Cisco Secure Workload リリース 3.8.1.1 リリースノート

初版：2023 年 5 月 19 日

はじめに

このマニュアルでは、Cisco Secure Workload ソフトウェアリリース 3.8.1.1 の機能、不具合、および制限について説明します。

Cisco Secure Workload プラットフォーム（旧称 Cisco Tetration）は、ファイアウォールとセグメンテーション、コンプライアンスと脆弱性の追跡、動作ベースの異常検出、およびワークロードの分離を使用して、オンプレミスやマルチクラウド環境全体のすべてのワークロードにマイクロ境界を確立することにより、包括的なワークロードセキュリティを提供するように設計されています。このプラットフォームでは、高度な分析とアルゴリズムのアプローチを使用して、これらの機能を提供します。

このソリューションは、次の機能をサポートしています。

- アプリケーションの通信パターンと依存関係の包括的な分析から自動的に生成されるマイクロセグメンテーション ポリシー。
- ロールベースのアクセス制御による複数のユーザーグループの包括的な制御をもたらす、階層型ポリシーモデルを使用した動的なラベルベースのポリシー定義。
- ネイティブ オペレーティング システム ファイアウォール、および ADC（アプリケーション デリバリ コントローラ）や物理ファイアウォールまたは仮想ファイアウォールなどのインフラストラクチャ要素の分散制御による、一貫したポリシーの大規模な適用。
- すべての通信のほぼリアルタイムのコンプライアンス モニタリングにより、ポリシー違反または潜在的な侵害を特定して警告。
- ワークロード動作の基準値設定とプロアクティブな異常検出。
- 動的な緩和と脅威ベースのワークロード分離を行う、一般的な脆弱性の検出。

Cisco Secure Workload プラットフォーム内での分析とさまざまな使用事例をサポートするため、環境全体からの一貫したテレメトリ（フローデータ）が必要です。Cisco Secure Workload は、ソフトウェアエージェントやその他の方法を使用して豊富なテレメトリを収集し、データセンターのインフラストラクチャ内にある既存と新規の両方のインストールをサポートします。

このリリースでは、次のテレメトリソースがサポートされています。

- 仮想マシンおよびベアメタルサーバーにインストールされている Cisco Secure Workload エージェント。
- コンテナホストのオペレーティングシステムで実行されている DaemonSet。
- ミラーリングされたパケットから Cisco Secure Workload テレメトリを生成できる ERSPAN コネクタ。
- アプリケーション デリバリ コントローラ（ADC）からのテレメトリの取り込み：F5 と Citrix。
- Cisco Secure Workload テレメトリベースの NetFlow v9 または IPFIX レコードを生成できる NetFlow コネクタ。
- NetFlow セキュアイベントロギング（NSEL）テレメトリを収集するための ASA コネクタ。
- VPC フローログ構成を使用して生成されたフローテレメトリデータ用の AWS コネクタ。
- NSG フローログ構成を使用して生成されたフローテレメトリデータ用の Azure コネクタ。
- GCP データシンクを使用して生成されたフローテレメトリデータ用の GCP コネクタ。

さらに、このリリースでは、以下との統合によるエンドポイントデバイスのポスチャ、コンテキスト、およびテレメトリの取り込みもサポートされています。

- ラップトップ、デスクトップ、スマートフォンなどのエンドポイントデバイスにインストールされた Cisco AnyConnect。
- Cisco Identity Services Engine

また、Cisco Secure Workload エージェントは、アプリケーション セグメンテーションのポリシー適用ポイントしても機能します。このアプローチを使用して、Cisco Secure Workload プラットフォームは、パブリック、プライベート、およびオンプレミスの展開全体で一貫性のあるマイクロセグメンテーションを実現します。エージェントはネイティブのオペレーティングシステム機能を使用するポリシーを適用し、データパスにエージェントを置く必要がなく、フェールセーフなオプションが提供されます。その他の製品マニュアルについては、「関連資料」の項を参照してください。

