Red Hat

セキュリティとコンプライアンスの強化

オープンソースの Linux プラットフォームでリスクを軽減

目次

3 第1章：
Linux は将来への基盤

4 第2章：
セキュリティとコンプライアンスに対する効果的なアプローチの導入

5 第3章：
Linux 環境における脆弱性の特定と修復

6 第4章：
Linux 環境におけるコンプライアンス管理

7 第5章：
ベストプラクティスとツールの推奨事項

8 第6章：
Red Hat でセキュリティとコンプライアンスを強化

9 第7章：
統合ツールを活用する

10 第8章：
Zoom は Red Hat を使用して堅牢なエンタープライズシステムを確立

11 データを最大限に活用する

以下は、セキュリティ対策が不十分な場合に生じるインシデントの典型的な結果を示す**最近のベンチマークです。**[1]

- **440 万米ドル**：2025 年のデータ侵害の平均総損害額
- **241 日**：2025 年のデータ侵害の特定と阻止にかかった平均時間
- **97%**：AI 関連のセキュリティインシデントを報告した組織のうち、適切な AI アクセス制御が行われていなかった組織の割合

第 1 章

Linux は将来への基盤

Linux® は最も人気のあるオペレーティングシステム (OS) の 1 つであり、先進的な IT 環境に最適なプラットフォームを提供します。データセンターやクラウドコンピューティング環境において、可用性、信頼性、重要性の高いワークロード向けの標準となっており、さまざまなユースケース、ターゲットシステム、デバイスをサポートしています。多くのパブリッククラウドプロバイダーが、マーケットプレイス内で複数の Linux ディストリビューションを提供しています。

しかし、IT 環境の効率、セキュリティ、相互運用性は、どの Linux ディストリビューションと管理ツールを選ぶかで大きく変わります。この e ブックでは、セキュリティ管理の効果的なアプローチ、統合されたツールの主要な機能と推奨事項、Linux 環境におけるセキュリティ脆弱性およびコンプライアンスリスクの管理に関するガイダンスを提供します。

AI がもたらす新たな課題

多くの組織が IT セキュリティとコンプライアンスの管理を常に懸念しています。「世界中で、5 社のうち 1 社は過去 2 年以内に重大なサイバーインシデントを経験しています。これらのイベントには多額の費用がかかり、データ侵害の世界平均被害額は 444 万米ドルに上ります」。[1] AI の台頭によって新たな脅威がもたらされ、セキュリティ環境はさらに複雑化しています。特に、IT 部門の把握していないところで従業員が未承認の AI ツールを使用すること (「シャドー AI」と呼ばれる) が新しい大きな脅威の源となっています。「シャドー AI が関与した侵害では、[合計] 被害額が平均 67 万米ドル多くなっています。これは、[標準的な侵害のコストよりも] 15% の増加です」。[1]

セキュリティの不備による代償を回避

侵害のリスクと影響を軽減するには、スピードが不可欠です。潜在的な脅威の特定が早いほど、経済的および運用上の損失は小さくなります。以下は、セキュリティ対策が不十分な場合に生じるインシデントの典型的な結果を示す最近のベンチマークです。[1]

- **440 万米ドル**：2025 年のデータ侵害の平均総損害額
- **241 日**：2025 年のデータ侵害の特定と阻止にかかった平均時間
- **97%**：AI 関連のセキュリティインシデントを報告した組織のうち、適切な AI アクセス制御が行われていなかった組織の割合

セキュリティに関する 3 つの一般的な課題

次のようないくつかの要因により、先進的なセキュリティ脆弱性とコンプライアンスの管理は難しくなります。[1]

セキュリティとコンプライアンスの状況の変化

チームはもはやデバイスを管理しているだけではありません。承認された AI モデルを管理すると同時にシャドー AI ツールに対する防御を行うのに苦労しています。

- **20%**：シャドー AI に関連するセキュリティインシデントによって引き起こされた侵害の割合

データが複数の環境に保存されている場合、保護の困難さは大きく高まります。この複雑さにより、単一の環境内にデータを保存する場合と比較して、セキュリティチームが侵害を特定および阻止することはさらに困難になります。

