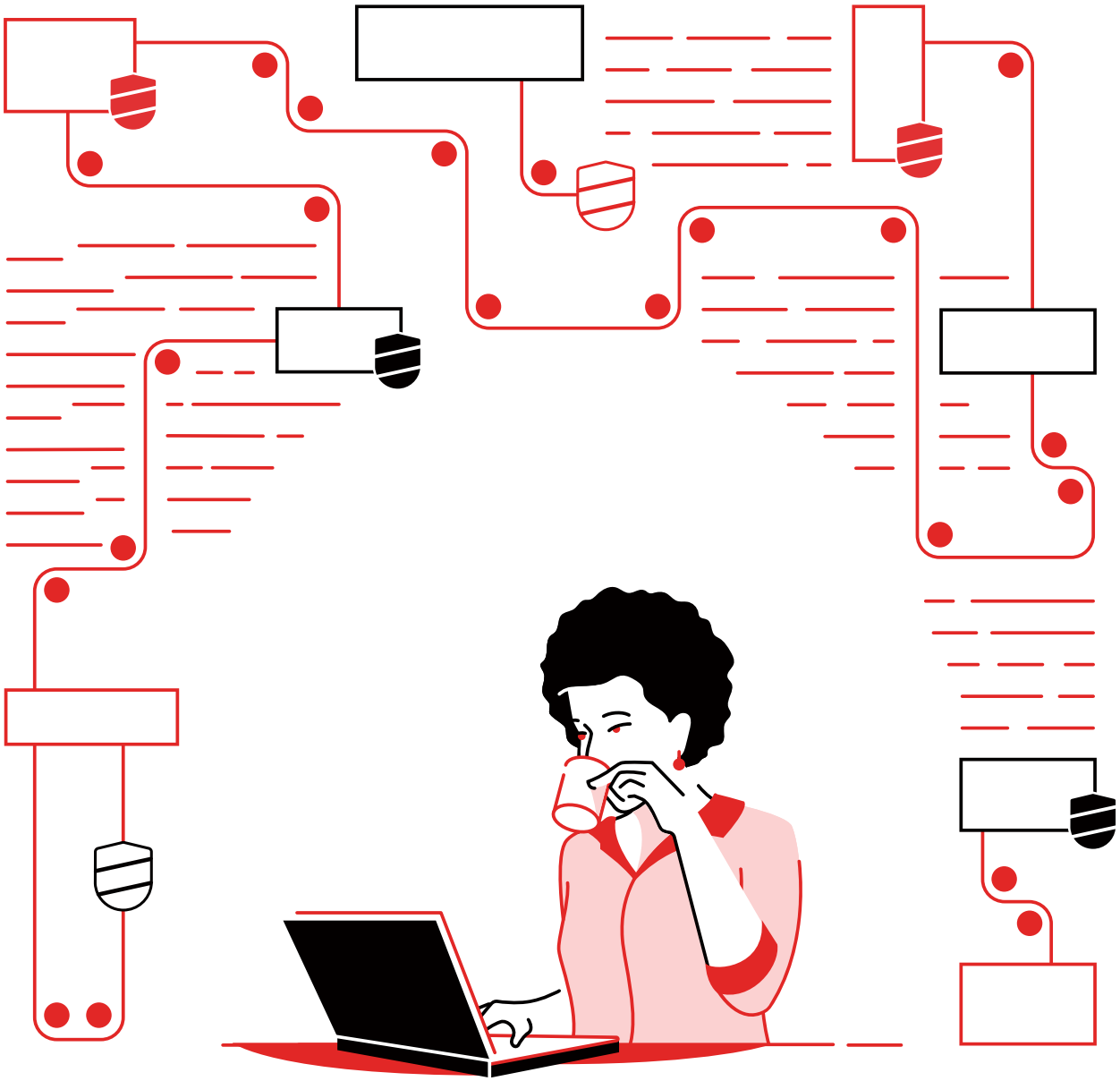
セキュリティ運用センターを単純化する

統合自動化プラットフォームで
高速化、時間の節約、セキュリティの向上を実現



Red Hat

目次

IT セキュリティは最重要事項

ほとんどの組織にとって、セキュリティは主要な問題です。実際、CEO の 33% がサイバー脅威を非常に憂慮しています。[1] この懸念には根拠があり、過去 2 年間に重大なサイバー攻撃を受けた組織は実に 32% にのぼります。[2]

