O'REILLY®
Report

OS選択の再定義

Linux戦略を見直し、競争上の優位性に変える

Ned Bellavance および Chris Hayner
共著

提供：
Red Hat

Red Hat
Enterprise Linux

OS の選択を競争上の優位性につなげる

迅速なイノベーションには先進的なプラットフォームが必要です。アジリティと制御性に優れた Red Hat Enterprise Linux なら、進化するニーズに対応できます。

さらに詳しく

OS選択の再定義

Linux戦略を見直し、競争上の優位性に変える

Ned Bellavance およびChris Hayner 共著

O'REILLY®

OS選択の再定義

Ned Bellavance および Chris Hayner 共著

O'Reilly Media, Inc. (141 Stony Circle, Suite 195, Santa Rosa, CA 95401) 発行。

O'Reilly の書籍は、教育用、ビジネス用、販促用に購入できます。ほとんどのタイトルでオンライン版もご用意しています (*http://oreilly.com*)。詳細については、当社の企業/教育機関向け営業部門 (800-998-9938)、または *corporate@oreilly.com* までお問い合わせください。

企画編集: Megan Madusaw
開発編集: Gary O'Brien
制作編集: Jonathon Owen
校閲: Stephanie English
表紙デザイン: Ellie Volckhausen
本文デザイン: David Futo
本文イラスト: Kate Dullea

2026 年 2 月: 第 1 版

第 1 版の改訂履歴

2026 年 2 月 13 日: 初回リリース

979-8-341-66786-0

[LSI]

目次

はじめに

従来、組織においてはオペレーティングシステム (OS) のデプロイ戦略を変更するのに時間がかかっていました。企業の運営は単純な技術的要件と好みに基づいており、どうしても必要な場合にのみ複数の OS が使用されていました。重要なアプリケーションの技術的要件や、サポート終了を迎える OS の強制アップグレードによって、変更が必要となることもありました。そのため組織は、OS の選択は解決済みの問題である (まず何よりも、技術的に必要である) と考えるようになりました。実際には、先進的かつグローバルなテクノロジー環境の急速な進化により、OS の選択が戦略的に不可欠なものに変わりつつあります。

今日の企業は、これまで経験したことのない急速な変化に直面しています。わずか数年の間に、コンテナ化などのテクノロジーによってワークフローの柔軟性が向上し、アプリケーション・デプロイのツールセットと戦略は一変し、AI や量子コンピューティングなどのテクノロジーによってあらゆる常識が完全に覆されました。企業がテクノロジーのニーズを再評価する際には、こうした激動の時代に合わせてOS の選択戦略も見直す必要があります。

このレポートでは、OS の選択が新たな戦略的優先事項となった要因を検証します。また、アンケートやアナリストレポートなどの実証的調査に基づいて、現代の IT 組織が直面している具体的な課題を明らかにします。これから説明するように、さまざまな戦略的かつ先進的な要因がこうした変化をもたらしています。新しいアプリケーション、ハードウェア、プラットフォームはすべて、イノベーションを加速させる

ものでなければなりません。イノベーション以外についても、組織は、不確実な経済情勢、サイバーセキュリティに対する先進的かつ高度な脅威、データ主権やサプライチェーンの検証などの地政学的問題にも対処する必要があります。

企業の OS 選択に対する考え方が、運用上の義務から、競争力をもたらす戦略的取り組みへと変わりつつある現状について説明します。

第1章

OSの選択における戦略的変化

先進的な IT 環境によって生じるさまざまな要件により、企業における OS インフラストラクチャおよびアプリケーション・デプロイ戦略は根本的に変わりつつあります。何も変わらず、見直しもされていない OS エコシステムの従来のメリット (管理とデプロイの単純化、トレーニングの必要性が低いなど) が、現代の進歩のスピードを踏まえて再点検されています。組織は、柔軟性に欠ける OS は強みではなく欠点であることを認識し始めており、現状維持よりも、柔軟性と迅速な機能拡張が重要となっています。こうした方針転換を検討していない企業は、より準備が整った柔軟な競合他社に後れを取るリスクがあります。また、調達の決定に直接影響を与える地政学的要因によって、急速に変化するテクノロジー環境がさらに複雑になっています。

主要なテーマと変更点

現在、複数のテーマが企業における OS の選択に大きな影響を与えています。それぞれが独立したトレンドというよりは相互に連携し、企業のインフラストラクチャ戦略に対する取り組みを再定義しつつあります。各テーマについては、このレポートの後半で詳しく説明します。

OS 選択の決定に最も大きな影響を与えているのが、*イノベーションの加速*です。簡単に言えば、AI、自動化、エッジコンピューティングとクラウドコンピューティング、IoT、新しいカスタムハードウェアなどが、企業が対応できないほどのスピードで進化しています。テクノロジーがかつてない速さで進化するなか、企業は技術的負債を懸念してい

ます。以前は、先進テクノロジーの本稼働まで数年を要していましたが、今では数カ月で構想からデプロイまで進めることができます。これが、企業が競争力を強化するためにOSを探している主な要因です。

サプライチェーンに関する*世界的な不確実性*は年々高まっており、企業は自社のローカル環境だけでなく、利用しているツール、ソフトウェア、サービスを提供するサプライチェーン全体に目を向けることが重要になっています。多くの企業は、サプライチェーンが寸断する可能性を踏まえ、単一ベンダーとの関係、特に外国企業との関係を潜在的なリスクと認識するようになりました。こうした懸念から、ベンダーの多様化は、リスク軽減策であると同時に戦略上不可欠なものとなっています。