- **30%**：複数の環境に保存されたデータに関連する侵害の割合

1 IBM Security、「2025 年データ侵害のコストに関する調査」、2025 年。

複雑さによる代償

大規模なインフラストラクチャには多くの場合、複数のセキュリティツールおよびコンプライアンスツールが組み込まれており、それらによってリスク管理業務が複雑になります。

- 複数の環境が関与したデータ侵害は現在、最も一般的かつ被害が最も高額となっており、その損害額はインシデントあたり平均 **505 万米ドル**となっています。これは、オンプレミスのみで発生した侵害よりもわずかに高額です。

人員配置の課題

多くの組織では、セキュリティとコンプライアンスに関するタスクを手動で管理するのに必要な人員を確保できていません。さらに、リモートワークの増加により、デバイスや組織のデジタル資産へのアクセスポイントを保護する負担が増大しています。

- **63%**：AI の管理に必要なガバナンスポリシーを備えていない組織の割合。その主な理由は、ポリシーを作成して適用するスタッフがいないため。

第 2 章
セキュリティとコンプライアンス管理に対する効果的なアプローチの導入

セキュリティとコンプライアンスの管理は、リスクベースの継続的な規律によって実現します。そのような規律により、組織はセキュリティポスチャを強化し、複雑する環境全体で規制要件およびビジネス要件を満たすこともできます。先進的なアプローチを導入すると、オンプレミス、クラウド、ハイブリッド・インフラストラクチャを含む IT 環境全体で一貫性のある反復可能で監査可能なプラクティスを確立できるようになるため、次のことが可能になります。

評価

非準拠または脆弱性のあるシステムを継続的に検出します。インフラストラクチャからワークロードまで、組織の環境全体のセキュリティ状態を評価し、個々のシステムが実際にどのセキュリティ・アドバイザリーの対象となっているかを判断します。

優先順位付け

検証済みの自動化と AI 駆動のツールを活用して、リスク、影響、運用の労力に基づいて修復作業に優先順位を付けます。リスク管理手法を使用して各問題のビジネスインパクトを把握し、それに応じて修復作業を計画します。たとえば、同じ脆弱性でも開発システムで見つかった場合は最小限のリスクで済む場合がありますが、プロダクション・ワークロードで見つかった場合は即座に対応することが必要です。

修正

システムへのパッチ適用と再構成を迅速に行います。修復プロセスを自動化することで、システム間の一貫性を確保し、人的ミスのリスクを軽減できます。自動化ツールを効果的に使用すればすばやく修復を行い、ビジネスとそのデータを保護できます。

レポート

変更が適用されたことを継続的に検証し、レポート作成を自動化して監査を効率化します。経営幹部、監査担当者、技術チームがそれぞれの役割に応じた明確なレポートを取得できれば、現在のセキュリティ

スクウェア・エニックス、オンラインゲームのインフラ管理をシンプル化

「Red Hat Enterprise Linux に切り替えてから、以前使用していた Linux ディストリビューションよりも不具合や脆弱性の調査、発見を迅速に行えるようになりました」

宮本侑季氏
株式会社スクウェア・エニックス
情報システム部
IT インフラストラクチャ/ビジネスオンラインインフラストラクチャシステムグループ

注：このコンテンツに含まれる情報は、インタビュー実施時点のものです。

状況やリスクの推移を、各自に適したレベルで正確に把握できるようになります。継続的な検証と自動化された監査可能なレポートを組み合わせることで、事後対応的なセキュリティ運用から一歩前進して、スピード、一貫性、ガバナンスのすべてを共存させる DevSecOps のような先進的な運用モデルをサポートすることができます。

第 3 章
Linux 環境における脆弱性の特定と修復

脆弱性の特定と修復は、インフラストラクチャを評価して攻撃の影響を受けやすいシステムを検出し、修正するプロセスです。脆弱性は、新たな脅威、古いパッチ、パッチの適用漏れ、システムの構成ミスなどによって引き起こされる可能性があります。修復は通常、システムのパッチ適用、アップデート、再構成などを行うことで根本的なリスクを解消します。

脆弱性の特定が重要な理由

セキュリティの脆弱性があると、侵害によって大きな被害を受ける可能性があり、顧客からの信頼や企業の評判の失墜、収益の低下につながるおそれもあります。実際、「攻撃においては他の種類のデータよりも顧客の個人識別情報 (PII) が標的とされることが圧倒的に多く、53% にも上っています。さまざまな種類のデータの中で PII は盗難にあったり漏洩したりした件数が最も多くなっています」。[1] この種のデータは ID 窃盗や詐欺での使用価値が高いため、依然として最大の標的とされています。