リリースノートは、制限や不具合に関する新しい情報によって更新されます。このドキュメントの最新バージョンについては、次の Web サイトを参照してください。

http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.html

次の表に、このリリースの履歴を示します。

日付	リリース情報
2023 年 5 月 19 日	Cisco Secure Workload 3.8.1.1 が導入されました。

新しいソフトウェア機能

機能名	説明
使いやすさ	
初めてのユーザーの導入準備エクスペリエンスの向上	導入準備エクスペリエンスが次のように向上しました。 • アプリケーションとワークロードの通信全体に関するグローバルビューをユーザーに提供します。 • ポリシー ビジュアル ビュー マップにワークロードの脆弱性を表示します。 • AWS および Azure のロードバランサ設定を表示します。 • インストーラスクリプトまたはインストーラ イメージ メソッドを使用してソフトウェアエージェントをインストールする方法について、シンプルなエージェントウィザードで詳細な手順を示します。
移行の自動化	テナントからテナントへの構成の移行が完全に自動化され、仮想アプライアンスとコネクタがセットアップされるようになりました。
セキュアコネクタ	[セキュアコネクタ（Secure Connector）]ページが拡張され、トンネルインターフェイスの回線プロトコルがダウンしたとき、またはイベントログとともに起動したときにメトリックが表示されるようになりました。これにより、ユーザーはトンネルの安定性をより詳細に確認できます。
エージェントの移行の自動化	リホーム機能を使用して、ソフトウェアエージェントをオンプレミスから SaaS に、または SaaS からオンプレミスに移動できるようになりました。
ポリシーの使用状況のレポートとコンプライアンス	ポリシーヒットカウントをインジケータとして使用して、次のことができるようになりました。 • 時間範囲内の未使用のポリシーを検索します。 • 最初と最後のカウントを含む、時間範囲内の特定のポリシーのヒットカウントを返します。
ラベル管理：ラベルと IP のマッピング	ラベルの使用状況ごとに、ラベルとキー、ラベルとフィルタ、およびフィルタとワークスペースに加えて、ラベルと IP のマッピングを追加できるようになりました。
フロー送信元タイプ別のトラフィックフィルタリングとポリシー分析	センサータイプを使用して、フローの送信元およびフロー検索でフィルタリングできるようになりました。
ADM エクスポート	新しい ADM 機能により、ポリシーのグラフィカルビューの高解像度画像をダウンロードできるようになりました。

機能名	説明
Day 2 オペレーション	
スマート ライセンス	シスコ製品全体のソフトウェアライセンスを管理する統合ライセンス管理システムである Cisco Smart Licensing は、Cisco Secure Workload クラスタの登録、ライセンスの使用状況のレポート、および Cisco Secure Workload オンプレミスクラスタのコンプライアンスの追跡に使用できるようになりました。
アラートの拡張機能	外部オーケストレータの構成中に、アラートの重大度とアラートのしきい値を構成できるようになりました。 また、外部オーケストレータが機能を停止したときに生成されたアラート、またはコネクタからの接続障害が原因で生成されたアラートを Cisco Secure Workload でそれぞれ表示することもできます。 外部オーケストレータでアラートを有効にして表示する方法の詳細については、『Cisco Secure Workload ユーザーガイド』の「外部オーケストレータ」セクションを参照してください。
テストアラートの生成	レビューまたはテストの目的で、[テストアラートの生成（Generate Test Alerts）] ボタンを使用して、パブリッシャとの接続を確認します。 アラートの構成中、サンプルアラートを構成して、アラートタイプとリンクされたパブリッシャに基づいてアラートを送信することもできます。 テストアラートを生成する方法の詳細については、『Cisco Secure Workload ユーザーガイド』の「Generate a Test Alert on the Alert」セクションを参照してください。
レポート機能	エグゼクティブ、ネットワーク管理者、およびセキュリティアナリスト向けに設計されたレポートダッシュボードが導入されました。このダッシュボードには、重要なワークフローステータス、トラブルシューティング機能、およびレポート作成機能が視覚的に表示されます。
MITRE ATT&CK フレームワーク UI の強化	レポートダッシュボードには、MITRE ATT&CK レイアウトに一致するセキュリティサマリーの新しいカードレイアウトが含まれています。その表示には、戦術とその数が含まれます。
ホストエージェントでの拡張テレメトリバッファリング	ソフトウェアエージェントがホストで拡張ネットワーク テレメトリ バッファリングを提供するようになりました。この機能は、[フローディスククォータ（Flow Disk Quota）] を使用するか、エージェント設定プロファイルの [フロー時間枠（Flow Time Window）] を介して構成できます。