最適化と投資対効果（ROI）が重視されるようになり、*経済的な圧力*も高まっています。ROI は資金面だけではありません。スキル不足も、OS の選択を複雑にする予算の制約と同程度に問題となっています。以前は、1 人の管理者が複数の OS のエキスパートであることはほとんどありませんでした。単に企業にとって、複数の高度なエキスパートを雇用することが現実的ではなかったからです（これも単一の OS 環境がデフォルトとなっていた理由の 1 つです）。このため、実証可能な OS の使いやすさが優先事項となっています。

*セキュリティ上の懸念*から、インフラストラクチャの要件が再定義されています。多くのシステムが従来よりも短時間でデプロイされるようになり、企業の攻撃対象領域が劇的に増加しています。また、AI の導入、先進的なサイバー脅威、規制遵守という新たな環境には、先進的なアプローチが必要です。

そして最後に、*AI* によって、コンピュータの利用に関するこれまでの常識がすべて覆されています。管理者や開発者が大規模言語モデル（LLM）を利用して新しいアプリケーションを作成するスピードも、飛躍的に向上しました。単に LLM に接続して質問する場合でも、独自のチャットボットを作成する場合でも、高度なエージェント型 AI ツールを構築する場合でも、その作業に最適な OS が必要です。

OS 選択の重要性

これまで見てきたように、OS の選択に影響する要素は増加する一方です。不適切な OS を選択すると、重要な AI 機能へのアクセスが制限され、パフォーマンスが損なわれ、組織がセキュリティリスクやサプライチェーンの脆弱性にさらされる可能性があります。反対に、適切な OS を選択すると、ハイペースで先進的、かつ生産性の高い環境に移行するための足がかりとなります。OS を注意深く戦略的に選択することで、競争上の優位性とデジタルにおける柔軟性が向上します。これらはいずれも、先進テクノロジーがもたらす機会の活用を目指す企業にとって不可欠です。

では、選択に影響を与える各要素について詳しく見ていきましょう。

イノベーションの加速

絶え間ないテクノロジーの進歩に伴い、インフラストラクチャの決定に関する標準モデルも大きく変化しています。このセクションでは、これらの加速要因と、それらの要因によりデプロイ戦略に対する取り組みがどのように変化しているかについて説明します。

テクノロジーサイクルの短縮

2025 年版 McKinsey Technology Trends Outlook レポートによると、「世界のテクノロジー環境は、急速に変化するテクノロジーのイノベーションによって、大きな変化を遂げている」ということです。[1]つまり、テクノロジーは、これまで経験したことのないペースで発展しており、そのペースは今後も加速する見込みです。たとえば、クラウド導入のペースを考えてみると、多くの企業は導入までに時間を要しており、開発/テスト環境をクラウドにデプロイしてから、徐々に数年かけて本番ワークロードに移行していました。次に、生成AI（GenAI）やエージェント型 AI について考えてみると、こちらは、思考実験から企業向けの製品化まで数カ月で完了しています。

[1] McKinsey & Company、「McKinsey Technology Trends Outlook 2025」、2025 年 7 月 22 日、*https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top- trends-in-tech*

従来のインフラストラクチャ戦略では、企業は既存の OS を活用し、新しいテクノロジーをその OS 内で機能させる方法を模索していました。現代のグローバル市場は目まぐるしく変化しているため、これでは対応できません。開発チームは、古いインフラストラクチャを改良して機能させようとするのではなく、新しいプラットフォームを試して、最新のテクノロジーと最も相性のよいプラットフォームを探すようになっています。これが OS を試す大きな原動力となっており、既存の OS が開発者やエンジニアのニーズに対応できないのであれば、ニーズに対応できる OS を探し始めることになります。

ターゲットを絞った投資

OS の見直しと変更の最大の原動力が、新しいテクノロジーです。これは前述の傾向を反映しており、開発者や管理者は、社内で気に入っているインフラストラクチャを使い続けるよりも、最高水準のインフラストラクチャを求めています。とはいえ、組織は無制限にリソースを使おうとしているわけではありません。最初は、限られた資金を適切な方法で使用したいという強い要望があります。OS の選択は、単に 1 台のサーバーについてではなく、はるかに大規模なプラットフォームの一部としての判断であるため、投資の意思決定が一層重要になります。

こうした投資は、ビジネスニーズを満たすために行われます。テクノロジーは進歩しており、組織はその進化に対応していく必要があります。たとえば、AI 機能には専用のインフラストラクチャと開発ツールが必要であり、標準の OS では対応できない場合があることが認識され始めています。企業は、AI ツールのニーズに対応するためだけに、GPU ベースのサーバーの大規模なファームを構築せざるを得ませんでした。先進的な組織はイノベーションのペースを認識し、インフラストラクチャの可能性を最大限に高めるために戦略の見直しを図っています。企業は、テクノロジーをデプロイして最善の結果を期待するだけではなく、確実に最大の価値を引き出せるように迅速に進化したいと考えています。

世界的な不確実性

世界的な不確実性が、テクノロジー戦略に影響を及ぼす要因となっています。経済的な懸念につながる地政学的緊張が、近年にないレベルで意思決定に影響を与えるようになっています。そのため、組織は技術的なニーズだけでベンダーを検討することができなくなり、地政学的な留意事項を踏まえた判断が求められています。こうした不確実性について組織が抱える懸念が、これまでになく高まっています。[2]組織は、関税や規制、輸出規制についても考慮する必要があります。地政学的緊張は継続的かつ不確実であり、グローバル・サプライチェーンを脅かし、企業がテクノロジー・エコシステムを国内に留める動きにつながります。