脆弱性の効果的な特定と修復に関する課題

ほとんどの組織は、大規模な運用に適用する一貫したセキュリティ戦略を持っていません。そしてこのギャップは、AI ツールやワークロードの急速かつ無秩序な導入によってさらに拡大しています。その主な障壁には次のようなものがあります。

- スキルとリソースのギャップ：AI 環境が拡大するにつれて、スタッフは限られた人員で管理を行わなければならず、その業務に忙殺されてしまいます。また、包括的なセキュリティ戦略の開発と実行に必要なスキルが不足している場合もあります。
- アラート疲れ：汎用的なセキュリティ・スキャン・ツールを使うと、潜在的な脆弱性の膨大なリストが生成されます。しかしその多くは実際の環境に当てはまらないため、スタッフは本当のリスクを調査するために多くの時間を費やさなければなりません。
- 手動による障害：識別、修復、追跡プロセスを手動で行うことで運用に遅れが生じ、既知の脆弱性があるにもかかわらずパッチが長期間適用されないままになることがあります。
- 一貫性のない修復：その場しのぎの修復を行っていると、パッチの適用に一貫性がなくなり、インフラストラクチャ全体でセキュリティ侵害のリスクが増加します。

セキュリティ管理ツールの主な機能

組織が効果的に機能するためには、侵害が発生する前にシステムの脆弱性を迅速に特定し、解消できる必要があります。統合セキュリティ管理ツールを評価する際には、以下の主な機能に注目してください。

- **システムを分析**して OS レベルとワークロードレベルの両方で環境全体のシステムとインスタンスのリスクを特定できる
- 特定されたリスクを**自動的に修復**して、IT チームとセキュリティチームのスピード、正確性、効率性を向上させることができる
- **ベンダーの専門知識が組み込まれて**おり、検証済みの修正方法を含む製品修復ガイダンスを取得できる

- OS やアプリケーションのプロバイダーが公開する、既知の脆弱性とセキュリティリスクに関する**最新データに定期的にアクセス**できる
- 経営幹部、監査担当者、技術チームのそれぞれに適切なレベルの詳細情報を備えた**監査用のレポートを生成**できる

インフラストラクチャの管理とセキュリティの向上に Red Hat® Satellite ソリューションを使用することで、優れた IT 部門でもメリットを得ることができます。その詳細について、こちらの PeerSpot レポートをお読みください。[2]

第 4 章

Linux 環境におけるコンプライアンス管理

コンプライアンス管理は、システムが企業ポリシー、業界標準、および適用される規制に持続的に準拠させるプロセスです。これには、規制およびポリシーの変更や構成ミスにより非準拠となったシステム、またはその他の社内基準に準拠していないシステムを特定するためのインフラストラクチャ評価が含まれます。

コンプライアンス管理が重要な理由

適用される規制を遵守しなかった場合、セキュリティ侵害のリスクが増大するだけでなく、多額の罰金、企業の評判の低下、必要な認定資格の失効などのリスクも生じます。法令に違反した状態でデータ侵害を受けた場合、平均損害額は 17 万 3,692 米ドル増加します。[1]

効果的なコンプライアンス管理の課題

多くの組織は手動操作とカスタムスクリプトに依存していますが、これは動きの速いテクノロジー開発やビジネス運用に対応するには時間がかかり過ぎ、規模も限られてしまいます。次のような問題もあります。

- 汎用的な基準やベースラインが多数存在するため、特定の環境に適用される要件がどれなのかを判断するのが困難です。
- 手動プロセスでは、コンプライアンスの監視、修復、監査の処理に時間がかかるため、非効率なスタッフ運用、ポリシー適用の一貫性の欠如、コンプライアンスに関する問題のリスク増大につながります。
- セキュリティ管理とコンプライアンス管理に別々のツールを使用すると、運用効率が低下し、一貫性のあるカスタムポリシーの設定に必要な労力が大きくなります。

