Cisco Secure Workload リリースノート、リリース 3.6.x

初版：2022 年 2 月 14 日

最終更新：2023 年 2 月 2 日

このマニュアルでは、Cisco Secure Workload ソフトウェアリリース 3.6.x の新機能、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。

次の表に、リリースの変更履歴を示します。

表 *1:* リリースノートの変更履歴

日付	説明
2023 年 2 月 2 日	リリース 3.6.1.52 が導入されました。
2022 年 5 月 26 日	リリース 3.6.1.36 が導入されました。

日付	説明
2022 年 3 月 10 日	リリース 3.6.1.21 が導入されました。
2022 年 2 月 14 日	リリース 3.6.1.17 が導入されました。
2021 年 10 月 29 日	リリース 3.6.1.5 が導入されました。

互換性に関する情報

リリース 3.6.1.36

OS	フレーバ
新しいエージェントのオペレーティングシステムのサポート	• AIX 7.3 • AlmaLinux 8.x • Rocky Linux 8.x Ingest アプライアンス • AnyConnect アプライアンスで IPFIX V5 テンプレートをサポート • Windows 2008 R2 以降のエージェントで NPCAP バージョン 1.55 を使用
[エージェント（Agents）]	Windows 2008 R2 以降のエージェントで NPCAP バージョン 1.55 を使用

リリース 3.6.1.21

OS	フレーバ
このリリースにソフトウェアへの変更はありません。	–

リリース 3.6.1.17

OS	フレーバ
Cisco Secure Workload エージェントインストーラ	Cisco Secure Workload エージェントインストーラで、メジャーリリースがサポートされている Linux ディストリビューションのマイナーリリースへのインストールが可能になりました。Linux のマイナーリリースのサポートが対応するメジャーリリースのサポートを通じて拡張されています。 サポートされているオペレーティングシステムのバージョンは、Cisco.com のプラットフォーム情報に記載されています。

3.6.1.5 リリースのソフトウェアエージェントは、マイクロセグメンテーション（優れた可視性と適用）を実現するために、次のオペレーティングシステム（仮想マシンおよびベアメタルサーバー）をサポートしています。バージョンごとのリストには、プラットフォーム情報のページからいつでもアクセスできます。

リリース 3.6.1.5

OS	フレーバ
Linux	• Amazon Linux 2 • CentOS-6.x: 6.1 ～ 6.10 • CentOS-7.x：7.0 ～ 7.9 • CentOS-8.x：8.0 ～ 8.4 • Red Hat Enterprise Linux-6.x：6.1 ～ 6.10 • Red Hat Enterprise Linux-7.x：7.0 ～ 7.9 • Red Hat Enterprise Linux-8.x：8.0 ～ 8.4 • Oracle Linux Server-6.x：6.1 ～ 6.10 • Oracle Linux Server-7x：7.0 ～ 7.9 • Oracle Linux Server-8.x：8.0 ～ 8.4 • SUSE Linux-11.x：11.2 ～ 11.4 • SUSE Linux-12.x：12.0 ～ 12.5 • SUSE Linux-15.x：15.0 ～ 15.2 • Ubuntu-14.04 • Ubuntu-16.04 • Ubuntu-18.04 • Ubuntu-20.04

OS	フレーバ
Linux on IBM Z	• Red Hat Enterprise Linux-7.x：7.3 ～ 7.9 • Red Hat Enterprise Linux-8.x：8.2 ～ 8.4 • SUSE Linux-11.x：11.4 • SUSE Linux-12.x：12.4、12.5 • SUSE Linux-15.x：15.0 ～ 15.2
Windows Server（64 ビット）	• Windows Server 2008R2 Datacenter • Windows Server 2008R2 Enterprise • Windows Server 2008R2 Essentials • Windows Server 2008R2 Standard • Windows Server 2012 Datacenter • Windows Server 2012 Enterprise • Windows Server 2012 Essentials • Windows Server 2012 Standard • Windows Server 2012R2 Datacenter • Windows Server 2012R2 Enterprise • Windows Server 2012R2 Essentials • Windows Server 2012R2 Standard • Windows Server 2016 Standard • Windows Server 2016 Essentials • Windows Server 2016 Datacenter • Windows Server 2019 Standard • Windows Server 2019 Essentials • Windows Server 2019 Datacenter

OS	フレーバ
Windows VDI デスクトップクライアント	• Microsoft Windows 8.1 • Microsoft Windows 8.1 Pro • Microsoft Windows 8.1 Enterprise • Microsoft Windows 10 • Cisco Tetration リリースノート • Microsoft Windows 10 Pro • Microsoft Windows 10 Enterprise • Microsoft Windows 10 Enterprise 2016 LTSB
IBM AIX オペレーティングシステム	• AIX バージョン 7.1 • AIX バージョン 7.2
ポリシーを適用するためのコンテナホスト OS バージョン	• Red Hat Enterprise Linux リリース 7.1 ～ 7.9 • CentOS リリース 7.1 ～ 7.9 • Ubuntu-16.04 • Red Hat Enterprise Linux Core OS リリース 4.5