関税と輸出規制

関税への懸念と、それによって生じる為替変動により、国外調達に対する企業の考え方も変わりつつあります。長期契約の場合、激しい変動が生じて 2 国間の為替レートが変わると、締結から 1 年後には想定外の内容となる可能性があります。このことが、現在の IT 戦略全体を脅かす重大な問題となっています。ベンダーを選択する際にこうした経済情勢も考慮するという点が、IT の購買決定に関するこれまでの考え方とは大きく異なります。

デジタル主権

地政学的な圧力は、経済面だけにとどまりません。国ごとに異なる規制要件があり、顧客とベンダーの力関係が変化しています。この傾向は、クラウドコンピューティングの分野で最も顕著に表れています。クラウドコンピューティングでは、一般データ保護規則（GDPR）などの規制上の懸念により、企業はデータが EU 内に留まることが保証される「EU 限定」クラウドを強く求めています。長年にわたる論争の末、多くの企業が、特定の規制上のニーズに対応できるクラウドベンダーを積極的に探すようになりました。

---

[2] McKinsey & Company、「Navigating the New Geopolitical Uncertainty」、2025 年 1 月 16 日、*https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty*

経済的不確実性

経済的な圧力は、常に IT に影響を与えてきました。変化のスピードと世界的な圧力が相まって、状況はさらに複雑になっています。使える資金が限られており、スキル不足も問題となっているため、新たな管理者を採用することが資金面では可能でも、人材が見つからない場合があります。

予算の制約により、OS 選択における最大の決め手がコストの最適化になりました。企業は ROI と支出効率をますます重視するようになっています。コストの最適化に重点が置かれることが、財務負担と ROI の両面で OS 選択に影響を及ぼしています。

セキュリティとデータ侵害

IT 資産のセキュリティは長年にわたって最大の懸念事項となっており、Stack Overflow による 2025年開発者アンケートなどの調査では、開発者にとっての最優先事項がセキュリティ、脆弱性分析、テストであることが明らかになっています。開発者が特定のテクノロジーの使用を止めた理由としてトップに挙げられたのが、「セキュリティとプライバシーに関する懸念」でした。

サプライチェーン攻撃

ソフトウェアの出所を把握することは全体の一部にすぎません。企業はこれまで以上に、ソフトウェアの依存関係の出所についても把握する必要があります。これ自体がセキュリティ上の問題になる可能性があります。主要なソフトウェア製品にとって重要なマイナーパッケージが侵害された場合、組織はリスクにさらされるからです。おそらく最も有名な例は、2021 年の SolarWinds のハッキング事件です。このハッキングでは、安全でない SolarWinds サプライチェーンにより、SolarWinds の多数の顧客がデータ侵害のリスクにさらされました。それでもまだ、依存関係の問題は散見されています。最近では、JavaScript レジストリ npm がサプライチェーン攻撃を受けたことにより、ユーザーのデバイスに安全とみなされて展開されたパッケージが暗号通貨のマイニングに悪用されました。

AI はセキュリティ上のリスクであると同時に、生産性やビジネス機能にメリットをもたらすことが証明されています。AI を利用した攻撃はここ数年で急増しており、その勢いが衰える兆しはありません。信用調査機関である Experian による最近のレポートでは、2026 年には AI が、データ漏洩においてヒューマンエラーを上回る最大の要因となる見込みです。[3]

量子暗号化に対する懸念

ここ数年で量子コンピューティングによって生じる新たな脅威が特定され、調査されてきました。懸念されるのは、量子コンピュータは従来の暗号化の問題に対してまったく異なるアプローチをとるため、最終的に (10 年以内に実現される可能性が高いものの、その時期については議論の余地あり)、既存の暗号化アルゴリズムがすべて数秒で破られる可能性があるということです。この場合、「従来の方法で」暗号化されたファイルやデータストアは完全に脆弱になります。ハッカーたちはこの点を認識し、今はまだ暗号を解読できなくても、可能な限り多くのデータをダウンロードしています。このセキュリティリスクは、「Harvest now, decrypt later (今収集し、後で解読)」と呼ばれます。

ポスト量子暗号化 (PQC) とは、量子コンピュータの能力に耐えられるように設計された次世代の暗号化を指します。この種の暗号化は、コンピュータサイエンスにおける先進的な研究課題の 1 つであり、まだすべての OS が活用しているわけではありません。PQC アルゴリズムを使用したテクノロジーの暗号化とは、ハッカーが今収集して後で解読することは不可能になるということです。

AI

AI は、多くのテクノロジーの購買決定を後押しする最大の要因となっています。この傾向は以前から明らかになっていましたが、その勢いは衰えることがありません。しかし、OS を取り巻くテクノロジーと同様に、AI が OS 選択の決め手となるケースが増えています。

---

[3] Experian、「2026 Data Breach Industry Forecast」、2025 年 12 月 5 日、*https://www.experian.com/thought-leadership/business/2026-data-breach-industry-forecast-report*

バイブコーディング

AI の登場により、OS の先進的なユースケースも変化しています。プログラミング、データ分析、ビジネス分析は、専門知識や技術知識がなくても利用できるようになりました。たとえば、バイブコーディングは、プログラマーやアプリケーション開発者でなくても、AI を活用してアプリケーションを作成できる手法です。このような作業を助ける AI 支援開発ツールと連携できる OS が市場で選ばれるケースが増えています。

