



# セキュリティと コンプライアンスの向上

堅牢なオープンソースの Linux プラットフォームでリスクを軽減

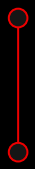
# 目次

1

Linux は将来への基盤

2

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



2.1 Linux 環境における脆弱性の特定と修復

2.2 Linux 環境におけるコンプライアンス管理

3

ベストプラクティスとツールの推奨事項

4

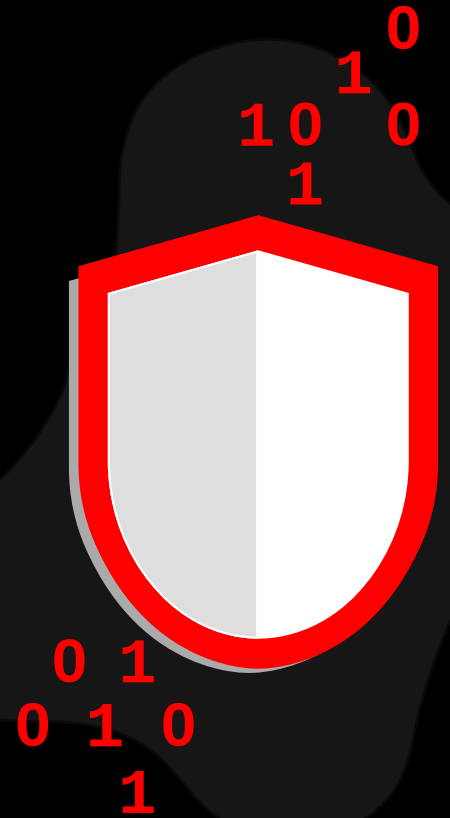
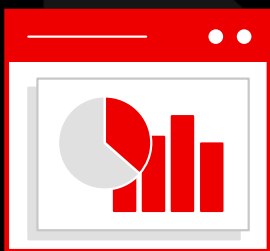
Red Hat でセキュリティとコンプライアンスを強化

5

成功事例を見る：英国気象庁

6

今すぐ始めましょう



# Linux は 将来への基盤



Linux® は世界で最も人気のあるオペレーティングシステムの1つであり、先進的かつ革新的な IT 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によく使用されており、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。主要なパブリッククラウドプロバイダーはいずれも、マーケットプレースで複数の 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、Linux 環境におけるセキュリティの脆弱性とコンプライアンスリスクに関する重要な考慮事項とガイダンスについて説明します。

## 最大の懸念事項はセキュリティとコンプライアンス

どの組織も IT セキュリティとコンプライアンスリスクの管理を常に懸念しています。事実、過去 2 年の間に 23% の組織が大規模なサイバーセキュリティ攻撃を経験しています。<sup>1</sup> また、セキュリティ侵害は大きな損害をもたらしかねません。データ漏洩が発生すると、その損害額は平均で 445 万ドルに上ります。<sup>2</sup>

業界や政府の規制も変化しています。その変化についていくことだけでも困難ですが、コンプライアンス違反があると、データ漏洩のコストは平均で約 5% も増加します。<sup>2</sup>

## セキュリティの不備による影響を回避

漏洩のリスクと影響を軽減するには、スピードが不可欠です。

# 445 万ドル

2023 年のデータ漏洩の平均総損害額 (米ドル)<sup>2</sup>

# 277 日間

2023 年のデータ漏洩の特定と阻止にかかった平均時間<sup>2</sup>

# 102 万ドル

漏洩を 200 日以内に特定し阻止することで節約できる平均コスト<sup>2</sup>

1 Nash Squared、「2023 Nash Squared Digital Leadership Report」、2023 年 11 月。

2 IBM Security、「Cost of a Data Breach Report 2023」、2023 年。

## セキュリティおよびコンプライアンスの一般的な課題

いくつかの要因により、セキュリティ脆弱性とコンプライアンスの管理が困難になります。

### セキュリティとコンプライアンスの状況の変化

セキュリティへの脅威は急速に変化しているため、新たな脅威やそれに併せて変化する規制に、迅速に対応する必要があります。

**23%**

過去 2 年で大規模なサイバーセキュリティ攻撃を経験した組織の割合 (規模問わず)<sup>3</sup>

**82%**

クラウド環境または複数の環境間に保存されたデータに関連したデータ漏洩の割合 (2023 年)<sup>4</sup>

### 分散クラウド環境

地理的、論理的に分散したハイブリッド環境やマルチクラウド環境では、IT インフラストラクチャを完全に把握することができず、すべてのシステム間で一貫した構成を維持することが難しくなります。

