

Cisco Secure Workload の新機能

初版：2022年5月19日

最終更新：2022年7月11日

リリースバージョン 3.7.1.5

Cisco Secure Workload リリース 3.7.1.5 の機能

機能名	説明
エージェントとエージェントレスのマイクロセグメンテーション	
Azure コネクタ検出のワークフローのサポート	<p>Cisco Secure Workload 3.7 は、Cloud Connector を使用して Azure と Azure Kubernetes Services (AKS) をサポートします。</p> <p>Azure クラウドコネクタを作成し、メタデータの取り込みを有効にして、Azure ベースのワークロードからラベルとフローデータを取り込み、ネットワークセキュリティグループ (NSG) を介してポリシーを適用できるようになりました。各ワークロードにエージェントをインストールする必要はありません。</p> <p>Azure コネクタを使用して、AKS で実行されている Kubernetes ワークロードからラベルを取得することもできます。</p> <p>この機能はベータ版です。</p> <p>詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「<i>Azure Connector</i>」を参照してください。</p>
マネージド Kubernetes サービスのサポート：GKE	<p>Cisco Secure Workload 3.7 は、Google Cloud Platform (GCP) コネクタを使用したマネージド Kubernetes サービスをサポートするようになりました。</p> <p>GCP コネクタは、Google Kubernetes Engine (GKE) を介して展開および管理されるコンテナのセグメンテーションとフローの可視性をサポートしており、選択したすべての Kubernetes クラスタからノード、サービス、ポッドのメタデータを収集するのに特に役立ちます。</p> <p>GCP コネクタの使用方法の詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「<i>Managed Kubernetes Services Running on GCP (GKE)</i>」の項を参照してください。</p>

機能名	説明
FQDN/DNS ドメイン名ベースのフローの可視性	<p>Cisco Secure Workload 3.7 リリースから、コンシューマとプロバイダーに関連付けられた FQDN/DNS ドメイン名を表示するための新しいオプションが [フロー検索 (Flow Search)] ページに導入されました。</p> <p>[フィルタ検索 (Flow Search)] ページにあるテーブルフィルタは、IP アドレスに基づいてフィルタ処理できるドメイン名を表示するように構成できるようになりました。[フロー検索 (Flow Search)] テーブルは、IP アドレスに関連付けられたコンシューマとプロバイダーのドメイン名を表示するように構成できるようになりました。</p> <p>テーブルフィルタの構成方法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。</p>
パブリッククラウドの Kubernetes サービスオブジェクトタイプのロードバランサのサポート	<p>このリリースでは、ワークロードからメタデータを収集するために、パブリッククラウドプラットフォーム用の Kubernetes ロードバランササービスが導入されました。</p> <p>[ワークロードインベントリ (Workloads Inventory)] ページの [サービス (Services)] タブで、ロードバランサのリストと、他の方法では外部オーケストレータを介してのみ検出された他の Kubernetes サービスを表示できるようになりました。</p> <p>この詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。</p>
新しいメニュー項目	<p>Cisco Secure Workload 3.7 では、セキュアコネクタクライアントのメトリックが [外部オーケストレータ (External Orchestrators)] ページから移動されました。</p> <p>この変更により、ステータス行をクリックするだけで、[セキュアコネクタ (Secure Connector)] ページで追加のクライアントメトリックを表示できます。これらのメトリックは、[一般 (General)] 列、[インターフェイス (Interface)] 列、および [ルート (Routes)] 列の下に表として表示されるため、エラーのトラブルシューティングに関連する情報を見つけるのに役立ちます。</p> <p>詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「<i>Secure Connector</i>」の項を参照してください。</p>
KVM ベースの仮想アプライアンス (Edge と Ingest)	<p>Cisco Secure Workload 3.6 以前のリリースには、ESXi ホスト用の OVA テンプレートをダウンロードするための規定がありました。Cisco Secure Workload 3.7 以降では、QCOW2 イメージをダウンロードして、KVM ベースの環境に Cisco Secure Workload 仮想アプライアンス (Ingest と Edge) を展開できます。</p> <p>詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドの「<i>Virtual Appliances for Connectors</i>」の項を参照してください。</p>

機能名	説明
エージェント展開の強化	<p>Cisco Secure Workload 3.7 リリースでは、インストーラスクリプトが拡張され、スクリプトの使用を制限できるようになりました。これにより、スクリプトの使用方法をより詳細に制御できます。</p> <p>このリリースから、インストーラスクリプトを使用する期間を、利用可能な一連のオプションから実際に選択できるようになりました。</p> <p>その方法の詳細については、Cisco Secure Workload オンラインヘルプまたはユーザーガイドの「<i>Install the Agent</i>」の項を参照してください。</p>
ユーザーエクスペリエンスの向上	
ヘルプメニューの向上	<p>Cisco Secure Workload 3.7 リリースでは、UI の [ヘルプ (Help)] メニューが大幅に拡張され、ユーザーが探している情報にアクセスできるようになりました。</p> <p>ヘルプメニューには、ページレベル (状況依存) のヘルプ、ドキュメントセット/ビデオへの簡単なアクセスなど、役立つリンクがいくつかの追加されました。特定のリリースの新機能、[ソフトウェアダウンロード (Software Download)] ページへのクイックアクセス、プラットフォーム情報、サポートされているオペレーティングシステムと要件、およびクリックするだけで他の多くの情報の確認できます。</p>
オーケストレータ構成とコネクタ構成の DBR バックアップ/復元	<p>このリリースでは、データのバックアップと復元機能が拡張され、外部オーケストレータとコネクタの構成が含まれるようになりました。</p> <p>この機能強化により、Cisco Secure Workload クラスタのデータと構成を別のオフサイトストレージにコピーできるようになりました。また、これには、外部オーケストレータのこれらの構成も含まれます。障害や事故が発生した場合、これらのストレージにバックアップされたデータを使用して、新しいシステムを簡単に復元できます。</p> <p>拡張機能については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。</p>
新しいクイックスタートウィザード	<p>現在、スコープが定義されていない場合、このリリースから、スコープツリーの最初のブランチを作成する手順を案内できる新しいウィザードが用意されています。これは、選択したアプリケーションのポリシーを検出して適用するための最初のステップです。</p> <p>このウィザードは、ラベル、スコープ、および階層型スコープツリーの機能を説明し、これらの概念すべてがどのように関連しているかを示します。</p> <p>詳細については、『Cisco Secure Workload Quick Start Guide』を参照してください。</p>