OS	フレーバ
オペレーティングシステムのサポート	3.6.1.5 リリースでは、優れた可視性ユースケースについてのみ、次のオペレーティングシステムがサポートされています。 • Windows VDI デスクトップクライアント: • Microsoft Windows 7 • Microsoft Windows 7 Pro • Microsoft Windows 7 Enterprise 3.6.1.5 リリースでは、ユニバーサル可視性エージェントの次のオペレーティング システムがサポートされています。 • Windows Server（優れた可視性エージェントが使用できない 32 ビットおよび 64 ビット） • AIX 6.1（PPC） 3.6.1.5 リリースでは、次のオペレーティングシステムについては、いずれのソフトウェアエージェントでもサポートが終了しています。 • Red Hat Enterprise Linux リリース 5.x • CentOS リリース 5.x • AIX 5.3（PPC） • Microsoft Windows 8

3.6.1.5 リリースでは、NX-OS および Cisco Application Centric Infrastructure（ACI）モードでの次の Cisco Nexus 9000 シリーズスイッチのサポートが廃止されています。HW センサーを使用している場合は、代替ソースとして NetFlow への移行を計画してください。

NX-OS および ACI モードで以前にサポートされていた Cisco Nexus 9000 シリーズスイッチ（3.6.1.5 で廃止、動作の変更のセクションを参照）。

製品ライン	プラットフォーム	最小ソフトウェア リリース
Cisco Nexus 9300 プラットフォーム スイッチ (NX-OS モード)	Cisco Nexus 93180YC-EX、93108TC-EX、および 93180LC-EX	Cisco NX-OS リリース 9.2.1 以降
	Cisco Nexus 93180YC-FX、93108TC-FX、および 9348GC-FXP	Cisco NX-OS リリース 9.2.1 以降
	Cisco Nexus 9336C-FX2	Cisco NX-OS リリース 9.2.1 以降

製品ライン	プラットフォーム	最小ソフトウェア リリース
Cisco Nexus 9300 プラットフォーム スイッチ（Cisco ACI モード)	Cisco Nexus 93180YC-EX、93108TC-EX、および 93180LC-EX	• Cisco ACI リリース 3.1(1i) 以降
	Cisco Nexus 93180YC-FX、93108TC-FX	Cisco ACI リリース 3.1(1i) 以降
	Cisco Nexus 9348GC-FXP	Cisco ACI リリース 3.1(1i) 以降
	Cisco Nexus 9336C-FX2	Cisco ACI リリース 3.2 以降
	N9K X9736C-FX ラインカードのみを搭載した Cisco Nexux 9500シリーズスイッチ	Cisco ACI リリース 3.1(1i) 以降

使用上のガイドライン

ここでは、Cisco Secure Workload ソフトウェアの使用上のガイドラインを示します。

- Web ベースのユーザーインターフェイスにアクセスするには、Google Chrome ブラウザ バージョン90.0.0 以降を使用する必要があります。
- DNS を設定した後、Cisco Secure Workload クラスタの URL（https://<cluster.domain>）まで参照します。

Cisco Secure Workload 仮想アプライアンス環境でコミッション/デコミッション機能を使用する場合は、次の使用上のガイドラインに従ってください。

この機能は TAC の支援を受けて使用することを意図しており、誤って使用すると回復不能な障害を引き起こす可能性があります。TAC からの明示的な承認がない限り、2つの VM を同時にデコミッションしないでください。次の VM の組み合わせは、同時にデコミッションしないでください。

- 複数のオーケストレータ
- 複数のデータノード
- 複数の namenode（namenode または secondaryNamenode）
- 複数の resourceManager
- 複数の happobat
- 複数の mongodb（mongodb または mongoArbiter）
- 一度に実行できるデコミッション/コミッションプロセスは 1 つだけです。異なる VM のデコミッション/コミッションを同時にオーバーラップしないでください。

esx_commission スナップショット エンドポイントを使用する前に、必ず TAC にお問い合わせください。

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 *2 : 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 50,000（2x）。
1 秒あたりのフロー機能	最大 200 万。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

表 *3 : 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 10,000（2x）。
1 秒あたりのフロー機能	最大 500,000。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	最大 100（非推奨）。

表 *4 : 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。
ハードウェア エージェント対応 Cisco Nexus 9000 シリーズ スイッチの数	サポート対象外。