組織を守ることは重要ですが、多くの場合、それは非常に困難なタスクです。セキュリティチームはさまざまなベンダーが提供する複数のツールとサービスを使用して、複雑な環境の構築、維持、管理、調整を行わなければなりませんが、通常それらのベンダー同士は競合状態にあります。提供されるものが年々増加するため、セキュリティ環境の変化に応じて継続的に新製品を調査、評価、統合する必要があります。

さらに、セキュリティ侵害事例の発生件数、重大度、コストは増加し続けています。2 年以内に侵害を被る可能性は 29.6% で、2014 年の 22.6% から増加しています。[3] 1 件の侵害で漏洩するデータレコード数の平均は、2018 年から 2019 年にかけて 3.9% 増加しました。[3] また、データ漏洩の平均損害額は、2019 年に 392 万ドルまで増加しました。[3]

ほとんどの組織はセキュリティ運用を手動で行っています。人による作業が必要な場合、セキュリティ関連のタスクには時間がかかり、面倒で、エラーの入り込む余地が必ず生じます。その結果、セキュリティチームは多忙を極めることになります。彼らは多くのツールが発する脅威アラートの増加に直面しています。事実、セキュリティチームの 60% が 1 日に 5,000 件以上のアラートを受信し、16% が 100,000 件以上を受信しています。[4]

また、インフラストラクチャの規模が拡大して複雑さが増すと、脆弱性の特定と侵害の検証がさらに困難になります。ほとんどのセキュリティツールは相互に統合されていないため、セキュリティスタッフの手作業が増えることになります。これに応じて、インシデントの調査と対応にかかる時間が増加しています。2019 年、データ漏洩の特定と阻止にかかった平均時間は 279 日で、2018 年から 4.9% 増加しました。[3] チームを拡大して維持するための新しい人材を探すことは難しく、2019 年には 39% の組織がサイバーセキュリティのスキルが不足していると報告しています。[2] また、サイバーセキュリティにかける予算も限られています。高度なサイバーレジリエンスを実現できる十分な資金があると報告している組織はわずか 33% です。[5]

その結果、典型的なセキュリティチームが内容を確認して対応するアラートは、受信するアラートの 48% に過ぎず、現実に存在する脅威のうち対策されるのは 50% にとどまっています。[4] こうして、多くの組織が攻撃に対して脆弱になります。

77% セキュリティ・エコシステムの単純化と対応時間のスピードアップを図るために自動化の拡大を計画している組織の割合。[4]

効果のないセキュリティの影響

セキュリティ侵害事例の発生件数、重大度、コストは増加し続けています。

392 万米ドル
2019 年のデータ漏洩の平均損害額[3]

279 日
2019 年のデータ漏洩の特定と阻止にかかる平均時間[3]

122 万米ドル
漏洩の特定と阻止を
200 日
以下で行えた場合に防げる損害額[3]

29.6%
2 年以内に侵害を受ける可能性[3]

50%
現実の脅威が対策される割合[4]

1 PWC、「23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty」、2020 年。pwc.com/ceosurvey

2 Harvey Nash and KPMG、「CIO Survey 2019: A Changing Perspective」、2019 年。home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html

3 IBM Security、「2019 Cost of a Data Breach Report」、2019 年。ibm.com/security/data-breach

4 Cisco、「Cisco Benchmark Study: Securing What's Now and What's Next」、2020 年 2 月。cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

5 Ponemon Institute、IBM Security 後援、「The Cyber Resilient Organization」、2019 年 4 月。ibm.com/account/reg/us-en/signup?formid=urx-37792

セキュリティの自動化とは

セキュリティの自動化とは、企業のセキュリティ体制の維持に関連する手動タスクを自動化することです。複数の実践項目で構成されており、ここではそれらを次の 4 つの一般的なカテゴリに分類します。

