めなければならない。

インタビュー対象のVMwareの顧客は、現在では、チームが新しいアプリケーションや機能のビルド、テスト、デプロイにおいてネットワーキングやセキュリティ、その他のIT機能にアクセスしようとする際に、開発プロセスをより円滑に進めるのに役立つ機能にアクセスできるようになったと述べている。

特に、追加機能の提供や、その際に必要とされるテスト環境やデプロイ環境の構築が全体的に容易であることに加え、各自で機能にアクセスできるところが特に影響が大きかったと述べている。

開発業務の効率化：

「VMware Cloud Foundationの導入によって、開発者はプロビジョニングをすべて自分たちで行えるようになり、インフラストラクチャを待つ必要がなくなったため、生産性が約20%向上しました。〈中略〉現在では、インフラストラクチャ管理チームにDevOpsの手法を導入しています。ネットワークエンジニアは、プログラミングやセキュリティも少し担えるようになり、クラウドエンジニアにより近づきました」

実装時間の短縮：

「VMware Cloud Foundationは、実装時間を短縮しビジネスをしっかりサポートしています。たとえば、開発チームが新しいアプリケーションを導入する必要があるがあっても、インフラストラクチャについてしっかりと理解していない場合でも、VCFを使用すればアプリケーションを迅速に導入し、トラフィックをモデル化し、必要なファイアウォールルールを決定できます。ボタンをクリックするだけで完了です」

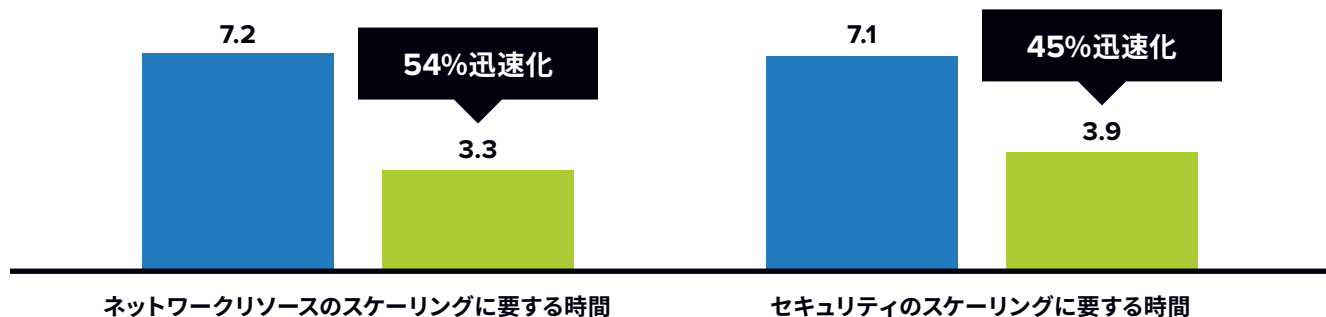
Figure 6は、VMware NSXとVMware vDefendソリューションによって、調査参加企業がネットワーキングやセキュリティの能力を、開発や事業運営の必要に応じて容易にスケーリングできることを示している。インタビュー対象のVMwareの顧客は、平均して、新しいネットワークリソースの提供に必要な時間を54%、新しい環境へのセキュリティの展開に必要な時間を45%短縮できたと報告している。これは、開発プロセスを迅速化し、顧客の需要に合わせて事業運営をスケーリングする上で重要な要素である。

FIGURE 6

アジリティへの影響

(日数)