（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。

動作の変更

リリース 3.6.1.36

機能	説明
新しいエージェントのオペレーティングシステムのサポート	• AIX 7.3 • AlmaLinux 8.x • Rocky Linux 8.x Ingest アプライアンス • AnyConnect アプライアンスで IPFIX V5 テンプレートをサポート • Windows 2008 R2 以降のエージェントで NPCAP バージョン 1.55 を使用
[エージェント（Agents）]	Windows 2008 R2 以降のエージェントで NPCAP バージョン 1.55 を使用

表 *5 :* リリース *3.6.1.21*

機能	説明
このパッチリリースにソフトウェアへの変更はありません。	–

表 *6 :* リリース *3.6.1.17*

機能	説明
Cisco Secure Workload エージェントインストーラ	Cisco Secure Workload エージェントインストーラで、メジャーリリースがサポートされている Linux ディストリビューションのマイナーリリースへのインストールが可能になりました。Linux のマイナーリリースのサポートが対応するメジャーリリースのサポートを通じて拡張されています。 サポートされているオペレーティングシステムのバージョンは、Cisco.com のプラットフォーム情報に記載されています。

表 *7:* リリース *3.6.1.5*

機能	説明
[外部オーケストレータ（External Orchestrators）]	AWS または Kubernetes EKS の新しい外部オーケストレータは作成できなくなりました。代わりに、AWS クラウドコネクタを作成します。詳細については、上記を参照してください。 3.6.1.5 へのアップグレード前に作成された AWS または Kubernetes EKS の外部オーケストレータのインスタンスは引き続き機能しますが、変更することはできません。変更が必要な場合は、代わりに、同じクラウドアセットのセットから情報を取り込む新しい AWS クラウドコネクタを作成し、古い AWS または EKS の外部オーケストレータの設定を削除する必要があります。
UI	リリース 3.6.1.5 以降では、ページが上部のナビゲーションバーから左側のメニューに移動されたため、左側のメニューがナビゲーションの主要なポイントになりました。 主な変更点は次のとおりです。 • ADM、適用ステータス、適用テンプレートなど、すべてのセグメンテーション関連の機能がトップレベルの [防御（Defend）] メニューの下に表示されるようになりました。 • フロー、プロセス、および脆弱性に関連するすべての分析データの情報がトップレベルの [調査（Investigate）] メニューの下に表示されるようになりました。 • 外部オーケストレータ、エージェント、およびコネクタに関連するすべての統合がトップレベルの [管理（Manage）] メニューの下に表示されるようになりました。 • すべてのアプライアンス関連の設定とトラブルシューティング機能がトップレベルの [プラットフォーム（Platform）] メニューと [トラブルシューティング（Troubleshooting）] メニューの下にそれぞれ表示されるようになりました。
クラスタ機能	ルックアウト機能は 3.5 で廃止され、その状態のままです。3.6 では、ルックアウト機能をオンにすることはできません。ただし、ルックアウトを現在使用している場合は、既存の設定を引き続き表示できます。 この製品を簡素化するために、UserApps 機能は削除されました。

機能	説明
[エージェント（Agents）]	• WFP 適用モードがベータ版ではなくなりました。Windows Filtering Platform（WFP）を使用すると、Windows Advanced Firewall（WAF）を必要とせずに、適用エージェントでネットワークフィルタを直接適用できます。 • ユニバーサルエージェントが廃止予定としてマークされました。次のメジャーリリースでサポートが終了するかインストールできなくなります。ユニバーサルエージェントを使用している場合は、優れた可視性エージェントへの置き換えを計画してください。 • ハードウェアエージェントが廃止予定としてマークされました。次のメジャーリリースでサポートが終了するかインストールできなくなります。ハードウェアセンサーを使用している場合は、NetFlow または ERSPAN 仮想アプライアンスへの移行を計画してください。
仮想アプライアンス	ERSPAN 仮想アプライアンスは、Cisco Secure Workload Data Ingest OVA を使用して展開する必要があります。ERSPAN OVA は公開されなくなりました。古い ERSPAN OVA で展開された既存の ERSPAN 仮想アプライアンスについては、変更は必要ありません。
サポートポリシー	Cisco Secure Workload ソフトウェアバージョンの EOL サポート終了ポリシーをリリースしました。保守と運用のテクニカルノートを参照してください。

拡張機能

リリース 3.6.1.47

機能	説明
ソフトウェアエージェント	ソフトウェアエージェントは、x86_64 アーキテクチャと s390x アーキテクチャで Red Hat Enterprise Server 9 をサポートするようになりました。