ハードウェア・アクセラレーション

もちろん AI は、広範な OS 機能を必要とする従来型のユースケースもサポートしています。推論、モデルのトレーニング、LLM ベースのチャットボットのホスティングなどのタスクを実行するには、OS が GPU や他のカスタムハードウェアと効果的にやり取りできなければなりません。専用チップにより、さらに高速で大規模かつ汎用性の高い AI 機能が可能になるため、ハードウェアの互換性も重要な選択理由になります。AI を活用した自動化および管理機能は、OS が利用できるハードウェアリソースにも引き続き負担をかけることになります。そのため、OS が先進的ハードウェアに対応しているかどうかが OS の選択に影響します。

まとめ

市場の破壊的革新によって組織が OS の選択を見直す必要性が高まったことで、新たな可能性を模索する戦略的な機会が生まれています。組織は、この世界的な混乱とイノベーションの爆発によってもたらされる、これまでにない機会を認識し始めています。変化に対応できない既存のプラットフォームに固執するのではなく、新たな機会をますます積極的に模索するようになっています。このように OS の選択を義務から機会に変えることは、ビジネス運用を強化する最も重要な機会の 1 つでもあります。これまでどおりではなく、変化の波の中で業務に最適なツールを見つける必要があります。

第 2 章

問題と解決策

第 1 章では、OS の選択に影響を与えるいくつかの重要な要因 (イノベーションの加速、世界的な不確実性、経済的な圧力、セキュリティ上の懸念、AI の需要) を明らかにしました。しかし、こうしたプレッシャーを認識することは、始まりにすぎません。IT リーダーが直面している課題は、新たに運用上の混乱や脆弱性を招くことなく、こうしたプレッシャーに効果的に対応するにはどうすればよいかということです。成功している組織は、こういった問題を認識したうえで、生産性が高く競争力のある方法で対応します。この章では、それぞれの課題について解説し、問題を解決する方法について説明します。

イノベーション加速戦略

イノベーションの加速は、IT リーダーの意思決定に大きな影響を与える要因となっています。競合他社に後れを取らないためだけではありません。先発優位などの考え方により、最も迅速に対応できる組織が最大の報酬を獲得する傾向があります。こうした考え方が OS の選択戦略にも大きな影響を与えています。OS は、組織が実現しようとしているイノベーション加速の基盤となるからです。このようなイノベーションは企業を未知の領域へと導くため、慎重になり、明白なニーズとメリットに基づいて判断することが重要です。イノベーションの加速とは、思い付きで変革を進めることではありません。先進的な OS は、セキュリティ、パフォーマンス、信頼性を確保しながら、実験をサポートする必要があります。

入念な実験を迅速に実施

テクノロジーのイノベーションが加速する中、従来の開発方法や評価方法ではそのスピードに対応できなくなっています。アプリケーション開発の世界では少し前からこうした傾向が続いており、ウォーターフォールベースの年次リリースサイクルから、アジャイルベースのソフトウェア開発や DevOps ベースの継続的デリバリー、さらには毎日複数のアップデートが提供される最新のハイパーファスト・デプロイメント・モデルへの移行が進んでいます。これと同じ傾向がテクノロジー業界全体に見られ、IT リーダーは時代の先を行くためにこの動きに追従する必要があることを理解しています。

このようなイノベーションのスピードに対応するには、開発とテストを短期間で繰り返し行いつつも、セキュリティのベースラインを維持し、ビジネスをリスクにさらさないようにしなければなりません。効果的な実験には、企業データ (やアプリケーションをホストする OS) のセキュリティを維持しながら本番環境と同様の条件を再現できる、高度なサンドボックス環境が必要です。これは、実際の本番環境の条件下での迅速なパフォーマンス評価に使用できる、現実的なテスト環境を用意する場合に最も効率的な方法です。

同様に、アプリケーションにも、テストから本番環境までの迅速で信頼性の高いルートが必要です。これは、テストで実証済みのアプリケーションが本番環境で確実に動作できる、シームレスなプロセスである必要があります。使いやすさだけではなく、アップグレードが最初のテストデプロイ並みに効率的 (かつ安全) に行えるという信頼性と再現性が重要です。

この点を考慮すると、OS の選択プロセスに対して慎重でありながらもオープンな考え方を維持することには明らかな価値があります。イノベーションが加速している時代にアジャイルであることは、明確な戦略上のメリットです。OS は最終的に対象のアプリケーションをホストするものですが、アプリケーションの要件は急速に変化しており、組織は OS がそうした要件に対応できることを確認する必要があります。この繊細なアプローチは、IDC や McKinsey などの企業による調査と分析によって裏付けられています。2024 年 6 月に McKinsey は次

のように述べています。「万能のアプローチは存在しません。それでも企業は、堅牢で信頼性の高い技術インフラストラクチャを維持しながら、イノベーションを追求することができます」。[1]

とはいえ、ツールやテクノロジーの選択は慎重に行う必要があります。「変更のための変更」にはリスクが伴います。OS のように基本的なものがチェックも受けずに変更されてしまうと、明白なメリットも得られずに複雑さが増すことになります。このような変更を正当化する最も強力な証拠は、組織の機能に関して明確なメリットがあることを示すものです。こうしたメリットは、単に新しいからという理由で新しい OS を導入するだけでなく、実証可能なものである必要があります。これに関しては、組織は現在の機能だけでなく、OS の将来的な可能性と安定性にも目を向ける必要があります。

セキュリティ重視のアーキテクチャ

テクノロジーのイノベーションが加速していることで恩恵を受けているのは、正当な企業だけではありません。サイバーセキュリティ脅威は進化し続けており、組織全体のセキュリティを確保しなければ、攻撃に対して脆弱な状態になります。CrowdStrike の *2025 年版世界の脅威レポート*などの市場調査により、サイバー脅威がサイバー防御の進化を上回る速さで進化し続けていることが明らかになりました。この先進的な脅威環境が、前例のない、絶えず進化する課題をもたらしており、従来のセキュリティ・フレームワークや IT ツールでは対処できなくなっています。このような先進的な脅威に対処する準備をしておくことが、戦略的に不可欠となっています。