コンプライアンス管理ツールの主な機能

組織が効果的に機能するためには、システムの整合性を維持し、また監査用のレポートをより短時間で生成できるよう、コンテキストに応じたポリシーを定義して適用する必要があります。統合コンプライアンス管理ツールを評価する際には、次の機能を持つツールを探しましょう。

- **分析機能を使用**して、コンプライアンスリスクを時間効率よく一貫して特定する
- 非準拠のシステムを自動**修正**する
- 現在の環境全体のコンプライアンスポスチャを**包括的に可視化**できる

2 PeerSpot レポート、「Red Hat Satellite がセキュリティとインフラストラクチャ管理の効率性を高める 7 つの方法」、2024 年 4 月 24 日。

Zoom は Red Hat を使用して堅牢なエンタープライズシステムを確立

「毎週、環境内のすべてのシステムに対してセキュリティスキャンを実行する必要があります。スキャナーにより、オペレーティングシステム上のパッケージの脆弱性が一覧表示されます。脆弱性が表示された場合は、いつでもすぐに Red Hat サイトにアクセスして脆弱性の詳細な説明を得ることができ、影響を受けるかどうかを判断できます。Linux ディストリビューションを提供している他の企業で、そのようなことを実施しているところはありません。これを使わずに政府の本番環境を運用しようとすると、すべての調査を毎月自分たちで行う必要があるため、すぐに悪夢のような状況になるでしょう」。

Ryan Kimbrell 氏
Zoom シニア・クラウド・オペレーション・エンジニア

- 監査要件や対象者のニーズに応じて**コンプライアンスレポートを自動的に生成**する
- 複数の環境全体で非準拠システムを修復するためのコンテキストに合ったガイダンスと**専門家のアドバイスを提供**する

次の章では、動的なエンタープライズ環境においてセキュリティとコンプライアンスのリスクをより効果的に管理するためのベストプラクティスについて説明します。

第 5 章
ベストプラクティスとツールの推奨事項

定期的にシステムを分析する

毎日監視を行えば、業務の中断や侵害が生じる前に、脆弱性やコンプライアンスのリスクを特定するのに役立ちます。OS ベンダーやアプリケーションベンダーから得られる最新のセキュリティデータを使用して分析の精度を向上させ、特定の環境に合わせたカスタム・セキュリティ・ポリシーを確立しましょう。

- CISA Known Exploited Vulnerability (KEV) カタログに記載されている脆弱性の場合、攻撃者が大規模な悪用を開始するまでの平均時間はわずか **5 日**です。[3]

パッチを頻繁に適用し、徹底的にテストする

システムを最新の状態に保つことで、セキュリティ、信頼性、パフォーマンス、コンプライアンスを向上させることができます。一般的なパッチを定期的に適用する一方で、重大なバグや欠陥にはただちに対応する必要があります。パッチを適用したシステムは、受け入れテストを行ってからプロダクション環境に戻します。

自動化と承認済みの AI ツールをデプロイする

インフラストラクチャの規模が大きくなると、手動での管理は難しくなります。監視の効率化、修復の迅速化、一貫したレポート生成のために自動化と AI 駆動のツールを使用しましょう。

- セキュリティチームが AI と自動化を幅広く活用している組織では、使用していない組織と比較して、侵害の特定および阻止にかかる日数が 80 日短く、侵害の平均被害額は **190 万ドル**低くなっています。[1]

ツールを接続し、プロセスを調整する

統合されていないプラットフォーム管理ツールをアプリケーション・プログラミング・インタフェース (API) 経由で統合し、分散環境全体の可視性を確保しましょう。インタフェースの数を減らすことで、運用が単純化され、より一貫した信頼性の高いセキュリティポスチャを確立できます。

- セキュリティシステムの複雑さが増すと、侵害による損失額は平均で **20 万 7,914 米ドル**増加します。[1]

一貫性のある継続的なセキュリティ戦略を採用する

効果的なセキュリティには、人、プロセス、テクノロジーが連携する包括的なアプローチが求められます。多層防御戦略をとると、OS、コンテナ・プラットフォーム、自動化および AI ツール、Software-as-a-

3 Verizon Business、「2025 Data Breach Investigations Report」、2025 年。

Service (SaaS) ソリューション、クラウドサービスなど、すべてのレイヤーにセキュリティ制御を適用することで保護を最大限に高めることができます。

- **63% の組織**には正式な AI ガバナンスポリシーがありません。これはそのまま侵害被害額の増加につながっています。[1]