対応と対策
セキュリティアナリストの関与、ガイダンス、またはその両方を含むイベント駆動型のアクティビティ

セキュリティ運用
テクノロジーチームがセキュリティ・インフラストラクチャで実行する日常的なプロセスおよびポリシー駆動型のアクティビティ

セキュリティ・コンプライアンス
インフラストラクチャをセキュリティポリシーと規制に確実に準拠させるためのアクティビティ

強化
意図と目標に沿ってインフラストラクチャにカスタム・セキュリティ・ポリシーを適用するアクティビティ

セキュリティ・コンプライアンスと強化についてさらに詳しく

以下のリソースでは、自動化がセキュリティ・コンプライアンスと強化にどう役立つかをご紹介しています。

- **e ブック：ハイブリッドクラウド・セキュリティを強化する**
- **概要：セキュリティとコンプライアンスを自動化する理由**
- **データシート：Red Hat Services - セキュリティと信頼性のワークフローを自動化**

この e ブックは、対応と修正のアクティビティ、およびセキュリティ運用の自動化に焦点を当てています。

セキュリティ運用、および対応と対策のアクティビティを自動化するメリット

スピードと効率の向上

自動化によりタスクが効率化され、手作業が不要になります。その結果、セキュリティ運用に要する時間が短縮されるので、スタッフは高い価値を生み出す活動に携わる時間と余裕を取り戻すことができます。また、自動化は IT インフラストラクチャの複雑さの軽減にも貢献します。高度に自動化されている組織の 40% が、使用しているセキュリティ・ソリューションとテクノロジーの数は適切であると回答しています。[6]

セキュリティを大規模に拡大

セキュリティ・インフラストラクチャ全体に自動化を適用すると、一貫性が向上し、より包括的なアプローチでセキュリティに取り組むことが可能になります。各スタッフメンバーが管理できるツール、デバイス、システムが増えるため、大規模な運用が可能です。また、自動化によって人的ミスのリスクも軽減され、精度が向上します。

侵害のリスクと損害を削減

広範囲に自動化を導入している組織は、セキュリティインシデントやビジネスの混乱をうまく回避できます。[6] セキュリティ自動化をフルデプロイすると、1 件の侵害によって生じる損害額は平均で 95% 削減されます。[7] その結果、ある程度のセキュリティ自動化をデプロイした組織は 52%、今後 24 カ月以内にセキュリティ自動化のデプロイを計画している組織は 36% にのぼります。[7]

6 Ponemon Institute、IBM Security 後援、「The Cyber Resilient Organization」、2019 年 4 月。ibm.com/account/reg/us-en/signup?formid=urx-37792

7 IBM Security、「2019 Cost of a Data Breach Report」、2019 年。ibm.com/security/data-breach

自動化はセキュリティツール、システム、プロセスを統合する

一貫性のある柔軟なプラットフォームで人、プロセス、ツールを一体化する

自動化プラットフォームは、セキュリティチーム、ツール、プロセス間の統合レイヤーとして機能します。柔軟で相互運用可能なプラットフォームにより、次のことが可能になります。

- セキュリティシステム、ツール、チームをつなげる
- システムから情報を収集し、それを事前定義済みのシステムと場所に手作業を介さずにすばやく転送する
- 一元化されたインタフェースから構成をすばやく変更して伝達する
- セキュリティツールとプロセスに関連するカスタム自動化コンテンツを作成、維持、利用する
- 脅威が検出されたときに、複数のセキュリティツール全体で自動化されたアクションをトリガーする

組織全体で一貫した自動化プラットフォームと言語を使用すると、コミュニケーションとコラボレーションも向上します。セキュリティ・ポートフォリオ内のあらゆるソリューションが同じ言語で自動化されている場合、アナリストとオペレーターの両方がどの製品でも一連のアクションをわずかな時間で実行でき、セキュリティチームを全体的に最大限効率化できます。また、共通のフレームワークと言語により、セキュリティチームと IT チームは設計、プロセス、アイデアをチーム内および組織全体でより簡単に共有できるようになります。