新しい OS の導入を検討する際には、こうしたセキュリティ・アーキテクチャを考慮する必要があります。OS の選択プロセスにセキュリティに関する質問や検証を取り入れていない組織は、システムでホストされているアプリケーションと、システム自体のセキュリティと信頼性と

[1] McKinsey、「Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure-ture」、2024 年 6 月 26 日、*https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure*

いう二重のリスクに直面しています。この傾向は、本書の執筆時点においては特に顕著です。OS ベンダーが OS に AI 機能を追加し、膨大な量のアクセスを可能にしてシステム管理タスクを自動的に実行できるようにするケースが増えているからです。

データセキュリティは不可欠

最も重要な点は、すべての OS が、アプリケーションを安全に実行してデータを安全に保存できる環境を提供する必要があるということです。企業は、OS の組み込みコンポーネントか、OS がホストするアプリケーションかを問わず、実行されているすべてのものが安全であることを確認しなければなりません。データセキュリティの次の 3 つのカテゴリを考慮する必要があります。

保存データ
: 将来使用するために保存されているデータ。

転送中データ
: システム間かシステム内かを問わず、アプリケーション間で何らかの方法で転送されているデータ。

使用中データ
: コンピューティング・プラットフォームで処理中のデータ。

保存データと転送中データの保護は、通常、暗号化によって解決できます。使用中データの保護は、それよりも困難です。先進的な OS アーキテクチャは、信頼できる実行環境 (TEE) を組み込むことでこの問題を解決しています。これは、信頼性の高いソフトウェアに限定され、厳密に制御されたメカニズムを通じてのみアクセスできるシステムの一部です。TEE 内で実行されるものは、通常、TEE の外部からアクセスすることはできません。ハードウェアベースのソリューションとソフトウェアベースのソリューションの両方があり (通常は複数のサーバーに拡張されます)、機能を維持するにはドライバーと互換性を最新の状態に保つ必要があります。実際にどのようなものであるかはベンダーによって異なり、このレポートの範囲外ですが、このような安全な環境でアプリケーションを実行できることを確認することが極めて重要です。

AI ワークロードは保護するだけでは不十分

あらゆる種類の計算ワークロードには前述したデータ保護とデータ主権保証が求められますが、AI ワークロードは新しく、データ集約型であり、計算が複雑であるというさらに 2 つの理由により、特に脆弱です。

AI ワークロードが新しいということは、本番ワークロードはまだ標準ワークロードほど時間をかけて徹底的にテストされていないことを意味します。セキュリティは共同作業であり、市場では、個々のベンダーが単独で行えるものよりもはるかに多くのテストと QA が行われることになります。このことは、製品自体にも、製品の構成方法や使用方法にも当てはまります。Tenable は、「*Tenable Cloud Security Risk Report 2025*」において、AI をサポートしているクラウドワークロードは他のワークロードよりも脆弱性が高いと報告しています。ワークロードがホストされる場所に関係なく、AI のデータ集約型という性質と、繰り返し発生する構成ミスや脆弱性により、サイバーセキュリティに関してはこれまで以上に細心の注意を払う必要があります。

OS を評価する際には、AI 固有のリスクを考慮する必要があります。これを怠ると、現在および将来のワークロードを危険にさらす可能性のある、未知のレベルのリスクを招くことになります。

まとめ

OS に関する意思決定を計画的に行うには、組織におけるテクノロジーの評価方法を根本的に変える必要があります。この章で取り上げた課題は、適切な選択を行って競争上の優位性を最大限に高めるために必要な仕組みを示しています。このレポートでは、これらすべての意思決定を網羅した意思決定のフレームワークについて検討します。現時点で、OS のデプロイに関して新しい考え方が必要 (先進的な課題の解決には先進的なソリューションが必要) であることは明らかです。この課題に取り組み、戦略的に思考する組織は、より有利な立場で新しいテクノロジーを活用し、競争上の優位性を最大限に高めることができます。

第3章

先進的なLinuxプラットフォーム

先進的な企業は、サーバー運用の大部分を Linux で標準化しています。このことは、少なくとも過去 10 年間にわたり、多数の調査で裏付けられています。たとえば、2025 年 8 月に公開された SQ Magazine によると、大企業の 61.4% が Linux で少なくとも 1 つのミッションクリティカルなワークロードを実行しており、インターネット向け Web サーバーの 78.3% が Linux を実行しています。[1]この優位な地位は、長年にわたる成長の結果であり、この傾向が衰える兆しはありません。

しかし、こうしたレポートでは個々のディストリビューションについて言及されないケースが多く、多くの意思決定者は「どの Linux でも同じ」と考えがちですが、それは誤りです。すべての Linux ディストリビューションは基本的な Linux カーネルを使用していますが、カーネルのデプロイ方法やカーネルを中心とするツールおよびアプリケーション・エコシステムは、大きく異なる場合があります。

組織に必要なのは、評価対象となる OS の重要な差別化要因を見極めることです。多くの先進的 OS は最先端の機能を進化させてきましたが、OS によって機能の扱い方が異なる場合があり、限られた場所でしか利用できない機能もあります。注目すべき最も有益な機能としては、先進的なセキュア・デプロイメント・モデル、AI 統合システムツール、フリート管理ツール、エンタープライズグレードのセキュリティ、広範なサポートおよびパートナー認定などがあります。さらに、OS の機能は、そ