リリース 3.6.1.36

機能	説明
FMC 外部オーケストレータ	FMC ドメインごとの適用のサポート。外部オーケストレータの設定時にドメイン名を選択することで、FMC ドメインで適用を有効または無効にできるようになりました。
Windows のセグメンテーションポリシー	Windows のセグメンテーションポリシーでは、単一のユーザー名に加えて、プロセスレベル制御セクションにユーザーまたはユーザーグループのリストを入力できます。

機能	説明
インストーラスクリプト作成時のインベントリラベル	インストーラスクリプトを作成するときに、インベントリラベルを指定できます。スクリプトでインストールされるすべてのエージェントに、それらのラベルが自動的にタグ付けされます。この機能は、Linux および Windows ワークロードの展開でのみサポートされています。

リリース 3.6.1.21

機能	説明
外部オーケストレータ統合の Kubernetes バージョン	外部オーケストレータ統合で Kubernetes バージョン 1.21 および 1.22 がサポートされるようになりました。

リリース 3.6.1.17

機能	説明
Cisco Secure Workload とフローログ	コネクタの作成中に提供された AWS ユーザーアカウントのログイン情報で VPC フローログと S3 バケットの両方にアクセスできる場合、Cisco Secure Workload で任意のアカウントに関連付けられた S3 バケットからフローログを取り込めるようになりました。

リリース 3.6.1.5

機能	説明
ServiceNow で ServiceNow のスクリプト化された REST API との統合がサポートされます。	設定ワークフローで ServiceNow コネクタを選択できます。ServiceNow のスクリプト化された REST API との統合がサポートされるようになりました。 Cisco Integrated Management Controller（CIMC）のバージョンが更新されました。M4 CIMC は 4.1(2b) に更新され、M5 CIMC は 4.1(3b) に更新されています。Cisco Secure Workload クラスタを 3.6 にアップグレードしても、ベアメタルノードの CIMC ファームウェアは自動的にはアップグレードされません。CIMC ファームウェアのアップグレードはオプションであり、ベアメタルホストごとに最大 4 時間かかる場合があります。このプロセスは、Cisco TAC から勧められた場合にのみ実行してください。 Cisco Secure Workload と Firepower Management Center（ベータ機能）の統合により、ファイアウォールを使用したポリシーの適用が可能になります。このリリースでは、プレフィルタポリシーの代わりにダイナミックオブジェクトを使用するアクセス コントロール ポリシーが統合で使用されるため、ネットワークインベントリの変更を展開する必要はありません。これにより、展開が少なくなり、インベントリの変更への対応が迅速になります。 サポートされているバージョンや要件などの詳細については、『Cisco Secure Workload and Firepower Management Center Integration Guide』（英語）を参照してください。リリース 3.5 で FMC 統合を設定済みの場合は、アップグレード前に『Cisco Secure Workload Upgrade Guide』（英語）の重要な注意事項を参照してください。 会話モードのフロー分析忠実度が AIX エージェントに適用されるようになりました。
Cisco Integrated Management Controller（CIMC）のバージョンの更新	Cisco Integrated Management Controller（CIMC）のバージョンが更新されました。 • M4 CIMC は 4.1(2b) に更新され、M5 CIMC は 4.1(3b) に更新されています。Cisco Secure Workload クラスタを 3.6 にアップグレードしても、ベアメタルノードの CIMC ファームウェアは自動的にはアップグレードされません。 （オプション）CIMC ファームウェアをアップグレードします。ベアメタルホストごとに最大 4 時間かかる場合があります。このプロセスは、Cisco TAC から勧められた場合にのみ実行してください。

機能	説明
FMC と Cisco Secure Workload の統合	Cisco Secure Workload と Firepower Management Center（ベータ機能）の統合により、ファイアウォールを使用したポリシーの適用が可能になります。このリリースでは、プレフィルタポリシーの代わりにダイナミックオブジェクトを使用するアクセス コントロール ポリシーが統合で使用されるため、ネットワークインベントリの変更を展開する必要はありません。これにより、展開が少なくなり、インベントリの変更への対応が迅速になります。 サポートされているバージョンや要件などの詳細については、『Cisco Secure Workload and Firepower Management Center Integration Guide』（英語）を参照してください。 （注） リリース 3.5 で FMC 統合を設定済みの場合は、アップグレード前に『Cisco Secure Workload Upgrade Guide』（英語）の重要な注意事項を参照してください。
[流動解析の忠実度（Flow Analysis Fidelity）]	会話モードのフロー分析忠実度が AIX エージェントにも適用されるようになりました。