- VMware NSXおよびVMware vDefend導入前／導入なし
- VMware NSXおよびVMware vDefend導入後



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

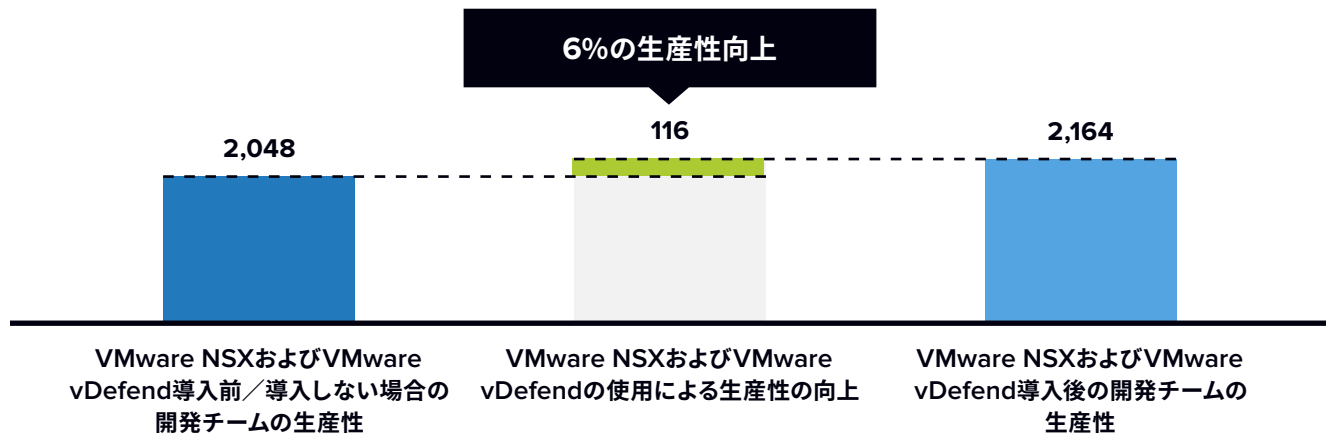
本図におけるデータを分かりやすくした表を見る場合は、補遺3のFigure 6 補足データを参照のこと。

Figure 7は、調査参加企業がVMware NSXとVMware vDefendを使用することで、開発チームの向上という点で大きな価値を得ていることを示している。調査参加企業は、従来型の開発、DevOps、さらにはネットワークやセキュリティ機能へのアクセスの大幅な改善によってベネフィットを得ている事業部門の開発者で構成される大規模な開発チームを持っている。このように、IDCは、平均で2,000人以上の開発者を抱えるこれらのチームが、VMware NSXとVMware vDefendソリューションの導入によって、平均6%の生産性向上を実現できると見積もっている。

FIGURE 7

開発チームの生産性への影響

(生産性換算、1企業当たりのFTE)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

本図におけるデータを分かりやすくした表を見る場合は、補遺3の[Figure 7 補足データ](#)を参照のこと。

運用リスク低減のベネフィット

調査参加企業はセキュリティに関するイベントに関連する直接的なリスクを最小限に抑え、業務の継続性を確保する方法を見つけなければならない。インフラストラクチャの問題によってアプリケーションやサービスが中断されると、従業員はおろか顧客にとっても、業務に大きな摩擦が生じる可能性がある。このような事態が生じると、従業員は日常の業務遂行に支障をきたすだけでなく、顧客とのコミュニケーションも損なわれる可能性がある。

インタビュー対象のVMwareの顧客は、一元管理、パフォーマンスに対する可視性の向上、堅牢な問題解決によって、計画外停止の頻度や影響を低減できたと一貫して述べている。

リスクの大幅な低減：

「VMware NSXとVMware vDefendを使用することで、データセンターで起きていることや、トラフィックをドロップしているIPなども確認できるようになりました。つまり、ネットワーク上で何が起きているのか、実際のトラフィックはどうなっているのか、本当の脅威は何なのかを把握できるのです。VMwareの導入によって、セキュリティ面で大きな改善が見られます」

計画外停止によるビジネスへの影響の軽減：

「VMware NSXとVMware vDefendの導入によって、すべてのインフラストラクチャが一元管理されるため、計画外ダウンタイムの頻度が明らかに減少しました」

Table 5は、VMware NSXとVMware vDefendソリューションの使用が、調査参加企業の計画外ダウンタイムに与える影響に関するIDCの調査結果を示している。以下に示すように、インタビュー対象のVMwareの顧客は、計画外停止頻度を平均58%削減できたと報告している。これは、計画外停止が従業員の生産性に与える全体的な影響を平均43%低減することに寄与している。IDCではこれを金額に換算し、従業員の生産性レベルの向上は、1企業当たり年間平均102万ドルに相当すると評価している。