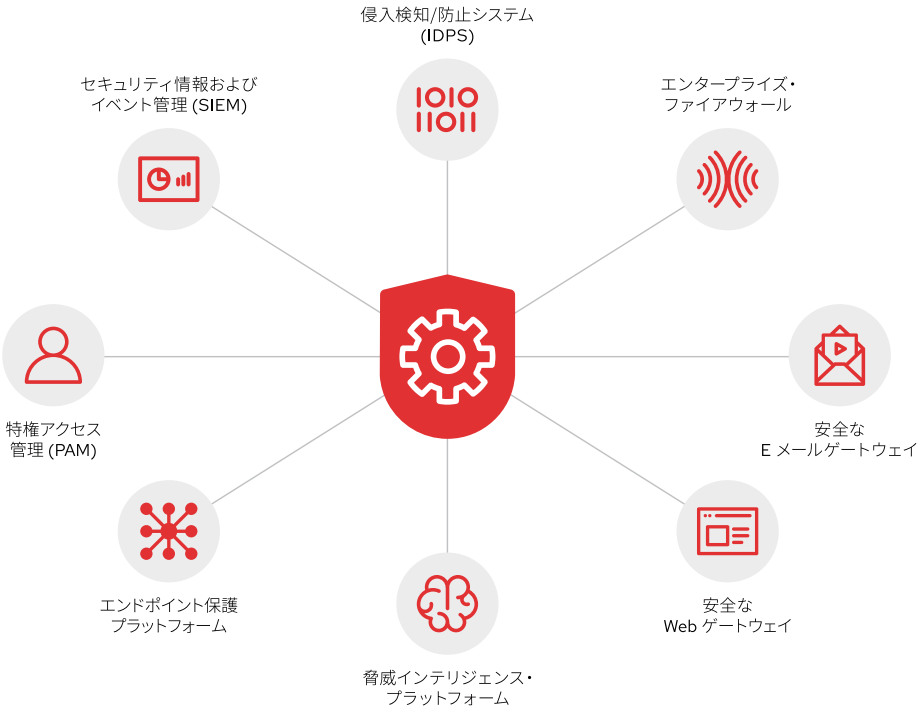


図 1. セキュリティシステム、ツール、チームをつなげる自動化プラットフォーム

自動化の成功 = 人材 + プロセス + プラットフォーム

ツールだけでは自動化の価値を最大化することはできません。人材、プロセス、プラットフォームも考慮する必要があります。

- **人材**はあらゆるビジネスイニシアチブの中核にあります。スタッフがチーム内で、またチームの壁を越えて関わり合うことにより、アイデアを共有し、より効果的にコラボレーションできます
- **プロセス**は組織内のプロジェクトを開始から終了まで進めるためのものです。効率的な自動化を行うためには、プロセスを明確化して、それを文書化することが不可欠です。
- 自動化**プラットフォーム**は、自動化アセットの構築、実行、管理に必要な機能を提供します。シンプルな自動化ツールとは異なり、自動化プラットフォームは一貫性のある自動化コンテンツと知識を大規模に作成、デプロイ、共有する統一された基盤となります。

e ブックを読む

セキュリティの自動化はプロセスである

組織が実装する自動化はどのようなものであれ、一晩で終わるものではなく、すべて自動化するか、まったく自動化しないかの二択でもありません。セキュリティの自動化はプロセスです。どこから開始するか、またどこまででやめるかは、各組織のニーズによって異なります。たどる道筋も、ニーズによって決定されます。いずれにせよ、組織がプロセスのどの時点にあるかにかかわらず、セキュリティ自動化の取り組みはたとえ小規模なものでもメリットがあります。

セキュリティ自動化の成熟度を評価する

セキュリティ自動化の成熟度は大きく 3 つの段階に分けることができ、ほとんどの組織はそのいずれかに分類されます。現在の段階を知ることで、組織は適切なツールとプロセスを適切なタイミングで導入し、自動化を成功させることができます。