新機能および変更された機能に関する情報

リリース 3.6.1.36 の新機能と変更情報

機能	説明
Inventory	インベントリのアップロード：[インベントリアップロード（Inventory Upload）] の [マージオプション（Merge Option）] で新しいオプションを使用できるようになりました。
外部オーケストレータ	Infoblox 外部オーケストレータ：さまざまなタイプの DNS レコード（A レコード、AAAA レコード、ネットワークレコード、ホストレコード）を選択できるようになりました。
Kubernetes インベントリのサポート	ADM クラスタリングと範囲の提案で Kubernetes インベントリがサポートされるようになりました。
VDI 導入	インストールスクリプトと MSI インストーラの新しい --goldenImage フラグにより、Windows ゴールデン仮想マシンへのエージェントのインストールが可能になり、ホスト名が変更されると複製された VM でエージェントが実行されるようになりました（エージェントソフトウェアは、メンテナンスまたはアップグレードのために VM が起動する場合でも、ゴールデン VM で実行されることはありません）。

リリース 3.6.1.21 の新機能と変更情報

機能	説明
コンテナワークロードのマイクロセグメンテーションのサポート	Red Hat OpenShift 4.x を介して導入されたコンテナワークロードのマイクロセグメンテーション サポートが利用可能になりました。 OpenShift 4.x は、Kubernetes のデフォルトのコンテナランタイムとして CRI-O を使用します。CRI-O がサポートされており、このような環境で実行するために既存の適用ワークフローを変更する必要はありません。ワーカーノードのオペレーティングシステムには、OpenShift 4.x で公式にサポートされている RHEL または CentOS のいずれかのバージョンが使用できます。 このリリースでは、外部オーケストレータの統合で Red Hat OpenShift バージョン 4.9 までがサポートされます。 また、Red Hat Enterprise Core OS バージョン 4.9 までのサポートも追加されています。

リリース 3.6.1.17 の新機能と変更情報

このパッチリリースには新しいソフトウェア機能はありません。

リリース 3.6.1.5 の新機能と変更情報

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デーモンセット
- 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
- ADC（アプリケーション デリバリ コントローラ）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
- NSEL（NetFlow セキュアイベントロギング）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

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が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（ISE）
- 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。

機能	説明
AWS コネクタ	AWS 用の新しいクラウドコネクタ（ベータ機能）により、フローテレメトリの取り込み、EC2 インスタンスと EKS ポッド/サービスワークロードの両方のクラウドワークロードタグ/ラベルの取り込み、AWS セキュリティグループを使用したポリシーの適用（EC2 ワークロードのみ）のサポートが追加されます。クラウドホストにソフトウェアエージェントをインストールする必要はありません。 この新しいクラウドコネクタは、外部アプライアンスを必要とせずに、さまざまな手段で以前に提供されていた機能を統合することで接続の管理を合理化します。 • Amazon Web Services（AWS）Elastic Kubernetes Service（EKS）マイクロセグメンテーション機能が外部オーケストレータから AWS コネクタに移行されました。 • Azure AKS 外部オーケストレータのサポートが追加されました。この機能は、外部オーケストレータとして Kubernetes を追加するときに選択できます。 • 管理者が Azure テナント ID とクライアントのログイン情報を提供する必要があります。 （注） ポッドレベルのフローテレメトリデータとポッドレベルのポリシー適用を提供するには、エージェントソフトウェアが引き続き必要です。

機能	説明
コンテナワークロードのマイクロセグメンテーションのサポート	Red Hat OpenShift 4.x を介して導入されたコンテナワークロードのマイクロセグメンテーション サポートが利用可能になりました。 OpenShift 4.x は、Kubernetes のデフォルトのコンテナランタイムとして CRI-O を使用します。CRI-O がサポートされており、このような環境で実行するために既存の適用ワークフローを変更する必要はありません。ワーカーノードのオペレーティングシステムには、OpenShift 4.x で公式にサポートされている RHEL または CentOS のいずれかのバージョンが使用できます。 このリリースは、Red Hat OpenShift バージョン 4.6 までをサポートします。 このリリースでは、ワーカーノードのオペレーティングシステムとして Red Hat CoreOS のサポートが追加されています。
ポリシーテンプレート	一般的な設定で始めるのに役立つポリシーテンプレートが追加されました。
PIV/CAC	PIV/CAC ID 検証との統合がサポートされるようになりました。
ハードウェアクラスタ	Cisco Secure Workload ハードウェアクラスタの展開時やバージョン 3.6.1.5 へのアップグレード時に、外部ネットワーク接続用に IPv6 を設定できるようになりました。 制限事項、要件、および手順については、該当するアップグレードガイドまたはハードウェア導入ガイドを参照してください。
Windows ワークロード	Windows ワークロードに対するサービス/アプリケーション/ユーザーベースのポリシー適用のサポートが追加されました。 Kubernetes ポッドおよびサービスフローに基づくポリシー検出のサポート。 （注） ポリシーの有効化のサポートは、範囲間のポリシーの生成に制限されます。
ソフトウェアエージェントの正常性	[ソフトウェアエージェントの正常性（Software Agents Health）] ページに、メモリと CPU の使用レベルとエージェントの実行状態の異常が表示されるようになりました。 会話モードのフロー分析忠実度で、会話の発信側を特定するたびに 4 タプルの会話の L4 ポートが報告されるようになりました。