機能名	説明
エージェント（Windows）を無効にしてアンインストールするパスワードの保護	Windows のソフトウェアエージェントを、サービスの停止/無効化およびアンインストールから保護できるようになりました。この機能は、エージェント設定プロファイルのサービス保護設定を使用してオンにすることができます。
Cisco Secure Workload クラスタに報告されるエージェントのアンインストール	エージェントをアンインストールすると、その情報がクラスタに送信され、その情報で [ソフトウェアエージェント（Software Agent）] ページが更新されます。 [ソフトウェアエージェント（Software Agent）] ページの UI からエージェントを手動で削除することもできます。また、ユーザーは、エージェント設定プロファイルからクリーンアップ期間をオンにして、エージェントの自動クリーンアップまたは削除を有効にすることもできます。 詳細については、『Cisco Secure Workload ユーザーガイド』の「Removing Software Agents」にある Linux、Windows、AIX エージェントの「Remove a Deep Visibility or Enforcement」セクションを参照してください。
統合	
Cisco Secure Firewall Management Center 統合の拡張機能	ネットワーク管理者は、ワークロードに関連付けられた特定のルールセットを対応する FMC/FTD ドメインにプッシュできるようになりました。
Cisco Secure Firewall Management Center を使用したワークロードの仮想パッチ適用	ネットワーク管理者は、CVE 情報を Cisco Secure Workload から Cisco Secure Firewall Management Center にプッシュして、ファイアウォールの脅威からの保護機能を強化できるようになりました。これにより、ワークロードを既知の脆弱性から保護し、ファイアウォールで IPS シグニチャを使用した補完コントロールとして仮想パッチ適用を提供できます。
ISE コネクタでの AD/LDAP 設定に対するユーザー権限	ISE および AnyConnect NVM コネクタの導入準備のために、標準のドメインユーザーアカウントを使用してコネクタに LDAP を設定できるようになりました。 詳細については、『Cisco Secure Workload ユーザーガイド』の 「LDAP Configuration」セクションを参照してください。
ISE と ISE-PIC の統合	Cisco Secure Workload の ISE コネクタは、pxGRID を使用して ISE-PIC に接続し、ISE を通じて報告されたエンドポイントから ISE グループ名と ISE グループタイプを含むメタデータを取得するようになりました。

機能名	説明
ISE 統合：ISE PxGrid から取り込まれたエンドポイントとその属性を選択/フィルタ処理する機能	ISE を通じて報告されたエンドポイントのコンテキスト情報をすべて取り込みたくない場合は、ISE コネクタの設定中に ISE 属性を無視できるようになりました。 ISE コネクタを設定するときに、複数の IPv4 または IPv6 サブネットを入力して ISE エンドポイントをフィルタ処理できるようになりました。
NF 送信元のリストを報告する NF コネクタ	NetFlow コネクタに NetFlow を送信する NetFlow 送信元のリストを収集してクラスタに報告できます。
フォレンジック、脆弱性、アラートに関する AIX/UNIX の機能拡張	より詳細なフォレンジックモニタリングおよびポリシー適用のため、ネットワークの可視性、オペレーティングシステムのプロセスレベルの可視性を管理する Tetration エンジンが 1 つだけになりました。AIX、Linux、および Solaris 上のソフトウェアエージェントは、csw-agent サービスでのみ表されます。
製品の進化	
Windows のネイティブ OS API を介してパケットをキャプチャする	Windows エージェントは、ndiscap.sys（Microsoft 組み込み）ドライバと Windows を使用した eventstTracing（ETW）フレームワークを使用してネットワークフローをキャプチャするようになりました。既存の Cisco Secure Workload にバンドルされている Npcap バージョンは、ホストで使用できなくなりました。
フォレンジック、脆弱性、アラートに関する AIX/UNIX の機能拡張	より詳細なフォレンジックモニタリングおよびポリシー適用のため、ネットワークの可視性、オペレーティングシステムのプロセスレベルの可視性を管理する Tetration エンジンが 1 つだけになりました。AIX、Linux、および Solaris 上のソフトウェアエージェントは、csw-agent サービスでのみ表されます。
Solaris 11.4 x86_64 でネットワークの可視性をサポート	Solaris 11.4 にネットワークの可視性のサポートが追加されました。
コンテナ	
Kubernetes コントロール プレーン トラフィック用の事前作成済みポリシーテンプレート	k8s クラスタでのポリシーの検出と実装を容易にするために、Kubernetes 環境（eks、aks、gke、openshift）用のポリシーテンプレートが提供されます。 そのため、k8s コントロール プレーン コンポーネントに関わらず、ポリシーをカスタマイズおよび追加して、アプリケーション側のニーズに対応できます。