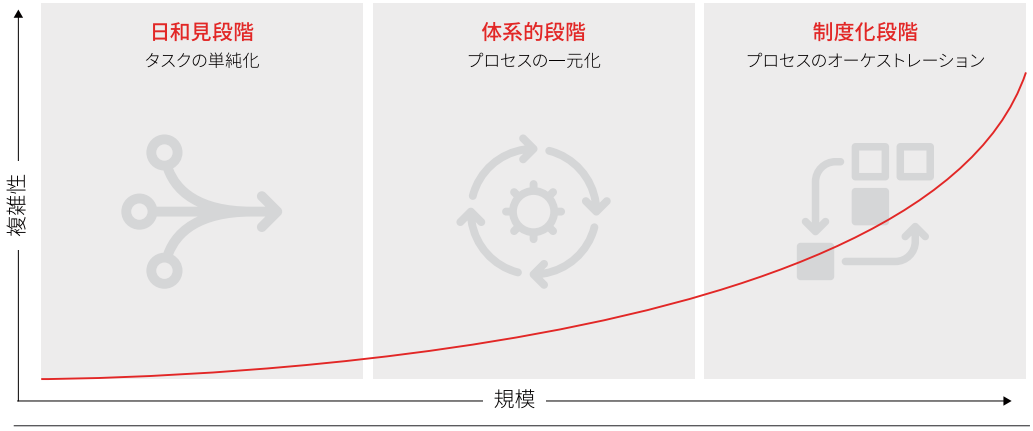


図 2. セキュリティ自動化の成熟度の段階

段階 1：日和見

この段階におけるセキュリティ運用の自動化は、主に時間の節約を主眼として行われます。目標として一般的なものには、類似のデバイスやテクノロジー全体でのセキュリティアクションの標準化、さまざまなベンダーの製品すべてで実行される手動タスクの最適化などがあります。

段階 2：体系的

この段階では、セキュリティ運用ツールとサービスをまとめてセットで導入することによるプロセスと効率の向上が中心的な目的となります。目標として一般的なものには、上位レベルのワークフローへのセキュリティプロセスの組み込み、セキュリティ対応プロセスの一元化などがあります。

段階 3：制度化

この段階では、組織全体のコラボレーションの強化とセキュリティの統合に注力します。目標として一般的なものには、セキュリティのあらゆる側面に及ぶプログラム化された自動化ワークフローの作成、セキュリティと IT テクノロジーの統合などがあります。

ブログを読む

ユースケースと統合

セキュリティ自動化の道筋を定義する

セキュリティ自動化の一般的な概要レベルのユースケース

以下で紹介する各ユースケースは、セキュリティ自動化の出発点になります。重要なのは、シンプルなものから小さく始め、時間をかけて徐々に構築していくことです。

調査の強化

セキュリティアラートとインシデントの調査では、さまざまなセキュリティシステムから情報を収集して、現実にイベントが発生したかどうかを評価します。通常、情報はユーザー・インタフェース、E メール、電話を通じて集められます。この非効率なプロセスによって脅威に対するアクションが遅れるため、ビジネスは脆弱なままになり、侵害に起因する潜在的な損害額は増加します。自動化により、セキュリティシステム全体にわたって情報をプログラムで組み立てることができ、セキュリティ情報およびイベント管理 (SIEM) システムを通じて実行されるトリアージアクティビティをオンデマンドで強化することが可能になります。その結果、アラートとインシデントをより迅速に評価し、対応することができます。

脅威ハンティング

脅威ハンティングでは、セキュリティに対する潜在的な脅威を予防的方法で特定して調査します。このケースでもインシデント調査と同様、スタッフは複数のシステム間で手動で情報を収集して送信します。自動化によって、アラート、相関検索、署名操作をカスタマイズして最適化し、潜在的な脅威をより迅速に調査することが可能になります。また、SIEM 相関クエリと侵入検知システム (IDS) ルールを自動的に作成および更新して、検出性能を向上させることもできます。その結果、組織のセキュリティ防御をより頻繁かつ効率的に更新して、ビジネスをより適切に保護できます。

インシデント対応

インシデント対応では、侵害の継続を阻止するためのアクションを取ります。侵害が発見されると、セキュリティスタッフはそれを阻止するために迅速かつ大規模に対応する必要があります。しかし、多くの場合、対応アクションには複数の手動タスクが含まれているので対策の実施に時間がかかり、組織が脆弱な状態が長時間続くことになります。自動化によって、アクションを繰り返し可能な事前承認済みの Playbook にコード化することで、対応を迅速化できます。IP アドレスやドメインへの攻撃のブロック、脅威ではないトラフィックの許可、悪用された資格情報の凍結、インシデントに関連する損害を最小化するためにさらに調査をする際の疑わしいワークロードの分離などのタスクをスピードアップできます。