互換性の詳細については、Cisco.com の「Platform Information」（英語）を参照してください。

警告

このセクションでは、解決済みおよび未解決のバグと既知の動作のリストを示します。

このリリースで解決済みのバグと未解決のバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース 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バグ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。

既知の動作

Cisco Secure Workload ソフトウェアリリース 3.6.x の既知の動作を参照してください。

リリース	既知の動作
3.6.1.47	3.6.1.5 の既知の動作と同じ
3.6.1.36	3.6.1.5 の既知の動作と同じ
3.6.1.21	3.6.1.5 の既知の動作と同じ
3.6.1.17	3.6.1.5 の既知の動作と同じ

リリース	既知の動作
3.6.1.5	• [エージェント接続用の強力な SSL 暗号（Strong SSL Ciphers for Agent Connections）] が有効になっているクラスタで 3.6.1.5 にアップグレードする場合は、TAC にお問い合わせください。（CSCwa19256 を参照） • エージェント設定プロファイルのフロー分析忠実度構成の会話設定は、ユニバーサル可視性エージェントではサポートされていません。 • 新しいルートスコープの作成直後に新しいコネクタを有効にすると、Cisco Secure Workload の UI に誤った AWS コネクタワークフローが表示される。（CSCvz43857） • [データタップ管理（Data Taps Admin）] ページには Alpha のラベルが表示されますが、Alpha にはポリシー ストリーム データ タップはありません。 • [データタップ管理（Data Taps Admin）] には引き続き表示されますが、データエクスポートタップは 3.6 ではサポートされなくなりました。 • このリリースでは、クロスアカウント（異なるアカウントに属する VPC および S3 バケット）のフローログの収集はサポートされていません。 • [AWS インベントリプロファイル（AWS inventory profile）] ページでは、コネクタでセグメンテーションが有効になっている場合でも、有効になっている適用が無効として表示されます。

リリース 3.6.1.52 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

ID	見出し
CSCwc72280	ユーザーが IP 仮想化を使用してネットワーク情報を取得している場合、Tetration UI でデータがレンダリングされない。
CSCwd00625	ホスト IP に関連付けられたラベルが、そのホストで報告される他のすべての IP に複製される。
CSCwd80353	プロバイダーポート 0 が TCP フローのポートとして検出される。

ID	見出し
CSCwb65874	フォレンジックルールの正規表現が正しくないため、データノードでディスク容量が枯渇する。

未解決の警告

次の表は、このリリースで開いている注意事項のリストです。バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

表 *8*: 未解決の不具合

ID	見出し
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる。
CSCvz99865	AWS フローログ：AWS フローログを使用したポリシー分析が機能しない。

リリース 3.6.1.47 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

ID	見出し
CSCwc02772	Cisco Secure Workload 内部クラスタオーケストレータのローカル DNS がごくまれに失敗することがある。
CSCwc14819	Kafka Producer のエラーでメッセージが長すぎたため、DNS 外部オーケストレータでメタデータを取得できない。
CSCwb76311	Windows エージェントインストーラの PowerShell スクリプトに、カスタムパスにエージェントをインストールするオプションがない。
CSCwc79283	RHEL ホストのエージェントがエージェントの再起動の異常で繰り返し表示される。
CSCwc77006	オーケストレータの rsync バージョンが 3.1.2 未満の場合、CSW 3.7 のアップグレードが失敗することがある。

ID	見出し
CSCwc17237	ネットワークの可視性を無効にすると、プロセス/パッケージの可視性も無効になる。
CSCwb21235	namenode スイッチオーバースクリプトが namenode が起動するまで待機しないことがある
CSCwc68679	フォレンジック機能を無効にしても、監査ログへのイベントの記録が停止しない。
CSCwc23159	RHEL 8.x 適用エージェントが [アップグレード（Upgrade）] タブに表示されない。
CSCwc29903	エージェント インストーラ スクリプトによるユーザーラベルの更新に不具合がある。
CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある。
CSCwc59065	特定の IPv6 の範囲でポリシーを処理すると、適用エージェントが再起動することがある。
CSCwb94594	ワークロードに対して大規模なCSWエージェントの展開を実行できない。
CSCwc31985	ACI から受信した NetFlow データセットの復号化で EOF エラーが発生する。
CSCwc32016	Netflow センサーが受信した netflow データをドロップした。
CSCwc31977	NetFlow コネクタからの NetFlow パケットの復号化で一定のエラーが発生する。
CSCwb72418	ポリシーテンプレートをインポートしても、[最新のポリシーの分析（Analyze Latest Policies）] ボタンが変更されない。
CSCvy31758	[North Star] 機能する SSH キーをアップグレード前にインポートする要件を追加。
CSCvy04774	機能強化：すべてのラベルタイプの一致条件のサポート