TABLE 5

計画外ダウンタイムへの影響

1企業当たりの平均	VMware NSX およびVMware vDefend導入前/ 導入なし	VMware NSX およびVMware vDefend導入後	差	改善率
年間の計画外停止数	7.0	2.9	4.1	58%
1ユーザー当たりの 年間生産性の損失	1.2	0.7	0.5	43%
FTE換算による1企業当たり の年間生産性損失	34.0	19.4	14.6	43%
1企業当たりの年間生産性 時間の損失額	238万ドル	136万ドル	102万ドル	43%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

ビジネスベネフィット

調査参加企業は、VMware NSXとVMware vDefendソリューションによって、最終的には事業運営における柔軟性と信頼性が向上し、顧客の需要に対応し、顧客の期待に応えられるようになったと報告している。VMware NSXとVMware vDefendの導入によって、ビジネス機会が訪れた際に迅速に対応し、高品質なサービスを確保し、潜在的なセキュリティインシデントに伴う運用や風評被害のリスクを最小限に抑えられる。あるインタビュー対象のVMwareの顧客は次のように説明している。「VMware NSXとVMware vDefendを使用することで、ビジネス需要に対応するためのスケーリングを約70%高速化できました。ネットワークリソースとセキュリティに以前は数か月かかっていましたが、今は数週間しかかかりません」インタビュー対象のVMwareの顧客にとっては、このように迅速な対応能力が、新規顧客の獲得や収益認識の迅速化に役立っている。

Table 6で示すように、IDCの分析によると、調査参加企業はVMware NSXとVMware vDefendソリューションを使用することで、重要なビジネス成果を着実に達成している。調査参加企業は、年間平均196万ドル（1データセンター当たり15万2,000ドル）の増収が見込まれており、VMware NSXとVMware vDefendソリューションへの投資価値がさらに実証されるとIDCはみている。

TABLE 6

ビジネスインパクト、VMware NSXとVMware vDefendソリューションの活用

	1企業当たり	1データセンター当たり
年間収益増加額	196万ドル	15万2,000ドル
想定営業利益率	15%	15%
年間純収益の増加額	29万3,500ドル	2万2,800ドル

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

ROIの概要

Table 7（次ページ）は、VMware NSXとVMware vDefendソリューションを導入し、使用している調査参加企業の正味のベネフィットとコストに関するIDCの分析結果を示している。IDCは、ネットワークのスタッフとコストの効率化、セキュリティのスタッフとコストの効率化、開発生産性の向上、運用リスクの低減、純収益の増加によって得られる3年間の割引後ベネフィットを、1企業当たり平均3,785万ドル（1データセンター当たり294万ドル）と算出している。これらのベネフィットは、1企業当たりの3年間の割引後平均投資費用の533万ドル（1データセンター当たり41万ドル）に匹敵する。これらのベネフィットと投資コストによって、3年間の平均ROIは610%に達し、インタビュー対象のVMwareの顧客は、平均6か月で損益分岐点を越える。

TABLE 7

ROI分析

	1企業当たりの 3年間の平均	1データセンター当たりの 3年間の平均
ベネフィット (割引後)	3,785万ドル	294万ドル
投資 (割引後)	533万ドル	41万ドル
正味現在価値	3,251万ドル	252万ドル
ROI (NPV/投資)	610%	610%
投資回収期間	6か月	6か月
割引係数	12%	12%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

課題と機会

SDNとセキュリティは過去10年間で大きく進化してきたが、IDCはSDIテクノロジーの主な課題として、拡張性、パフォーマンスの一貫性、強固なセキュリティ、マルチベンダーの相互運用性、レジリエンスを挙げている。

IDCは、SDIテクノロジーの導入に伴う継続的な運用の課題を、VMwareのNSX Network VirtualizationとvDefend Distributed Firewallの機能にとって、新しい機能セットやプラットフォームの性能を活用して戦略的にベネフィットを得られる機会として捉えている。これによって、VMware Cloud Foundationがさまざまなポイント製品アプローチからSDIテクノロジー実装まで、広く差別化されると考えている。