統合は不可欠

一元化した自動化アプローチでは、自動化プラットフォームとセキュリティテクノロジーを統合する必要があります。統合が欠かせない要素には次のものがあります。

- **ファイアウォール**：ネットワーク間のトラフィックフローを制御し、インターネットに公開されたアプリケーションを保護します。自動化により、ポリシーを高速化し、構成の変更を記録できます。
- **侵入検知/防止システム (IDPS)**：疑わしいアクティビティがないかネットワークトラフィックを監視し、脅威アラートを発行して、攻撃をブロックします。自動化により、ルールとログの管理を単純化できます。
- **セキュリティ情報とイベント管理システム**：セキュリティイベントを収集して分析し、脅威の検出と対応に役立ちます。自動化により、プログラムによるデータソースへのアクセスを提供できます。
- **特権アクセス管理 (PAM) ツール**：特権アカウントとアクセスを監視および管理します。自動化により、資格情報管理が最適化されます。
- **エンドポイント保護システム**：デバイスを監視および管理して、セキュリティを向上させます。自動化により、一般的なエンドポイント管理タスクを単純化できます。

詳細はこちら

Red Hat Ansible Automation Platform でセキュリティ運用センターを単純化する

自動化ソリューションは多数存在していますが、そのすべてが効果的なセキュリティの自動化に必要な機能を備えているわけではありません。以下のような特徴を持つ自動化プラットフォームを探してください。

- **汎用性が高く、利用しやすい自動化言語。** 理解しやすく簡単に作成できる言語を使用すると、専門知識の領域が異なるセキュリティチームのメンバー間で情報を文書化して共有できます。
- **オープンで公平なアプローチ。** 自動化プラットフォームを効果的にするには、セキュリティ・インフラストラクチャ全体およびベンダーエコシステムと相互運用する必要があります。
- **モジュール式で拡張可能な設計。** モジュール式プラットフォームにより、自動化を段階的にデプロイできます。拡張性を有することで、必要に応じて、他のベンダーが今後提供するセキュリティツールを追加することもできます。

Red Hat でセキュリティ組織を前進させる

自動化サービスの広範な構築と運用の基盤となる **Red Hat® Ansible® Automation Platform** は、セキュリティ自動化の実装に必要なすべてのツールと機能を提供します。シンプルで読みやすい自動化言語と、信頼できる構成可能な実行環境、セキュリティを重視した共有機能およびコラボレーション機能を同時に実現しています。オープンな基盤により、セキュリティと IT インフラストラクチャのほぼすべてをつないで自動化し、組織全体の参加と共有を実現する共通のプラットフォームを作成できます。Red Hat Ansible Automation Platform は、IT やネットワークの運用、DevOps など、他の分野でも実績を上げています。

サポート付きの、**セキュリティに重点を置いた Ansible コレクション**(モジュール、ロール、Playbook など) がプラットフォームに含まれています。これらのアセットは種類の異なるセキュリティ・ソリューションのアクティビティを連携させ、サイバー脅威とセキュリティ運用へのより一貫した対応を実現します。

- ワークフローと Playbook を結びつけて、モジュールの再利用性を高める
- ログを統合して一元化する
- ローカルのディレクトリサービスとアクセス制御をサポートする
- RESTful アプリケーション・プログラミング・インタフェース (API) を使用して外部アプリを統合する

Red Hat Ansible Automation Platform には、自動化を最適化するのに役立つツールと機能も含まれています。**Automation Analytics** は、組織における自動化の使用方法について知見を提供します。**Automation Hub** はチームメンバーが一元的なリポジトリから認定済みの自動化コンテンツにアクセスできるようにします。そして、**Content Collections** は自動化アセットの管理、配信、使用を効率化します。

エキスパートのサポートを受ける

Red Hat は、自動化をスムーズにデプロイできるようサポートします。

- **Red Hat サービス・プログラム：Automation Adoption** は、組織全体に自動化を導入するプロセスを管理するためのフレームワークを提供します。
- **Red Hat トレーニングと認定**は、自動化をより効果的に使用するための実践的なトレーニングと実用的な認定を提供します。
- **Red Hat サポート**はお客様と連携して、IT のプロセスを成功に導きます。受賞歴を誇る Web サポート [8] には、ベストプラクティス、ドキュメント、更新、セキュリティアラート、パッチへのアクセスが含まれます。また、サポートエンジニアやテクニカルアカウントマネージャーに連絡して問題を解決したり、専門的なガイダンスを得たりすることもできます。
- **認定パートナーのコンテンツコレクション**を使用して、さまざまなベンダーのハードウェアとソフトウェアを手軽に自動化できます。この信頼できるビルド済みの自動化コンテンツは、Automation Hub を通じて利用でき、Red Hat とパートナーの両方がサポートしています。