### 大規模で複雑な IT 環境

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、それによりリスク管理の業務が複雑になります。

セキュリティシステムの複雑さにより増加したデータ漏洩のコスト

**\$240,889<sup>4</sup>**

リモートワークにより増加したデータ漏洩の平均コスト

**\$173,074**

(リモートワークが要因となっていないデータ漏洩との比較)<sup>4</sup>

### 限られた人員とリモートワークの指示

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ために必要な人員を確保できていません。さらに、リモートワークにより、組織のデジタル資産にアクセスするデバイスやアクセスポイントを保護する負担が増加します。

3 Nash Squared, 「2023 Nash Squared Digital Leadership Report」、2023 年 11 月。

4 IBM Security, 「Cost of a Data Breach Report 2023」、2023 年。

# 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

セキュリティ脆弱性とコンプライアンスの管理では、システムの監視と評価によって、システムが確実にセキュリティおよび規制ポリシーに準拠するようにします。理想的なセキュリティ脆弱性及びコンプライアンス管理のアプローチを採用すると、環境全体にわたって一貫性のある繰り返し可能なプロセスを開発し、以下を実現する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特定します。インフラストラクチャからワークロードまで、環境の実際のセキュリティ状態を評価します。大量のセキュリティアドバイザリーのうち、どれが実際に自社のシステムや環境に該当するものを把握します。



## 優先順位付け

労力、影響、問題の重大度に応じて修復アクションを整理します。リスク管理手法を適用して、各問題の実際のビジネスリスクを判断し、それに従って修復作業を計画します。リスクには、問題が侵害につながる可能性、侵害の潜在的な重大性、問題の修復による影響が含まれます。たとえば、開発システムやテストシステムでは修復することが合理的でない問題でも、本番システムでは優先的な対処が必要となる場合があります。



## 修正

アクションが必要なシステムに迅速にパッチを適用して再構成します。構成とパッチ適用のプロセスを自動化して、迅速な修正、システム間の一貫性の確保、ヒューマンエラーのリスクの軽減を実現します。自動化ツールは、効果的に適用すれば、問題を迅速に修正し、環境とビジネスのセキュリティを向上させることができます。



## レポート

変更が適用されたことを検証し、レポート作成を自動化して監査を効率化します。効果的なレポート作成により、経営幹部、監査担当者、技術チームが現在のセキュリティリスクとエクスポージャーを把握できるよう、それぞれに適切なレベルの詳細さで情報を提供することができます。

このアプローチは **DevSecOps** のような先進的で動きの速い開発および管理手法を活用するための準備にも役立ちます。次のセクションでは、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重要な考慮事項とアクションについて説明します。

# 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、攻撃に対して脆弱なシステムを検出し、修正するプロセスです。これらの脆弱性は、新たな脅威、古いパッチやパッチの適用漏れ、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。多くの場合、修復アクションは、脆弱性を解消するためのシステムのパッチ適用、更新、再構成です。

## なぜ重要か

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ます。また、顧客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、データ漏洩の平均的なコストのうち、29.2% はビジネス機会の逸失によるものです。<sup>5</sup>

## 脆弱性の効果的な特定と修復に関する課題

ほとんどの組織には、大規模な運用に対する一貫したセキュリティ戦略がありません。

- ▶ 限られたスタッフでは対応が追いつかず、完全なセキュリティ戦略を策定し実行するために必要なスキルを持ち合わせていない可能性があります。
- ▶ 汎用的なセキュリティスキャンツールを使えば、潜在的な脆弱性の膨大なリストを得ることができます。しかしそのすべてが現在使用している環境に当てはまるわけではないため、スタッフは脆弱性や修復作業の調査に膨大な時間を費やす必要があります。
- ▶ 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適用されないままになることも少なくありません。
- ▶ その場しのぎの修復方法では、パッチの適用に一貫性がなくなり、潜在的なセキュリティリスクが増大します。