[1] Robert A. Lee 氏、「Linux Statistics 2025: Desktop, Server, Cloud & Community Trends」、*SQ Magazine*、2025 年 11 月 18 日更新、*https://sqmagazine.co.uk/linux-statistics*

の OS で実行されるホスト型ワークロードの要件、つまり先進的な要件を満たす最高水準の機能を考慮して検討する必要があります。

OS デプロイの変革

OS のデプロイに関しては、長年にわたって大きな変化はありませんでした。従来のデプロイでは、何らかのインストーラーによってカーネルなどのツールがハードディスク上に階層化され、その後ユーザーによってアプリケーションがインストールされていました。パッケージ管理の登場は、アプリケーション管理とシステム管理において大きな飛躍となりました。それによってユーザーが、アプリケーションのインストールやアップデートのたびにコードをゼロからコンパイルする必要がなくなったためです。

先進的な Linux ディストリビューションは、基本的にはシステムが必要に応じて交換可能なイミュータブル・コンテナとなるデプロイメントモードを提供する必要があります。ユーザーは新しいイメージをダウンロードできます。また、簡単な再起動だけで、変更するシステムのあらゆるコンポーネントをアップグレード (またはダウングレード) できます。これにより、セキュリティと信頼性が確保され、フリート内のすべてのシステムが、すべてのバイナリーとライブラリの想定されたバージョンを実行しているという確信が得られます。

作成されたイメージは、アプリケーション・コンテナ (またはイメージ) と同じ方法で管理できますが、より小規模 (バイナリーや OS カーネル自体も) になります。この点は、以前のパッケージベースのアップデートモデルから大幅に改善されています。パッケージは、ソースからコンパイルする場合に最も優れたデプロイメントモデルですが、互換性、パッケージの要件、バージョンが競合するリスクに関して固有の問題があります。コンテナベースのモデルでは、すべてがイメージに含まれるため、これらの懸念が解消されます。コンテナ内のあらゆるもののバージョンの一貫性が保たれるため、構成ドリフトに関して多くのシステム管理者が抱える懸念が大幅に軽減されます。また、イメージのインストールをはるかに短時間で簡単に行えるようになっており、イメージをダウンロードして適用し、再起動するだけで済みます。

イメージはイミュータブルであるため、セキュリティ上のメリットもあります。これは、悪意のある攻撃者やマルウェアがイメージをその場で変更したり、差し替えたりできないということです。これらのイメージはアプリケーション・コンテナとほぼ同じ方法で管理されるため、Podman などの標準的なコンテナツールや多くの一般的なコンテナプラットフォームでイメージを確認できます。ツールが一般的なものであれば、アプリケーション・コンテナに精通している管理者は、OS イメージを迅速かつ確実にデプロイできます。

最後に、作成したイメージはどこでも使用できます。デプロイ先が物理、仮想化、クラウド、エッジのいずれであっても問題ありません。イメージはどこでも同じ方法でデプロイされ、実行されます。イメージを最初から最後まで管理することも容易になります。図 3-1 は、イメージのビルド、イメージのデプロイ、デプロイ後のイメージの管理という簡単な 3 ステップで行われるイメージモード・プロセスの例を示しています。

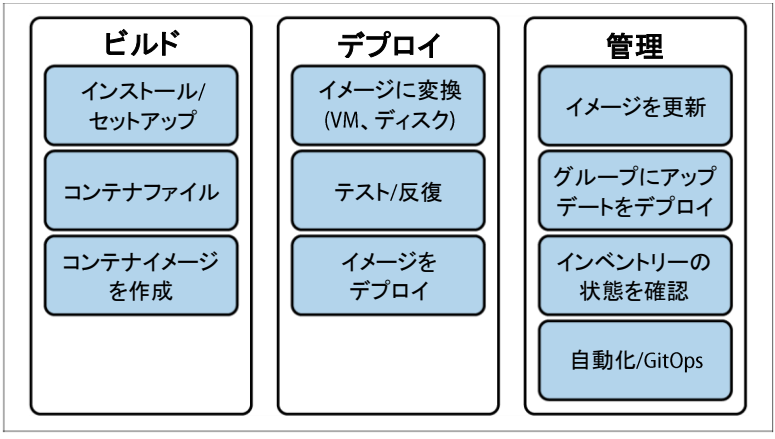

図 3-1. コンテナ化された (イメージモード) OS デプロイメントモデルの例

AI 支援システム管理

多くのアプリケーション作成者が、ターミナル・エミュレーター (コマンドラインへのアクセスを提供するツール) などのシステム管理ツールに直接 AI を組み込み始めています。管理者がブラウザーウィンドウや別のアプリケーションを開くことなく任意の LLM にクエリを実行で

きるようになるため、非常に有益です。当然、OS メーカーにとっての次のステップは、同じように OS 自体に直接 AI を組み込むことです。それにより、エンドユーザーがどのターミナルを選択しても、コマンドラインから AI アシスタントを呼び出せるようになります。この機能は、あらゆるスキルレベルの管理者に大きなメリットをもたらしますが、特に経験の浅い管理者にとっては、コマンドラインで AI アシスタントに直接質問をして、その場で見直し、適切な作業を適切な方法で行っていることを確認できるというメリットがあります。

すべての AI ツールと同様に、コマンドライン・アシスタントも慎重に使用する必要があります。正確な回答を得るために、コマンドライン・アシスタントに質問する内容を改善しなければならない場合もあります (シェルスクリプトなどのコードの生成をアシスタントに依頼する場合はなおさらです)。