8 Red Hat カスタマーポータルの受賞歴、access.redhat.com/recognition

自動化の事例

実証済みのビジネス価値を提供する Red Hat Ansible Automation Platform

Red Hat Ansible Automation Platform によって、より効率的で最適化された方法でセキュリティ運用センターを自動化できます。Red Hat Ansible Automation Platform を使用する組織のアナリスト調査では、測定可能なビジネス価値が示されています。**IDC** は実際に Red Hat Ansible Automation Platform の使用経験について複数の意思決定者にインタビューを行い、各組織が自動化によって顕著な生産性とアジリティの向上、および運用上のメリットを実現したと報告しています。

IT セキュリティチームの効率と生産性の向上[9]

セキュリティインシデント緩和の効率の向上[9]

セキュリティパッチの効率の向上[9]

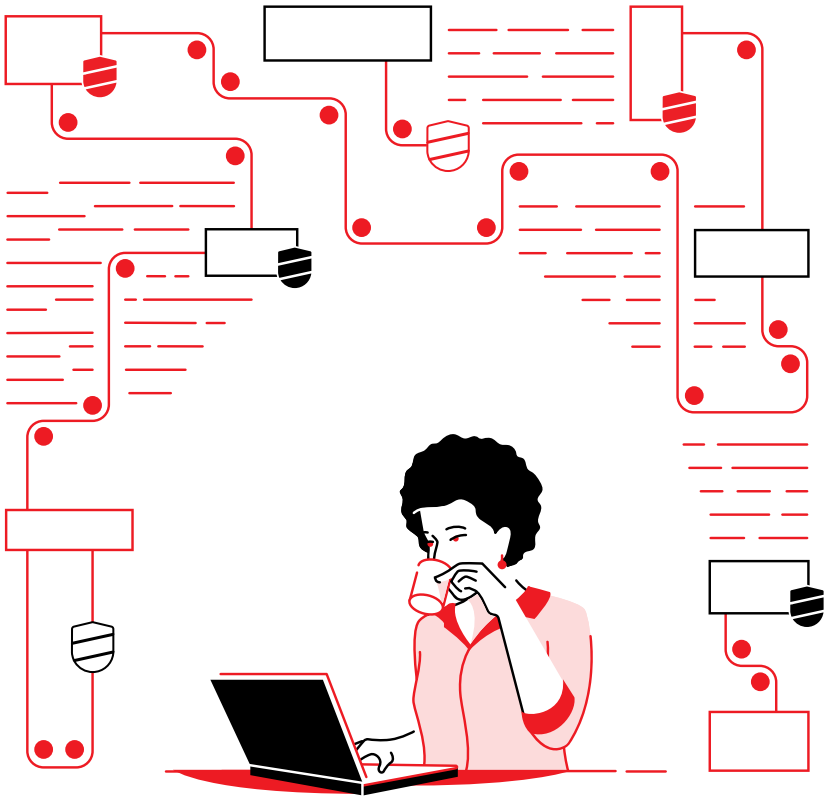
「Red Hat Ansible (Automation Platform) は、IT チームを一つにまとめる驚異的なツールです。サーバー、セキュリティ、ネットワーク、データベースの各チームは、それぞれ別々の層で作業してから、Red Hat Ansible Automation を使用して独自の Playbook を作成できます。」[9]

アナリストレポートを読む

9 Red Hat 後援の IDC ホワイトペーパー。「Red Hat Ansible Automation、IT のアジリティ向上と市場投入時間の短縮を実現」、2019 年 6 月。**redhat.com/ja/resources/business-value-red-hat-ansible-automation-analyst-paper**

セキュリティ運用センターの単純化を始めましょう

自動化によって、増大するセキュリティの脅威を迅速かつ大規模に特定して対応することができます。Red Hat は、セキュリティチーム、ツール、プロセスを一貫性のある協調的な自動化プラットフォームと結びつけて、お客様のビジネスを守るお手伝いをします。



Red Hat Ansible Automation Platform によるセキュリティ自動化の詳細は、**red.ht/automate-security** をご覧ください。

F24343_0720_KVM

Red Hat