機能名	説明
パブリッククラウドのK8sサービスオブジェクトタイプのロードバランサに対応	AKSおよびEKSクラスタのKubernetesサービスオブジェクトタイプのロードバランサをサポートします。
Kubernetesまたはコンテナ化されたワークロードに対するADMの有効性	外部オーケストレータページから [ポリシー検出のクラスタリングに使用（Use for policy discovery clustering）] が削除されました。 ポリシー検出のKubernetesサポートの新しいトピックが追加され、ポリシー検出でKubernetes設定のポッドとサービスに関する情報を使用して、ポッドとサービス両方のクラスタを作成します。
Kubernetes - Windowsワーカーノードのサポート	ソフトウェアエージェントは、AKS上のKubernetes Windowsワーカーノードと、Windowsワーカーノードを使用する標準のKubernetesクラスタで、ホストとポッドのネットワークテレメトリをキャプチャしてレポートするようになりました。 （注） GKEまたはEKSには適用されません。
クラウド ネイティブ ワークロード	
クラウドとオンプレミスのエージェントレス ワークロードをUIで区別する	フローから学習した通常のIPと、EC2などのエージェントレス クラウドインスタンスをUIで区別します。
スケーリング	
SaaSおよび39 RUアプライアンスの拡張性の強化（75k）	• SaaSのシングルテナントは、最大75Kのワークロードをサポートできます（会話モード）。 • 39 RUのシングルテナントまたはマルチテナントは、最大75Kのワークロードをサポートできます（会話モード）。 • 8 RUのシングルテナントまたはマルチテナントは、最大20Kのワークロードをサポートできます（会話モード）。
ハイブリッド マルチクラウド ワークロード	
GCPコネクタの拡張機能	GCPコネクタは、タグの取り込み、VPCフローログの取り込み、GCP組み込みファイアウォールを使用したセグメンテーションなどの新機能をサポートするようになりました。
AWSコネクタのセキュリティ強化	AWSコネクタにAWS IAMロールベース認証のサポートが追加されました。

機能名	説明
AWS コネクタのトラブルシューティングの拡張機能	各 AWS コネクタのイベントを表示する新しい [イベントログ（Event Log）] タブが追加されました。このログは、さまざまな機能から AWS コネクタごとに発生する重要なイベントを理解するために役立ちます。

ワークフロー改善のためのバックエンドと UI のアップグレード	AWS コネクタページが強化され、ワークフローが改善されました。次の拡張機能が含まれます。
	• 改善された UI では、各クラウドコネクタに対して作成されたすべての設定の概要が表示されます。
	• テンプレートの生成と開始が別のビューに追加されました。
	• Assume Role の登録/更新/削除とその状態およびトリガーアクションが追加されました。
	• 登録の状態が設定ごとに一目でわかるように追加されました。
	• UI での使用スペースを減らすための機能強化：
	  • Assume Role ワークフローが [設定（Settings）] に追加されました。
	  • リソース選択は、各レベルでリソースを取得するツリー状の構造で行うことができます。
	• 別個の [インベントリ（Inventory）] タブが追加され、選択したリソースおよびスコープコンテキストのインベントリテーブルが表示されます。これにより、ユーザーはそれらの違いを比較できます。
	• [設定（Settings）] を除き、リソース/範囲の選択に役立つフィルタがすべてのビューに追加されました。