IDCが企業のIT意思決定者を対象に実施した基礎調査によると、GenAIやマルチクラウドネットワーキングなど、新しい長期的な成長の原動力がさまざまな業界で本格的に高まり始めており、一連の機能の差別化は時宜を得たものになっている。

たとえば、VMware NSXとVMware vDefendのIT運用指標は、ITOpsチームが使用する修復とパフォーマンス向上のアプローチに加え、特に「LLMトレーニング」やVCFプラットフォームが生成するデータセットによって大幅に高まる可能性がある。これは、VCFプライベートクラウドプラットフォームと連携するGenAIのアプリを通じて、ITやビジネスの意思決定者に自然言語や画像によるインタラクションを提供する会話型Q&AのUIを提供することである。VMwareは、IT担当者向けの付加価値機能としてこのGenAIアプリケーションの収益化を可能にする。

プライベート/ハイブリッドクラウドの運用モデルとユーザーエクスペリエンスが、パブリッククラウドのフレームワークにおける製品やユーザーエクスペリエンスのイノベーションに対して同等以上であるために、ハイパースケイラーと歩調を合わせることは、Broadcom/VMwareにとっての最優先事項である。これは、世界中の中堅企業や大企業がアプリケーションのモダナイゼーションやデジタルトランスフォーメーションの進捗を加速させる中で、競合他社に先んじてITマインドシェアや顧客内シェアを拡大するためである。

結論

最新のSDDCへの移行は、多くの企業のデジタルトランスフォーメーションの過程で極めて重要な要素になっている。VMware Cloud Foundationは、クラウド管理機能と共に、コンピューティング、ストレージ、ネットワーク、セキュリティのSoftware-Definedサービス一式を提供する包括的なソリューションとして登場した。この統合アプローチは、企業が、プライベート/パブリッククラウド環境に分散型の仮想化やコンテナ化したワークロードを導入する際のセキュリティ、レジリエンシー、管理性、コスト効率に関する課題の対応に役立つ。

本調査レポートでは、VMware Cloud FoundationプラットフォームにVMware NSXとVMware vDefendソリューションを導入することで、企業が達成できる実質的なビジネス価値を明確にしている。本調査結果では、デジタルトランスフォーメーション (DX) とデータセンターモダナイゼーションへの取り組みの迅速化、企業によるクラウドスケールアプリケーションのより効率的な構築/管理の実現、より優れたビジネス成果の創出の実現における最新のSDIの重要性を強調している。インタビュー対象のVMwareの顧客は、VMware NSXとVMware vDefendを使用することで、ネットワークやセキュリティスタッフの効率化、コスト削減、機能の向上などの大きなベネフィットを得ていることを明らかにし、1データセンター当たりの年間平均ベネフィットは124万ドル、それによる3年間の平均ROIは610%になると見込んでいる。

補遺1: 調査方法

本プロジェクトにおいては、IDCの標準的なビジネス価値およびROIの算出方法が使用されている。この方法は、モデルの基盤としてVMware NSX Network VirtualizationとvDefendラテラルセキュリティソリューションを現在使用中の企業から収集したデータを基にしている。

VMware NSXとVMware vDefendを使用する企業とのインタビューに基づき、IDCは以下の3ステップのプロセスによって、ROIと投資回収期間の算出を行った。

1. **VMware NSXとVMware vDefendの使用の影響についての事前／事後評価手法を用いて、インタビューにおいて定量的なベネフィットの情報を収集した。** 本調査では、ベネフィットには、コスト削減、ITスタッフおよび開発チームの効率と生産性の向上、リスク関連のコストの削減、収益の増加などが含まれる。
2. **インタビューに基づいた詳細な投資（3年間の総コスト分析）プロフィールを作成した。** 投資額には、VMware NSXとVMware vDefendの使用にかかる初期費用と年間費用に留まらず、移行、計画、コンサルティング、およびスタッフやユーザーのトレーニングに関連する追加費用も含まれる場合がある。
3. **ROIと投資回収期間を算出した。** IDCは、VCFのネットワーキングとラテラルセキュリティを企業が3年間使用する際のベネフィットと投資額について減価償却キャッシュフロー分析を行った。ROIは、正味現在価値と割引後の投資額の比である。投資回収期間は、累積ベネフィットが最初の投資と等しくなった時点である。