## セキュリティ管理ツールの主な機能

効果的であるためには、侵害が発生する前にシステムの脆弱性を迅速に特定し、修正できる必要があります。次のような機能を持つ統合セキュリティ管理ツールを探しましょう。



**システムを分析**して、オペレーティングシステム・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する



**特定されたリスクの修復を自動化**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



**ベンダーの専門知識を取り入れて**、製品の修復ガイダンスを提供する(簡単なアクションでリスクを軽減できる場合があります)



オペレーティングシステムやアプリケーションのベンダーが公開する、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する**



さまざまな対象者のそれぞれに対して適切なレベルの詳細さで、潜在的なリスク、修復アクション、監査に関する**レポートを生成する**

## 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。インフラストラクチャ評価により、規制、ポリシー、基準の変更、構成ミス、またはその他の理由によって非準拠となったシステムを特定します。

## なぜ重要か

準拠していないことにより、セキュリティ侵害に加えて、罰金、ビジネスへの損害、認証の喪失につながる可能性があります。コンプライアンスに違反すると、データ漏洩の平均コストが増加します。<sup>6</sup>

## 効果的なコンプライアンス管理の課題

多くの組織では、手動操作とカスタムスクリプトを使用してコンプライアンスを管理しています。しかしこれらのプロセスでは、先進的な動きの速い開発と運用を行うには時間がかかりすぎ、規模も限られてしまいます。

- ▶ 汎用的な基準やベースラインは多数存在するので、自社の環境との関連性や影響を把握することが困難です。
- ▶ 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。
- ▶ 多くの組織では、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しているため、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が困難です。

## コンプライアンス管理ツールの主な機能

効果的であるためには、コンテキストに応じたポリシーの定義と適用、システムのコンプライアンスの維持、監査レポートの迅速な作成と管理を行う必要があります。次のような機能を持つ統合コンプライアンス管理ツールを探しましょう。



**分析を使用**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



環境全体のコンプライアンス体制の**完全な把握**に役立つ



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



環境全体で非準拠システムを修復するための**専門家のアドバイス**とコンテキストに合ったガイダンスを**提供する**

# 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。分析の精度を高めるために、オペレーティングシステムやアプリケーションの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ます。また、環境や業務に合わせたカスタム・セキュリティ・ポリシーを設定することで、より正確なコンプライアンス結果を生成することができます。

侵害の発見および阻止を

**200 日以内**

に行えれば、結果として生じるコストを大幅に削減できます。<sup>7</sup>

## パッチを頻繁に適用し、パッチをテストする

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。重要な問題への全般的な対応として、定期的にパッチを適用します。重大なバグや欠陥については、可能な限り迅速にパッチを適用します。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本番環境に戻します。

効果的な管理ツールを使用することでシステムのパッチ適用が最大

**56%** 高速化<sup>8</sup>

## デプロイを自動化する

インフラストラクチャの規模と複雑性が増すにつれ、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、一貫性の向上、定期的なレポート生成のために自動化を使用しましょう。

セキュリティ自動化と人工知能 (AI) を使用することでデータ漏洩のコストを

**39.3%** 削減可能<sup>7</sup>

<sup>7</sup> IBM Security、「[Cost of a Data Breach Report 2023](#)」、2023 年。

<sup>8</sup> IDC ホワイトペーパー (Red Hat 後援)、「[Red Hat Satellite によるエンタープライズ組織の支援: 自動化ツールを使用したインフラストラクチャの最適化](#)」、Document #US46109220、2021 年 8 月。

## ツールを接続し、プロセスを調整する

分散型の環境には、プラットフォームごとに異なる管理ツールが含まれていることがよくあります。アプリケーション・プログラミング・インターフェース (API) を介してそれらのツールを統合し、好みのインターフェースを使用して他のツールのタスクを実行します。使用するインターフェースを減らして運用を効率化し、環境内の全システムのセキュリティとコンプライアンスの状態に対する可視性を向上させます。また、複数環境間でプロセスを調整し、一貫性と信頼性を高めます。