Azure コネクタのトラブルシューティングの拡張機能	各 Azure コネクタのイベントを表示する新しい [イベントログ（Event Log）] タブが追加されました。このログは、さまざまな機能から Azure コネクタごとに発生する重要なイベントを理解するために役立ちます。
データのバックアップと復元	
S3 バケット設定チェックの詳細なステータスとエラーメッセージ	データのバックアップを設定するときに、S3 バケット設定の詳細なステータスチェックを表示できるようになりました。

機能名	説明
バックアップの失敗をデバッグするためのエラーレポートの強化	エラーレポートが強化され、チェックポイントの表形式のビューがバックアップ ステータス ページに追加のフィルタオプションとともに表示されます。

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。

（注） M4 のサポートはリリース 3.8.1.1 に限定されており、リリース 3.8.1.1 より後のリリースでは M4 はサポートされません。

拡張機能

- クラスタの内部ワークロードは、デフォルトの範囲のインベントリとエージェントリストに表示されなくなりました。
- Windows 10 および Windows 2012 以降で実行されているソフトウェアエージェントには、Npcap は必要ありません。Windows エージェントは、ndiscap.sys（Microsoft 組み込み）ドライバと Windows を使用したイベントトレース（ETW）フレームワークを使用してネットワークフローをキャプチャするようになりました。Cisco Secure Workload にバンドルされている既存の Npcap バージョンはホストからアンインストールされます。
- ソフトウェアエージェントでネットワーク、プロセス、およびパッケージの可視性のために、x86_64 アーキテクチャの Oracle Solaris 11.4 がサポートされるようになりました。
- Power8 以降の AIX-7.2 で、リモートエージェントログの収集とプロセスおよびパッケージの可視性がサポートされるようになりました。
- ソフトウェアエージェントで Debian 8、9、10、および 11 がサポートされるようになりました。
- ソフトウェアエージェントで x86_64 アーキテクチャの Oracle Linux、AlmaLinux、および Rocky Linux 9.x がサポートされるようになりました。
- ソフトウェアエージェントのサポートは、ppc64le アーキテクチャでサポートされているすべての el9 ベースの Linux ディストリビューションに拡張されます。
- ソフトウェアエージェントのサポートがすべての Windows Server エディションに拡張されました。たとえば、Windows Server 2022 Datacenter: Azure Edition などです。
- ソフトウェアエージェントを使用した適用では、Linux ワークロードで ipset user-space ユーティリティは必要なくなりました。

- --golden-image エージェント インストール スクリプト フラグのサポートが AIX、Linux、および Solaris に拡張されました。
- NetFlow、Cisco Secure Firewall（ASA）、Meraki、NetScaler、F5 コネクタのステータスページに、NetFlow/IPFIX ソースの IP アドレスのリストが表示されるようになりました。
- NetFlow、Cisco Secure Firewall（ASA）、Meraki、NetScaler、F5 コネクタは、NetFlow/IPFIX テンプレートのリストを共有するようになりました。これは、NetFlow/IPFIX メッセージが異なるコネクタ間で負荷分散される場合に役立ちます。
- NetFlow および ASA コネクタの報告されたフローでのクライアント検出が改善されました。
- ソフトウェアエージェントで、VLAN タグ付きフレームによって伝送されるフローを処理するようになりました。
- SuseLinuxEnterpriseServer ワークロードでのエージェントによるフォレンジックイベントのキャプチャが改善されました。
- アクセス コントロール ポリシー（ACP）から Cisco Secure Workload アプリケーションスコープへのマッピングが Firewall Management Center コネクタでサポートされます。
- 会話モードが有効な場合、39 RU で 75K ワークロードがサポートされます。他のすべてのスケール制限に変更はありません。
- 会話モードが有効な場合、8-RU で 20K ワークロードがサポートされます。他のすべてのスケール制限に変更はありません。