未解決のバグ

ID	見出し
CSCvz95962	会話モード：会話モードの短時間の非TCPフローでクライアントサーバーが切り替わることがある
CSCvz99865	AWS フローログの子範囲のポリシー分析が機能しない

ID	見出し
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。

リリース 3.6.1.36 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

ID	見出し
CSCwb25813	Cisco Secure Workload 適用エージェントで IPv6 サブネットが誤って集約されることがある
CSCwb39558	パッチアップグレード後に AgentContainer および HelmChart のサービスが失敗する。
CSCwb21235	namenode スイッチオーバースクリプトが namenode が起動するまで待機しないことがある
CSCwb86649	40Gbps リンクのサーバーで実行されている ERSPAN センサーで 100Kpps しか受信しない
CSCwb83818	適用モードが WFP の場合に適用エージェントが Windows ファイアウォールサービスに依存する
CSCvz57161	EHN：Tet エージェントのインストール時にエージェントタイプの詳細情報の提供が必要
CSCwb27430	SNOW 統合に最低限必要なロールを文書化
CSCvz32417	ENH：NPCAP バージョンの最新の 1.5 へのアップグレード
CSCwb25637	ゾーン転送で DNS 外部オーケストレータが失敗する
CSCwa64962	フェデレーション/DBR：ソースクラスタからのセンサー移行のステータスを特定できない
CSCwb71970	サイトの DNS リゾルバの設定の変更に失敗することがある
CSCwb11295	3.6 でポートなしで HTTP プロキシを有効にすると、AppServer の iptables テンプレートが破損する

ID	見出し
CSCwa17868	LDAP と統合されている場合、ISE コネクタで複数の memberOf 属性を処理できない
CSCwb92959	AppServer 仮想マシンの noisy.log のログローテーションが機能しない
CSCwb01213	Cisco Tetration に Rocky Linux 8 との互換性がない
CSCvz95962	会話モード：会話モードの短時間の非 TCP フローでクライアントサーバーが切り替わることがある

未解決のバグ

CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある
CSCvz99865	AWS フローログの子範囲のポリシー分析が機能しない
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCwb97537	ライセンス数が正確でない
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる

リリース 3.6.1.21 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

不具合 ID	説明
CSCwa91086	センサーの導入に関するドキュメントで NIC チーミングバージョンの互換性マトリクスを反映。

未解決のバグ

ID	見出し
CSCwb86649	40Gbps リンクのサーバーで実行されている ERSPAN センサーで 100Kpps しか受信しない。

ID	見出し
CSCwb83818	適用モードが WFP の場合に適用エージェントが Windows ファイアウォールサービスに依存する。
CSCwa64962	フェデレーション/DBR：ソースクラスタからのセンサー移行のステータスを特定できない。
CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある。
CSCvz99865	AWS フローログの子範囲のポリシー分析が機能しない。
CSCvz95962	会話モード：会話モードの短時間の非TCPフローでクライアントサーバーが反転することがある。
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる。

リリース 3.6.1.17 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

ID	見出し
CSCvz80415	Cisco Tetration の脆弱性サイトの出力の問題
CSCwa90905	すべてのプロトコルでマークされたサービスが F5 外部オーケストレータで適切に処理されない
CSCvu75902	VMware VDI インスタントクローンの使用時にエージェントが登録に失敗する（Windows 10 で適用を有効にしている場合）
CSCvz64463	フェデレーションのクラスタのプライマリサイトとセカンダリサイトで Cisco Tetration の SSH キーが同期されない
CSCwa00954	ADM の会話モードでプロバイダーポートが 0 に設定されたポリシーが生成される
CSCvy09204	[強力な暗号の有効化（Strong Ciphers Enabled）] オプションセットの True と False の違いの説明