IDCは、次に示されるさまざまな仮定に基づいて投資回収期間とROIの計算を行った。

- 効率化とマネージャーの生産性の節減分を定量化するに当たり、時間の価値として会社負担の給与（給与に福利厚生および諸経費として28%を加算）を乗じた。こうした分析を行うに当たり、IDCは、ITスタッフメンバーの会社負担を含む給与を平均で年間10万ドル、非ITスタッフメンバーの会社負担を含む給与を年間7万ドルと仮定した。また、従業員の年間労働時間は1,880時間（47週間×40時間）と仮定している。
- 3年間の節減分の正味現在価値は、元の金額から、それを12%の利回りの証券に投資した場合に実現されたとあろう金額を減じて（逸失される機会のコストを計算に入れるため）算定する。これによって、想定される資金コストおよび想定される収益率の両方が計算に入れられる。

- IDCは、インタビュー対象企業のVMware NSXとVMware vDefendの使用による総収益の増加に対し、想定純利益率 (15%) を適用しており、その結果、IDCモデルに適用される純収益計算になる。
- VMware NSXとVMware vDefendには導入期間が必要であるため、導入期間においてはソリューションが提供するすべてのベネフィットを得られるわけではない。この事実を反映させるため、IDCではベネフィットを月次ベースで案分し、初年度の節減分から導入期間分のベネフィットを減じている。

補遺2: VMware NSXとVMware vDefendソリューションの使用に関するベネフィットの数値化

Table 8は、調査参加企業がVMware NSXとVMware vDefendソリューションの使用に起因するとしている年間平均価値を詳細に示しており、IDCはその金額が3年間で年間1,600万ドルに相当すると計算している。

TABLE 8

年間平均ベネフィット

価値のカテゴリ	平均定量的ベネフィット	年間平均換算価値*
ITインフラストラクチャのコスト削減	平均70%のコスト削減、年間350万ドルの節約	350万ドル
ネットワークインフラストラクチャチームの効率	平均25%の効率化、5.0 FTEに相当、想定給与10万ドル	42万8,600ドル
セキュリティチームの効率	平均35%の効率化、7.7 FTEに相当、想定給与10万ドル	65万5,000ドル
トラブルシューティングチームの効率	平均31%の効率化、4.8 FTEに相当、想定給与10万ドル	41万4,000ドル
開発チームの生産性向上	平均6%の生産性の向上、116 FTEに相当、想定給与10万ドル	988万ドル
ユーザーの生産性向上、ダウンタイム	計画外ダウンタイムを43%削減、1ユーザー当たり0.5時間の生産性向上、1企業当たり14.5 FTEに相当、想定給与7万ドル	86万8,200ドル
純収益の増加	年間196万ドルの収益増加（想定マージン15%）	25万800ドル
1企業当たりの総年間平均ベネフィット	1,600万ドル	

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

*初年度5.2か月の導入期間を含むデータ

Note: 本調査レポートに含まれる数値はすべて四捨五入などの影響によって、合計値が一致しない場合がある。

補遺3：補足データ

本補遺は、本書の複雑な数字のデータを分かりやすく表にしている。表の下の「元の図に戻る」をクリックすると、対応する元のデータ図に戻る。

FIGURE 1 補足データ

1データセンター当たりの年間平均ベネフィット

	1データセンター当たりの 年間平均ベネフィット (ドル)
ITスタッフの生産性ベネフィット	88万3,800ドル
ITインフラストラクチャのコスト削減	27万2,200ドル
ビジネス生産性とリスクの軽減のベネフィット	8万6,900ドル
合計	124万ドル