動作における変更

- ソフトウェアエージェントのインストーラスクリプトは、Cisco Secure Workload クラスタのバージョンと同期している必要があります。たとえば、3.7.1.22 インストーラスクリプトからのすべての要求は、3.8.1.1 バージョンを実行しているクラスタによって拒否されます。
- ソフトウェアエージェントのアンインストールで、すべてのファイルが完全に削除されるようになりました。
- AIX、Linux、および Solaris 上のソフトウェアエージェントは、csw-agent という名前の 1 つのサービスのみで表されます。tet-sensor、tet-enforcer、および tet-main の個別のサービスはなくなります。
- クラスタへのソフトウェアエージェントのランタイム通信が、CiscoSSL 1.1.1s.7.2.463 バージョンを使用するようにアップグレードされました。
- ソフトウェアエージェントからコレクタへの接続数が 2 分の 1 に削減されました。
- FMC 外部オーケストレータが Cisco Secure Firewall コネクタに移行されました。
- FMC では、ドメインからアプリケーションへのスコープマッピングはサポートされなくなりました。

- フロー学習されたインベントリは、[範囲とインベントリ（Scopes and Inventory）] ページに表示されなくなります。これは、ポリシー検出、ポリシー分析、および適用には影響しません。範囲とインベントリフィルタもフロー学習されたインベントリを表示しないため、フィルタ/範囲が空であるように見える場合があります。ただし、内部では、ポリシーの検出/分析/適用は、サブネット一致を使用することで正常に機能します。

廃止された機能

機能	機能説明	
フローテーブル列は廃止されました	フローテーブルの次の列は使用できなくなりました。	
	• [TCPのパフォーマンス（TCP Performance）] • [順方向TCPボトルネック（Fwd TCP Bottleneck）] • [逆方向TCPボトルネック（Rev TCP Bottleneck）] • [順方向輻輳ウィンドウの削減（Fwd Congestion Window Reduced）] • [逆方向輻輳ウィンドウの削減（Rev Congestion Window Reduced）] • [変更された順方向MSS（Fwd MSS Changed）] • [変更された順方向MSS（Fwd MSS Changed）] • [変更された逆方向MSS（Rev MSS Changed）]	• [順方向TCP受信Window Zero（Fwd TCP Rcv Window Zero?）] • [逆方向TCP受信Window Zero（Rev TCP Rcv Window Zero?）] • [順方向ファブリックパス（Fwd Fabric Path）] • [逆方向ファブリックパス（Rev Fabric Path）] • [順方向バーストインジケータ（Fwd Burst Indicator）] • [逆方向バーストインジケータ（Rev Burst Indicator）] • [順方向最大バーストサイズ（KB）（Fwd Max Burst Size (KB)）] • [逆方向最大バーストサイズ（KB）（Rev Max Burst Size (KB)）] • フローフィルタ
アラート機能は廃止されました	近接アラートとファブリックアラート、および外部 Kafka（データタップ）パブリッシャは、このリリースから廃止されました。	

互換性に関する情報

Cisco Secure Workload エージェントのオペレーティングシステム、外部システム、およびコネクタのサポートについては、「互換性マトリックス」を参照してください。

検証済みスケーラビリティの制限値

次の表に、Cisco Secure Workload（39-RU）、Cisco Secure Workload M（8-RU）、および Cisco Secure Workload Cloud の拡張性の制限を示します。

表 *1 : Cisco Secure Workload*（*39-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 25000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 75,000（3x）。
1 秒あたりのフロー機能	最大 200 万。

表 *2 : Cisco Secure Workload M*（*8-RU*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 5,000（VM またはベアメタル） すべてのセンサーが会話モードの場合、最大 20,000（4x）。
1 秒あたりのフロー機能	最大 500,000。