改善への最初のステップは、組織のセキュリティポスチャとコンプライアンス体制のニーズを常に把握できるようにすることです。セキュリティおよびコンプライアンスツールには、次のようないくつかの主要な特徴や機能が備わっているのが理想的です。

- **プロアクティブな分析：**プロアクティブな自動分析を行うツール。これにより、システムを定期的に監視し、手作業で常に監視しなくても問題があればアラートを受信できます。
- **対応の優先順位付け：**規範的な修復手順を提供するとともに、潜在的な影響に基づいてアクションに優先順位を付けるツール。これによって、限られたパッチ適用期間を最大限に活用できます。
- **カスタマイズ可能な成果：**誤検知を減らすために、組織の IT リーダーがビジネスコンテキストを定義できるツールを探しましょう。これにより、関連するシステムとワークロードのみチェックできます。一部の脆弱性およびコンプライアンスのチェックは、用途、構成、ワークロードによって、特定のシステムに適用されない場合があります。
- **直感的なレポート：**パッチのステータスやポリシーのコンプライアンスに関して、複数の役割のユーザーそれぞれに明確で理解しやすいレポートを生成するツール。監査性とステークホルダーの連携が向上します。
- **統一されたインタフェース：**IT 環境の複数の層を管理できるツール。セキュリティ運用を単純化し、現在のセキュリティポスチャとコンプライアンス体制をより適切に把握できます。統一されたツールを使用すれば、スキャンや修復ガイダンスに関するコンテキストの情報量も増加します。
- **実用的なインサイト：**IT 環境に応じた情報を提供するツール。影響を受けるシステムや、脆弱性の潜在的な影響を迅速に特定するのに役立ちます。これによって組織は、修復作業の優先順位を付けて計画することができます。

第 6 章
Red Hat でセキュリティとコンプライアンスを強化

Red Hat は、セキュリティおよびコンプライアンスのリスク管理に対する包括的でプロアクティブなアプローチを採用しており、ベアメタルサーバーや仮想サーバーからプライベート、パブリック、ハイブリッドクラウド、エッジデプロイメントに至るまで、IT 環境全体のスピード、スケーラビリティ、安定性を向上させます。Red Hat® プラットフォームは、人、プロセス、テクノロジーを連携させることで、運用効率の達成、イノベーションの促進、従業員の満足度向上を支援します。

この戦略の中核となるのが、先進的な IT のための一貫したインテリジェントな運用基盤である Red Hat Enterprise Linux です。インフラストラクチャ全体で一貫性が得られるため、IT チームはあらゆる場所で同じツールを使用してアプリケーション、ワークロード、サービスをデプロイできます。

セキュリティは、Red Hat Enterprise Linux のアーキテクチャとライフサイクルの鍵となる要素です。多層侵害防御機能は、自動化された反復可能なセキュリティ管理を使用して、脆弱性にさらされるリスクを軽減します。Red Hat Enterprise Linux サブスクリプションの一部として重要なセキュリティ・アップグレードとライブパッチが提供されるので、IT 環境をダウンタイムなく安全に保護するのに役立ちます。

Zoom が実施する FedRAMP と DoD の要件への対応方法

「コンプライアンスは規律によってのみ達成できます。Red Hat には、私たちが必要としている規律があります」

John Keese 氏
Zoom テクノロジー・コンプライアンス統括責任者

「Red Hat Enterprise Linux に切り替えてから、以前使用していた Linux ディストリビューションよりも不具合や脆弱性の調査、発見を迅速に行えるようになりました」。[4]

宮本侑季氏
株式会社スクウェア・エニックス
情報システム部
IT インフラストラクチャ/ビジネスオンラインインフラストラクチャシステムグループ

Red Hat Enterprise Linux は、統合管理ツールと AI を活用したインサイトで強化されており、ハイブリッド環境におけるセキュリティとコンプライアンスの管理について包括的に把握できます。これにより、次のようなメリットが得られます。