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

[元の図に戻る](#)

FIGURE 3 補足データ

3年間の運用コスト

	インフラストラクチャ/ VMware VCFネットワーキング とラテラルセキュリティのコスト	スタッフの作業時間のコスト (インフラストラクチャ、 セキュリティ)
VMware NSXおよびVMware vDefend 導入前／導入なし	116万4,400ドル	82万6,300ドル
VMware NSXおよびVMware vDefend 導入後	34万7,800ドル	57万3,300ドル
合計	199万ドル	0.92ドル (54%削減)

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

[元の図に戻る](#)

補遺3: 補足データ (続き)

FIGURE 6 補足データ

アジリティへの影響

	VMware NSXおよびVMware vDefend導入前／導入なし	VMware NSXおよびVMware vDefend導入後
ネットワークリソースのスケーリングに要する時間	7.2	3.3
セキュリティのスケーリングに要する時間	7.1	3.9
差	54%迅速化	45%迅速化

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

[元の図に戻る](#)

FIGURE 7 補足データ

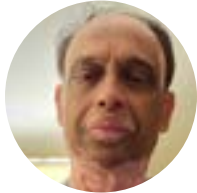
開発チームの生産性への影響

	生産性に相当、1企業当たりのFTE
VMware NSXおよびVMware vDefend導入前／導入しない場合の開発チームの生産性	2048 FTE
VMware NSXおよびVMware vDefend導入後の開発チームの生産性	2164 FTE
VMware NSXおよびVMware vDefendの使用による生産性の向上	116 FTE
差	6%の生産性向上

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

[元の図に戻る](#)

IDCのアナリストについて



Vijay Bhagavath

リサーチバイスプレジデント、Cloud and Datacenter Networks

Vijay Bhagavathは、IDCのCloud and Datacenter Networks担当のリサーチバイスプレジデントである。Vijayは、実践的なソートリーダーシップを発揮し、クラウドやデータセンターネットワークの市場やテクノロジーに関して実用的なインサイトを提供している。また、ネットワークの市場、テクノロジー、製品ロードマップ、競争上の差別化、および導入戦略を全体的に深く理解しており、ベンダー、クラウドプロバイダー、企業ITのバイヤーや専門家に対して、洞察力に富んだコメントや助言を提供している。

[Vijay Bhagavathの詳細についてはこちら](#)



Matthew Marden

リサーチバイスプレジデント、Business Value Strategy Practice

Matthewは、さまざまなテクノロジー分野の顧客に対して、ビジネス価値に関するカスタム調査やコンサルティングプロジェクトの実行を担当し、エンタープライズにおけるテクノロジー使用のROIの決定に注力している。Matthewの調査では、多くの場合、効率化やビジネスイネーブルメントを通じて価値を創出するために、企業がいかにしてデジタル技術のソリューションや取り組みへの投資を活用しているかが分析されている。

[Matthew Mardenの詳細についてはこちら](#)

IDC Custom Solutions

本調査レポートはIDC Custom Solutionsが発行したものです。本調査レポートに記載する見解、分析、調査結果は、ベンダースポンサーの記載がない限り、IDCが独自に行い、発行した詳細な調査と分析から導き出されたものです。IDC Custom Solutionsは、さまざまな企業による配布に対応するため幅広いフォーマットでIDCのコンテンツを提供しています。このIDCの資料は、外部使用を目的としてライセンスされたものであり、IDC調査結果の使用または公表は、スポンサーまたはライセンシーの製品または戦略に対するIDCの支持を示すものではありません。



IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

[idc.com](https://www.idc.com)

[in @idc](#)

[X @idc](#)

International Data Corporation (IDC) は、ITおよび通信分野、消費者向けテクノロジー市場に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です世界中に1,300人以上のアナリストを擁するIDCは、110か国以上を対象として、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っていますIDCの分析と洞察は、IT専門家、企業経営者、および機関投資家が客観的にテクノロジー導入の意思決定を行い、主要な事業目標を達成するのに役立ちます。

©2024 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)