表 *3 : Cisco Secure Workload Virtual*（*VMWare ESXi*）の拡張性の制限

設定可能なオプション	規模
ワークロードの数	最大 1,000（VM またはベアメタル）
1 秒あたりのフロー機能	最大 70,000。

（注） サポートされているスケールは、最初に制限に達したパラメータに基づいています。

解決済みおよび未解決の問題

このリリースで解決済みの問題と未解決の問題には、Cisco Bug Search Tool を使用してアクセスできます。この Web ベースのツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品での問題と脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。

（注） Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、アカウントを登録できます。

Cisco Bug Search Tool の詳細については、Bug Search Tool（BST）ヘルプおよび FAQ を参照してください。

解決済みの問題

ID のリンクをクリックして、シスコのバグ検索ツールにアクセスし、その問題に関する詳細情報を表示します。

ID	見出し
CSCwe83822	3.7.1.22 からの Windows エージェントのアップグレードが MSI 署名チェックに失敗する場合がある。
CSCwf78123	[Linux] iptables-legacy が存在する場合、新しいプラットフォームでポリシーの逸脱/修正が継続的に発生する。
CSCwe27066	Anyconnect コネクタ - コントローラのクラッシュ：フローデータをエクスポートできない。
CSCwf29111	ポリシー分析で、Windows ワークロードによって拒否されたフローが誤って表示される場合がある。
CSCwf29138	Windows ワークロードで TetSen.exe プロセスに障害が発生する。
CSCwe83822	3.7.1.22 からの Windows エージェントのアップグレードが MSI 署名チェックに失敗する場合がある。
CSCwf18991	AIX：Catch-all が DENY の場合、DHCP が機能しない。
CSCwf03825	AIX エージェントのインストーラが ipfilter v5.3.0.7 よりも新しい ipfilter バージョンを認識しない

未解決の問題

ID のリンクをクリックして、シスコのバグ検索ツールにアクセスし、その問題に関する詳細情報を表示します。

ID	見出し
CSCwd67224	AIX 7.x で適用が有効になると、フラグメンテーションが原因でエージェントが CSW クラスタに接続できない。
CSCwb39541	タイムアウトしている Investigate Traffic クエリのエラーメッセージを変更します。

ID	見出し
CSCwb91717	保留状態のソフトウェアエージェントのSWステータスのアップグレードチャートのデータがない。
CSCwb80213	vNICがベアメタルサーバーでハングアップする（BMのeNICバージョンをアップグレードする必要がある）。
CSCwc63711	Azureセグメンテーションのアクセス許可がありません。
CSCwd93604	3.7でDruidセグメントのロードキューが過負荷状態なる場合がある。
CSCwb42177	ライブポリシーと適用ポリシーの分析：テーブルにカーソルを合わせると、範囲列とテキストが切り取られる。
CSCwf37266	AIX適用ルールが、先頭にゼロが含まれるサブネットでは正しく一致しない。

関連資料

Cisco Secure Workloadのマニュアルは次のWebサイトからアクセスできます。

- Cisco Secure Workload Platform Datasheet
- Cisco Secure Workloadのドキュメント

表 *4:* インストールマニュアル

ドキュメント	説明
Cisco Secure Workload Cluster Deployment Guide	Cisco Secure Workload（39-RU） プラットフォームとCisco Secure Workload M（8-RU）のシングルおよびデュアルラックインストールの物理的な構成、設置場所の準備、およびケーブル配線について説明します。 Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide
Cisco Secure Workload Virtual Deployment Guide	Cisco Secure Workload仮想アプライアンス（旧称 Tetration-V）の展開について説明します。 Cisco Secure Workload Virtual (Tetration-V) Deployment Guide

ドキュメント	説明
Cisco Secure Workload Upgrade Guide	Cisco Secure Workload Upgrade Guidehttps://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/upgrade/appliance/cisco-secure-workload-upgrade-guide.html （注） ベストプラクティスとして、メジャー バージョン アップグレードを実行する前に、クラスタにパッチを適用して使用可能な最新のパッチバージョンにすることを常に推奨します。
最新の脅威データ ソース	Cisco Secure Workload

シスコへのお問い合わせ

上記のオンライン リソースでは問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。