- **アラート疲れの軽減：**構成可能なツールとベースラインにより誤検知が減少し、現在の IT インフラストラクチャのステータスを正確に把握できます。
- **プロアクティブな修復：**自動化によって構成とパッチ適用の精度が向上して人的エラーが減少し、サポートへの連絡が必要なくなります。
- **包括的な可視性：**脆弱性およびマルウェアの検出機能を使用してシステムをスキャンし、共通脆弱性識別子 (CVE) やマルウェアのシグネチャを検出します。また、ビューをカスタマイズできるので、さまざまな役割のユーザーが適切なデータを適切なタイミングとスピードで取得できます。
- **最適化された統合：**Red Hat Enterprise Linux を既存のセキュリティ、コンプライアンス、管理ツールおよびインタフェースとスムーズに接続できるよう、オンサイトや Software-as-a-Service (SaaS) のデプロイオプション、および API を利用できます。この最適化された統合に関するリソースが数多く登録されたライブラリが提供されており、詳細で的を絞った情報を 24 時間 365 日得ることができます。
- **リソース最適化機能：**IT チームは、コンピュート、メモリー、パフォーマンスの指標を使用して、パブリッククラウド・デプロイメントの適切なサイズを選択できます。
- **防御機能の準備：**米国国立標準技術研究所 (NIST) が承認した耐量子アルゴリズムとコンフィデンシャル・コンピューティング[5] を使用して、将来の量子コンピュータの脅威に備え、機密データを (使用中であっても) 保護します。

コンフィデンシャル・コンピューティングとはを読む

第 7 章
統合ツールを活用する

Red Hat 管理ツールは、Linux の開発とサポートに関する何十年もの経験に基づいています。これらの Red Hat ツールが連携して IT 管理を効率化し、最適化されセキュリティ重視で信頼性の高い環境を維持するとともに、IT チームの貴重な時間の節約に貢献します。

Red Hat システムの分析、観察、管理

Red Hat は、セキュリティ重視の運用とイノベーションに必要な、信頼できる Linux プラットフォームと統合管理ツールおよびサービスを提供します。

4 Red Hat 導入事例、「スクウェア・エニックス、オンラインゲームのインフラ管理をシンプル化」、2023 年 5 月 17 日。
5 Red Hat 概要、「コンフィデンシャル・コンピューティングとは」、2025 年 10 月 22 日。

- **Red Hat Lightspeed：**サブスクリプションに含まれており、サービスとして提供される Red Hat Lightspeed (旧称 Red Hat Insights) は、プラットフォームとアプリケーションを継続的に分析して、リスクの予測、アクションの推奨、コストの追跡を行います。これにより、組織はハイブリッドクラウド環境全体でセキュリティとコンプライアンスのリスクを管理しながら、IT の効率、安定性、パフォーマンスを監視できます。

Red Hat Lightspeed の詳細

システム管理の効率化と自動化

組織を保護するには、効果的で自動化された管理アプローチとツールの導入が不可欠です。

- **Red Hat Satellite：**デジタル主権を実現し、エージェント型の Red Hat Enterprise Linux 管理機能を提供するプラットフォームです。この管理ツールのプロビジョニングは数分で Red Hat Enterprise Linux システムに構成できます。これにより、エアギャップ環境でのコンテンツおよびパッチ管理を通じて、セキュリティを重視した Red Hat のサプライチェーンを拡張し、コンプライアンスを一貫して監視できます。統合された分析により、IT セキュリティチームは先回りして問題を特定し、修復の推奨事項を受け取ることができます。また、修復を大規模に自動化することも可能です。

Red Hat Satellite の詳細

第 8 章

Zoom は Red Hat を使用して堅牢なエンタープライズシステムを確立[6]

Zoom Video Communications, Inc.(Zoom) は、2011 年から革新を続けているグローバルな通信技術企業です。ビデオ通信ソリューションの提供から開始した同社は、多くのソリューションを提供する企業へと成長しました。それらのソリューションには Zoom for Government も含まれます。Zoom はこのプラットフォームを、Federal Risk and Authorization Management Program (FedRAMP) および国防総省 (DoD) の厳しいセキュリティ要件を満たすために Red Hat Enterprise Linux 上で実行しています。また、Red Hat Ansible Automation Platform および Red Hat Satellite を活用してインフラストラクチャを自動化しており、コンプライアンス機能を実現し、デプロイメントを管理しています。