セキュリティシステムが複雑な場合、データ漏洩の平均コストは

**31.6%** 増加<sup>9</sup>

## 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、テクノロジーを組み込んだ包括的なアプローチが求められます。継続的なセキュリティ戦略が先進的な開発技術、DevSecOps、デジタルビジネスのニーズをサポートするためには、フィードバックと適応が欠かせません。環境内のオペレーティングシステム、コンテナ・プラットフォーム、自動化ツール、SaaS (Software-as-a-Service) アセット、クラウドサービスといった各層の機能を最大限に活用するために、階層化された多層防御のセキュリティアプローチを採用しましょう。

DevSecOps アプローチを採用すると、データ漏洩の平均コストを

**38.4%** 削減可能<sup>9</sup>



理想的なセキュリティおよびコンプライアンスツールには、いくつかの主要な特徴と機能があります。

## プロアクティブな分析

セキュリティとコンプライアンスの体制を向上させるには、まずそれを理解することが必要です。自動分析を行うツールがシステムを定期的に監視し、スタッフが多くの時間や労力を費やさなくても、問題があれば確実に警告します。



## 優先度付けされた対処

規範的な修復手順を提供するツールによって、自分でアクションを調査する必要がなくなり、時間を節約してミスのリスクを軽減できます。潜在的な影響と影響を受けるシステムに基づいてアクションに優先順位を付けることで、限られたパッチ適用の機会を最大限に活用できます。

## カスタマイズ可能な成果

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。理想的なツールを使用すると、ビジネスコンテキストを定義して誤検知を減らし、リスクを管理し、セキュリティとコンプライアンスのステータスをより現実的に把握できます。

## 直感的なレポート

パッチが適用されているシステム、パッチ適用が必要なシステム、セキュリティポリシーに準拠していないシステムに関する明確で理解しやすいレポートを生成するツールによって、監査性が向上し、環境のステータスをより深く理解できます。

## 統一されたインタフェース

環境の単一のコンポーネントまたはレイヤーを管理する以上のことができるツールを使用すると、セキュリティ運用が簡素化され、セキュリティとコンプライアンスの体制をより深く把握できるようになります。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。

## 実用的な知見

環境に応じた情報を提供するツールは、存在する潜在的なセキュリティの脆弱性やコンプライアンスの問題、影響を受けるシステム、予想される潜在的な影響をより迅速に特定するのに役立ちます。これらのツールは、修復作業の優先順位付けと計画にも役立ちます。



# 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化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・インフラストラクチャ、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、人材、プロセス、テクノロジーを統合することで、業務効率の達成、イノベーションの促進、従業員満足度の向上を支援します。

この戦略の中核となるのが、**Red Hat Enterprise Linux** です。Red Hat Enterprise Linux は、先進的な IT およびエンタープライズ・ハイブリッドクラウドのデプロイメントに対応するための、一貫性のあるインテリジェントな運用基盤であり、組織に最適なメリットをもたらします。インフラストラクチャ全体で一貫性を保つことができるため、あらゆる場所で同じツールを使っ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、環境を最新の状態に保ち、より安全に保つのに役立ちます。

## 66

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**。<sup>10</sup>

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 の管理ツールは Red Hat Enterprise Linux と統合されており、セキュリティ脆弱性リスクとコンプライアンスを効果的に管理するために必要な機能を提供します。



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、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。



自動化機能により、構成とパッチ適用の精度が向上し、人的ミスが減少します。



カスタマイズ可能なビューは、適切な情報を適切な対象者に適切なタイミングで迅速に提供します。



自動化されたプロアクティブな修復によって問題をより迅速に修正することができ、サポートに連絡する必要がありません。



広範なリソースのライブラリは、詳細的を絞った情報を 24 時間 365 日提供します。



オンサイトおよび SaaS (Software-as-a-Service) オプションを使用すると、好みに応じてツールをデプロイできます。



既存の優先セキュリティ、コンプライアンス、管理ツールおよびインタフェースに API で接続できます。



脆弱性およびマルウェア検出機能がシステムをスキャンし、共通脆弱性識別子 (CVE) およびマルウェアシグネチャを検出します。



リソース最適化機能は、コンピューティング、メモリー、パフォーマンス指標を使用して、パブリッククラウド・デプロイメントを適切なサイズに設定するのに役立ちます。

# 統合ツールを活用する

Red Hat 管理ツールは、Linux の長年の開発とサポートの経験に基づいています。これらは連携して IT 管理を効率化し、チームの時間と労力を節約して、環境をより安全で、最適化された、信頼性の高いものにします。