このような若手管理者が迷ったときは、AI アシスタントの答えが意図したとおりに機能するかどうかを上位の管理者に確認することをお勧めします。

このツールは、基本的な bash スクリプトのようなものを理解するだけではなく、より強力な機能を備えており、コマンドライン・アシスタントは、アプリケーションやサービスの構成方法に関する便利なヒントを提供したり、OS 機能を利用してトラブルシューティングを行ったりすることができます。重要なのは、これらのアシスタントが、一般的な Linux についてだけでなく、ディストリビューションの細部や特定のニーズ/要件に関しても特別なトレーニングを受けていることです。このファインチューニングは AI の世界でよく知られています。カスタムモデルか、適切な種類のドキュメントのみでトレーニングされ、ハルシネーションを最小限に抑えるように構築された汎用 LLM かは、組み込みツールにおける大きな差別化要因となっています。

コマンドライン・アシスタントは、Security-Enhanced Linux (SELinux) や組み込みファイアウォールなどのツールで特に有効です。どちらのツールもシステムの運用上極めて重要ですが、複雑であるため、構成が変更されることはほとんどありません。システム管理者は、コマンドライン・アシスタントを使用すれば、こうしたツールをはるかに短時間で簡単に設定できるようになります。さらに、AI ツールは比較のための検証例をいくつも提供できるため、ベストプラクティスを適切に把握し、経験豊富な管理者も見落としがちな設定ミスを指摘することができます。

最後に、コマンドライン・アシスタントを使用すると、使用されているツールの構造を理解しやすくなります。たとえば、先進的なホストベースのファイアウォールの実装方法を知りたい場合は、アシスタントに質問してみてください。アシスタントが、提示された情報に基づいてベストプラクティスや事例の関連資料を検索し、設定やソースコードの変更について補足した回答をわかりやすい表現で生成するため、推奨する作業とその理由を簡単に理解できます。

フリート管理ツール

前述した 2 つのツールは強力であり、個々のシステムレベルでシステムの管理を大幅に単純化するものでした。次のツールは、管理をより高いレベルに引き上げ、デプロイされた Linux 環境全体をユーザーがプロアクティブに管理できるようにします。このようなツールは、OS の製造元が提供するあらゆるものと密接に連携するため、プラットフォーム全体の一元管理が実現し、管理や監査の必要性が軽減されます。デプロイされたアプリケーションのライフサイクルと、それらが環境内で稼働しているシステムに与える影響を把握するのに役立つプランニング機能も備えていれば、理想的です。こうした統合により、組織全体のセキュリティと構成をリアルタイムで検証することが可能になります。

ロードマップ機能によって、次のアプリケーションや OS のリリースに関する詳細情報が提供されるため、新機能がリリースされてからそれに対応するのではなく、予想される新機能に基づいたアップグレードを計画できるようになります。

フリート管理ツールを使用して、システムを最新の状態に維持することもできます。調整されたパッチ適用（自動化またはスケジュール済み、成功を確認済み)、機能/ソフトウェアのアップデートまたはロールアウト、一元化された構成管理により、1,000 台のサーバーも 1 台のサーバーと同じくらい簡単に管理できます。

エンタープライズグレードのセキュリティ

セキュリティを念頭に置いて設計された OS は、前述したイミュータブルなイメージや構成管理といったセキュリティ上のメリットを上回る機能も備えているはずです。

最も話題となっている将来の攻撃の 1 つは、ポスト量子暗号化を中心に展開されます。前章で説明したように、PQC は鍵、暗号化、デジタル署名用の量子耐性アルゴリズムを組織に提供します。これはデータとアプリケーションを将来にわたって使用できるようにするのに役立ち、OS ディストリビューションを比較する際に注目すべき重要な機能です。

エンタープライズグレードの OS プラットフォームは、堅牢なサプライチェーンのセキュリティ機能セットも提供します。これは OS だけに限定されたものではなく、DevSecOps 手法でのデプロイを検討している開発者や組織をサポートするというプラットフォームレベルの戦略です。わかりやすい例として、既知の正常なアプリケーション依存関係をホストする際に信頼できる場所が挙げられますが、これがさらに強化される可能性があります。理想的な DevSecOps プラットフォームは、開発チームに対して、すべてのアプリケーションと依存関係に対応するエンドツーエンドのセキュリティ・パイプラインを提供するものです。

PQC 保護、管理者および開発者向けの自動化されたセキュリティツール、プロアクティブなソフトウェア管理を組み合わせた多層防御を構築することで、最新の状態を維持し、現代の高度な脅威の状況に対処できます。重要なのは、このセキュリティは組織が使用するツールや OS によって提供されるという点であり、サードパーティのセキュリティ製品への大規模な投資を強いるのではなく、あらゆる機能を備えたプラットフォーム戦略に貢献します。

広範なハードウェアおよびソフトウェアサポートと認定

OS プラットフォームは強力ですが、組織が運用するには外部互換性が必要です。これは、OS が実行されるハードウェアと、実行されるシステム自体で利用されるサードパーティのソフトウェアの両方に当てはまります。

現代において、ハードウェアの互換性は変化の激しい市場となっています。特に AI ハードウェアは急速に変化しており、その変化に対応するには OS ドライバーと互換性が必要です。選択したディストリビューションがこの点に優れており、最新の AI ライブラリ、ドライバー、アプリケーションのほか、NVIDIA、Intel、AMD などのメーカー向けにハードウェア最適化を提供していることを確認することが重要です。ただし、OS メーカーには、これら 3 つの主要企業に加えて、最新の機能を迅速かつ安全で信頼性の高い方法でエンドユーザーに提供している堅牢なサードパーティのエコシステムも必要です。