機能名	説明
ポリシー管理のワークスペースの向上	<p>各スコープのポリシーを操作するときに表示されるワークスペースが再設計され、セグメンテーションの目標を達成しやすくなりました。</p> <p>変更の中で「ADM」は、この強力な機能が実際に行うことをより適切に反映するため、名前が「ポリシーの自動検出」に変更されました。</p> <p>ワークスペースの改善の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。</p>
ラベルの影響分析	<p>Cisco Secure Workload 3.7 では、ユーザー定義ラベルが拡張され、カスタムラベルの使用方法が表示されるようになりました。</p> <p>[ユーザーがアップロードしたラベル (User Uploaded Labels)] ページで、これらのカスタムラベルを使用して、インベントリ、スコープ、またはフィルタの使用状況を表示できるようになりました。これらのカスタムラベルのいずれかを編集する必要がある場合は、使用状況を表示することが重要です。これは、変更がこれらのカスタムラベルを使用するスコープ、フィルタ、およびポリシーに直接影響するためです。</p> <p>これらの使用法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドを参照してください。</p>
古いエージェントレコードの自動クリーンアップ	<p>多くの実環境展開では、古いエージェントレコードが仮想マシンに蓄積されるいくつかのインスタンスが存在する可能性があり、これにより、最終的にエージェント ステータス アラートのデータベースが増大します。</p> <p>Cisco Secure Workload リリース 3.7 を起動すると、VM 上の非アクティブなエージェントをクリーンアップするプロセスが自動化されるため、指定した期間が経過した後に非アクティブなエージェントを削除するという手間のかかる手動タスクが不要になります。</p> <p>指定した期間内にエージェントで自動クリーンアップを有効にする方法の詳細については、Cisco Secure Workload のオンラインヘルプまたはユーザーガイドの「<i>Creating an Agent Config Profile</i>」の項を参照してください。</p>
IPv6 サポート (デュアルスタックモード)	IPv6 サポートの要件と制限については、cisco.com の『Cisco Secure Workload Upgrade Guide』を参照してください。
Microsoft Edge ブラウザのサポート	このリリースで Microsoft Edge ブラウザのサポートが導入されました。
統合とエコシステム	

機能名	説明
Cisco Secure Firewall Management Center の統合	<p>Cisco Secure Workload 3.7 リリースでは、Secure Firewall Management Center (FMC) の統合により、Cisco Secure Workload (CSW) のスケールロードをより適切に管理できるようになりました。</p> <p>CSW は数千の IP アドレスをスケールアップでき、ハイエンドアプライアンスでは 150 万に達することもあり、動的オブジェクトのマッピング数は最大 300k に達することもあります。ただし、動的オブジェクトごとに数千のマッピングを行う場合、統合がどのように動作するかはまだ明確ではありませんでした。さらに、アグレッシブすぎる統合を避けるために FMC に設定された「要求制限」があり、この制限では単一の IP から 1 分あたり 120 件を超える要求は許可されませんでした。</p> <p>このスケールロードの管理方法の詳細については、『Secure Firewall Management Center and Secure Workload Integration Guide』を参照してください。</p>
Cisco Secure Firewall Management Center のルール順序の管理	<p>Cisco Secure Workload 3.7 では、Cisco Secure Workload (CSW) の [外部オーケストレータ (External Orchestrator)] ページから Cisco Secure Firewall Management Center (FMC) で Cisco Secure Workload ルールの順序を構成するためのサポートが提供されています。</p> <p>この機能強化により、Cisco Secure Workload ルールがリストされる順序を、FMC の既存のアクセス制御ルールの上または下に指定できるようになりました。さらに、FMC でのアクセス制御ポリシーのデフォルトアクションの代わりに、Cisco Secure Workload からのキャッチルールを使用するオプションを有効にすることもできます。これらの機能は、Cisco Secure Workload の [外部オーケストレータ (External Orchestrator)] ページで構成されるようになりました。</p> <p>詳細については、『Cisco Secure Workload and Firewall Management Center Integration Guide』を参照してください。</p>

Cisco Secure Workload リリース 3.7.1.5 の新しいハードウェア機能

このリリースでは新しいハードウェア機能はありません。

Cisco Secure Workload リリース 3.7.1.5 で廃止された機能

表 1: Cisco Secure Workload リリース 3.7 で廃止された機能

機能	機能説明
Neighborhood アプリケーションの廃止	<p>Cisco Secure Workload 3.7.1.5 リリースでは、次の機能がサポートされなくなりました。</p> <ul style="list-style-type: none">パフォーマンス モニターリング見張りハードウェアエージェント構成とハードウェアエージェントのダウンロードダッシュボードフロー、ダッシュボードビュー、ダッシュボードカスタムソフトウェアエージェントからのユニバーサル可視性エージェントのタイプ

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。