## Red Hat システムの分析、観察、管理

Red Hat Enterprise Linux に含まれ、サービスとして提供される **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、ハイブリッドクラウド環境をより適切に管理できるようにします。Insights により、IT の効率性、安定性、パフォーマンスを監視し、セキュリティとコンプライアンスのリスクを管理し、クラウド全体の支出を追跡して最適化することができます。

**26%** セキュリティインシデントの解決を迅速化<sup>11</sup>

**24%** IT セキュリティチームの効率が向上<sup>11</sup>

**76%** 予定外のダウンタイムを短縮<sup>11</sup>



## システム管理の効率化と自動化

**Red Hat Satellite** は、物理環境、仮想環境、クラウド、エッジなど、どこであっても Red Hat Enterprise Linux システムをプロビジョニングし維持管理するように作られたインフラストラクチャ管理ソリューションです。プロビジョニング、パッチ適用、その他のシステム管理の繰り返しタスクを大規模に効率化し、システムのセキュリティ、可用性、ポリシーへのコンプライアンスを維持しながら運用効率を向上させます。

**56%** パッチ適用が効率化<sup>12</sup>

**56%** IT インフラストラクチャの効率が向上<sup>12</sup>

**28%** 総運用コストを削減<sup>12</sup>

11 IDC ビジネス価値スナップショット (Red Hat 後援)、「Red Hat Insights のビジネス価値」、Document #US51795124、2024 年 2 月。

12 IDC ホワイトペーパー (Red Hat 後援)、「Red Hat Satellite によるエンタープライズ組織の支援: 自動化ツールを使用したインフラストラクチャの最適化」、Document #US46109220、2021 年 8 月。

## 成功事例を見る

# 英国気象庁

英国の国立気象予報機関である英国気象庁は、世界中の人々に天気や気候に関連したサービスを毎日提供しています。サーバー管理への包括的なアプローチを確立するために、英国気象庁は Red Hat Insights を導入して Red Hat Satellite の使用を補完しました。そして、Red Hat テクニカルアカウントマネージャーのサポートを受けつつ、サーバー環境の可視性を大幅に改善させました。

英国気象庁はまず、既知の問題のあるマシン数台で Insights をテストすることから始めました。問題をすぐに洗い出すことができたので、IT チームはより広範な展開を進めることを決定しました。チームは、社内の変更管理プロセスに従って Satellite を使用し、資産全体への Insights のインストールを簡素化しました。

Insights により、タスクの優先順位付け、問題の有無の確認、影響を受けているシステムや問題の深刻度の把握が極めて容易になりました。また、構成の問題を特定して修正することで、サーバー資産を望ましい基準に近づけるのにも役立ちました。

英国気象庁は、今後も Insights と Satellite を利用して、環境全体を管理し、よりプロアクティブにセキュリティポスチャを改善していく予定です。

66

Red Hat Insights は、トップダウンの概要を提供し、**資産管理に対してより包括的なアプローチ**を採用するのに役立つことが分かりました。Red Hat Satellite は個々のマシンの問題を明らかにすることに長けており、Red Hat Insight は、マシンごとに問題を扱うのではなく、資産全体で共通する問題を結び付けることを強みとしています。

---

**Chris Wilkinson 氏**  
英国気象庁、  
シニアシステムエンジニア

# 今すぐ始めましょう

ビジネスには IT インフラストラクチャとアプリケーションが不可欠です。セキュリティの脆弱性およびコンプライアンスリスク管理の効果的なアプローチとツールを導入することで、組織を保護することができます。

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。



## Red Hat Insights でリスクを分析

- ▶ Red Hat Insights の詳細は[こちら](#)
- ▶ Red Hat Insights に関するアナリストの意見は[こちら](#)

## Red Hat Satellite で大規模に管理

- ▶ Red Hat Satellite の詳細は[こちら](#)
- ▶ Red Hat Satellite に関するアナリストの意見は[こちら](#)