Zoom for Government は、Red Hat Enterprise Linux とその他の Red Hat ツールを利用して、定期的な裁定プロセスがスムーズに実行されるようにしており、プロセスのほぼすべてのステップに Red Hat が関与しています。Zoom のデータセンターオペレーション統括責任者、Zak Peirce 氏は、Red Hat ソリューションの使用に確信を持っていました。「私はずっと Red Hat 派です」と Peirce 氏は言います。「私なら、堅牢なエンタープライズシステムを実行するためのエンタープライズ・プラットフォームとして Red Hat を選択します」。

Peirce 氏はさらに、エコシステム全体が有益だと感じた理由について述べています。「IdM を更新するとき、それが Red Hat システムで動作することがわかっています。System Security Services Daemon (SSSD) エージェントを更新するとき、それがうまく動作することがわかっています。そして、Red Hat Satellite を使用してこれらのパッケージをホストし、システムを最新の状態に保ち、システムに追加される正確なパッケージを管理できます。これは、システムをテストして開発段階と本番環境が同じであることを確認するのに役立ちます。これらすべての要素が運用に役立つのです」。

Common Vulnerabilities and Exposures (CVE) データベースや Red Hat セキュリティ・アドバイザリー (RHSA) など、Red Hat の Web サイトのリソースは、米国政府と協力する場合に非常に貴重な資産となります。

6 Red Hat 導入事例、「Zoom for Government、Red Hat プラットフォームを使用してセキュリティを強化」、2023 年 3 月 10 日。

「毎週、環境内のすべてのシステムに対してセキュリティスキャンを実行する必要があります。スキャナーにより、オペレーティングシステム上のパッケージの脆弱性が一覧表示されます。脆弱性が表示された場合は、いつでもすぐに Red Hat サイトにアクセスして脆弱性の詳細な説明を得ることができ、影響を受けるかどうかを判断できます。Linux ディストリビューションを提供している他の企業で、そのようなことを実施しているところはありません。これを使わずに政府の本番環境を運用しようとすると、すべての調査を毎月自分たちで行う必要があるため、すぐに悪夢のような状況になるでしょう」。

Ryan Kimbrell 氏
Zoom シニア・クラウド・オペレーション・エンジニア

データを最大限に活用する

企業の安定性と信頼性は、IT インフラストラクチャとアプリケーションにかかっています。組織の資産を保護するための最も効果的な方法は、セキュリティの脆弱性およびコンプライアンスリスクの管理に対するプロアクティブなアプローチを導入することです。

Red Hat は、セキュリティ重視の大規模な運用に必要な、信頼できる Linux プラットフォームと統合管理ツールおよびサービスを提供します。

Red Hat Lightspeed で組織のリスクを分析

- Red Hat Lightspeed の詳細
- こちらの概要[7] で、Red Hat Lightspeed がコンプライアンスと脆弱性の管理の単純化にどう役立つかをご確認ください。

Red Hat Satellite で大規模に管理

Red Hat Satellite の詳細

Red Hat Satellite のビジネス価値の詳細[8]

7　Red Hat 概要、「Red Hat Lightspeed で Linux 管理を単純化」、2025 年 5 月 2 日。

8　IDC ビジネス価値ホワイトペーパー (Red Hat 後援)、「Red Hat Satellite のビジネス価値」、2024 年 7 月。

Red Hat について

エンタープライズ・オープンソースソフトウェア・ソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備える Linux、ハイブリッドクラウド、コンテナ、および Kubernetes テクノロジーを提供しています。Red Hat は、クラウドネイティブ・アプリケーションの開発、既存および新規 IT アプリケーションの統合、複雑な環境の自動化および運用管理を支援します。受賞歴のあるサポート、トレーニング、コンサルティングサービスを提供する Red Hat は、フォーチュン 500 企業に信頼されるアドバイザーであり、オープンな技術革新によるメリットをあらゆる業界に提供します。Red Hat は企業、パートナー、およびコミュニティのグローバルネットワークの中核として、企業の成長と変革を支え、デジタル化が進む将来に備える支援を提供しています。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#US52390824_0426

Copyright © 2026 Red Hat, LLC.Red Hat、Red Hat ロゴ、および Ansible は、米国およびその他の国における Red Hat またはその子会社の商標または登録商標です。Linux® は、米国およびその他の国における Linus Torvalds 氏の登録商標です。