まとめ

OS のセキュリティ、エコシステム、機能セットを組み合わせることで、このレポートの冒頭で特定された課題、具体的には他の OS の検討が戦略的に不可欠であるという課題に対処できます。この章で取り上げた主要機能を備えた OS は、機能と管理性の両面で競合製品よりも優れています。テクノロジーの進歩と強力なパートナープログラムの組み合わせこそが、新たな OS プラットフォームを選択する際に無視できない、戦略的に重要な差別化要因となります。

第 4 章

次のステップ

OS の選択は組織の根幹に関わる決定であり、競争上の優位性や社内のインフラストラクチャ管理に影響を及ぼします。イノベーションの加速、世界的な不確実性、経済的な制約、先進的なセキュリティのニーズ、AI によるプレッシャーに対応するには、これらの課題に統合的に対処できるように構築された専用のプラットフォームが必要です。

この選択を軽視してはなりません。組織が将来の OS とプラットフォームを決定する際に考慮すべき 4 段階の重要な評価手順は次のとおりです。

- 組織にとって最大のプレッシャーを特定します。
- ワークロードを機能要件にマッピングします。
- ビジネスに対する全体的な価値を評価します。
- サプライチェーンのセキュリティと長期的な実行可能性を検証します。

最大のプレッシャーを特定する

組織は、チームがそれぞれ異なるプレッシャーにさらされていることに気づくはずです。AI 製品チームはイノベーションとハードウェアの要件を優先しますが、規制の厳しい業界ではセキュリティとコンプライアンスの機能により重点が置かれます。組織は、現在および予想される将来の重要性に基づいて、各プレッシャー領域（イノベーションの加速、世界的な不確実性、経済的な制約、セキュリティのニーズ、AI）を評価し、将来の評価において「必須」か「あれば便利」かに分類したリストを作成する必要があります。

ワークロードを機能要件にマッピングする

すべての要件に共通する要因の 1 つが、組織にとって最も重要なワークロードです。ワークロード分析を行うことで、ワークロードごとに最適化するメリットがあるかどうかや、より大規模な標準化を進める方が適切かどうかがわかります。ワークロードの数や重要性と企業規模は必ずしも関連しないため、あらゆる規模の組織にとってメリットがあります。

ビジネス価値を評価する

ワークロード分析が完了すると、組織はサーバーの台数、従業員数(およびスキルレベル)、管理しているすべてのワークロードを確実に把握できます。こうした情報は、OS のライセンス、サポート、インフラストラクチャのニーズなど、直接的なコストを評価する際に役立ちます。また、社内の専門知識のレベル、予期せぬ制約によるワークロードデプロイの遅延、柔軟性に欠けるインフラストラクチャに起因するビジネス機会の逸失など、間接的なコストの算定にも役立ちます。このデータを収集することで、企業においては、より多くの情報に基づいた戦略的な意思決定が可能になり、それによって運用効率を向上させ、競争上の優位性を高めることができます。

サプライチェーンのセキュリティと長期的な実行可能性を検証する

OS やプラットフォームに関する意思決定を行う組織は、対象の OS またはプラットフォームが長期にわたって使用されることを認識しておく必要があります。企業の歴史を理解することは重要ですが、その企業がアプリケーションをどのように検証しているか、パートナー・ポートフォリオの質と幅広さ、規制遵守などの重要な側面や AI などの最先端機能に関する経験と能力を把握することも重要です。多くの組織は、ワークロードデプロイのライフサイクルを複数年と想定していますが、そのプラットフォームが現在および将来にわたってワークロードを処理できることを確認しておく必要があります。

まとめ

このプロセスにおける成功の鍵は、インフラストラクチャの決定によって生み出される依存関係について理解することです。組織が今、何を選択するかで、今後数年間で成功を収めることができるか、それとも能力不足でプロジェクトが遅延するかが決まります。明確な要件と評価フレームワークを念頭に置き、OS の選択に戦略的に取り組む組織は、イノベーションを積極的に追求し、不確実性に適切に対処し、現在および将来にわたって生産性とセキュリティの両方を最適化することができます。

執筆者について

Ned Bellavance は、この分野で 20 年以上の経験を持つ IT プロフェッショナル兼技術教育者です。これまで、ヘルプデスクオペレーター、システム管理者、クラウドアーキテクト、プロダクトマネージャーを務めてきました。最近では Ned in the Cloud LLC を運営し、コースの開発、複数のポッドキャストの配信、書籍の執筆、テクノロジーベンダー向けのオリジナルコンテンツの作成を行っています。2017 年から Microsoft MVP となり、2020 年から HashiCorp Ambassador を務めています。不安を受け入れること、失敗を計画すること、親切であることを 3 つの柱としています。

Chris Hayner は、オペレーティングシステム、インフラストラクチャ、クラウドコンピューティング、サイバーセキュリティの分野で数十年の経験を持つ熟練した IT プロフェッショナルです。データセンターでキャリアを開始した後は、メインフレームから AlamaServer、ホワイトボックス x86 サーバーまで、さまざまなシステムを管理していました。そこから、担当範囲は仮想化、クラウドテクノロジー、包括的なサイバーセキュリティおよび IT 戦略へと拡大していきました。過去 15 年間はコンサルティング部門に所属し、対象分野のエキスパート (SME)、アーキテクト、アナリストを務めてきました。これらの職務において、多くの組織が抱えるビジネス目標と IT ソリューションのギャップ解消に貢献し、イノベーションと運用の成功を後押ししてきました。CISSP 認定など多数のベンダー資格と業界資格を保有するほか、テンプル大学から MBA を取得しており、技術的な専門知識とビジネス感覚を兼ね備えています。