ID	見出し
CSCvx63434	ENH：Windows Storage Server 2012R2/Storage Server 2016 の Cisco Tetration エージェントのサポート
CSCwa91167	提供されたサービスリクエストを使用してワークスペースの 3.6.1.5 にアップグレードした後に ADM ジョブが失敗する
CSCwa48895	2 つの ACI ファブリックが Cisco Tetration クラスタに接続されたシナリオで FabricPath が正しく表示されない
CSCwa55880	ロケール名に UTF-8 文字以外を含むセンサーのワークロード プロファイル ページを開く際にエラーが発生する
CSCvz38485	ENH：深部に及ぶ可視性センサーが新しい UBR を持つ Cisco Tetration の Windows レジストリの更新を定期的にポーリング
CSCwa15075	RHEL 8.2 VM でのエージェントのアップグレードが PGP 署名がないために失敗する
CSCvz86846	ワークロード プロファイル ページで適用エージェントの CPU オーバーヘッドメトリックの統計が誤って報告される
CSCwa91045	内部専用 DNS でプロキシを使用している場合、3.6.1.5 へのアップグレード後に Windows エージェントが非アクティブになる
CSCwa00947	エージェントが会話モードの場合、確立されていない TCP フローのポリシーが ADM で生成される
CSCwa19256	エラー：site_enable_strong_ciphers_sensor_vip が定義されていないために 3.6.1.5 へのアップグレードが失敗する
CSCwa07367	Windows ホストにおいて、3.6(1.5) エージェントのインストールスクリプトで 3.5(1.x) エージェントのパッケージをインストールできない
CSCvk23529	センサーの導入に関するドキュメントでNICチーミングバージョンの互換性マトリクスを反映
CSCvx62775	Windows 10 Enterprise LTSC の Cisco Tetration エージェントサポートを追加
CSCvz76583	admFlowDb バッチが大きすぎると、4 時間後に ADM が失敗する。
CSCwa23206	取り込みコネクタのリスニングポートを再設定すると、コネクタが非アクティブ状態になる。
CSCvv46629	新しいワークロードが初めて表示されたときにアラートが必要

未解決のバグ

ID	見出し
CSCwb86649	40Gbps リンクのサーバーで実行されている ERSPAN センサーで 100Kpps しか受信しない
CSCwb83818	適用モードが WFP の場合に適用エージェントが Windows ファイアウォールサービスに依存する
CSCwa91086	フロー学習されたインベントリが会話モードで単方向のフローから構築される
CSCwa64962	フェデレーション/DBR：ソースクラスタからのセンサー移行のステータスを特定できない
CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある
CSCvz99865	AWS フローログの子範囲のポリシー分析が機能しない
CSCvz95962	会話モード：会話モードの短時間の非 TCP フローでクライアントサーバーが切り替わることがある
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる。

リリース 3.6.1.5 の不具合

次の表は、このリリースの不具合のリストです。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

解決済みのバグ

ID	見出し
CSCvz57109	着信 WFP フィルタにより、古い Windows リリースの一部のポリシーで後続のポートがブロックされることがある
CSCvy59198	Windows での Cisco Tetration エージェントのアップグレードで Npcap のインストールに失敗することがある
CSCvx75320	ERSPAN アプライアンスで「PENDING REGISTRATION」を反映

ID	見出し
CSCvy73310	適用エージェントで Windows システムへのファイアウォールルールの展開が断続的に繰り返される
CSCvy99946	ERSPAN エージェントが 3.5.x の後にアップグレードされない
CSCvz08788	AnyConnect の LDAP 設定から削除した後も、古い LDAP 属性がフロー検索で引き続き表示される
CSCvx88167	自動ロールマッピングによる LDAP/AD アカウントからのエージェントインストーラ スクリプトがユーザーのログアウト後に失敗する
CSCvz72734	iptables バージョン 1.8.4 の問題が原因で、Linux 適用エージェントがファイアウォールルールのプログラムに失敗する
CSCvw06912	ENH：適用アラートタイプに CPU クォータ超過のアラートを追加。
CSCvy04287	NET の脆弱性が誤って照会され、最終的に Server 2008 R2 の Cisco Tetration で FP が発生する
CSCvz45848	最新のデータパックのインストール後に CVE が検出される
CSCvy45431	Windows エージェントのインストールのエラー：古いバージョンの Cisco Tetration エージェントを削除できない
CSCvz49507	ISE 統合により、EAP チェーンおよび IP アドレス変更ケースの注釈が失効する

未解決のバグ

次の表に、このリリースで未解決になっているバグを示します。

バグ ID をクリックして、Cisco バグ検索ツールにアクセスし、そのバグに関する追加情報を表示します。

ID	見出し
CSCwb86649	40Gbps リンクのサーバーで実行されている ERSPAN センサーで 100Kpps しか受信しない
CSCwb83818	適用モードが WFP の場合に適用エージェントが Windows ファイアウォールサービスに依存する
CSCvz86846	ワークロード プロファイル ページで適用エージェントの CPU オーバーヘッドメトリックの統計が誤って報告される
CSCwb80090	Windows Server 2008 R2 と Cisco Secure Workload エージェントでクロックにずれがある

ID	見出し
CSCvz99865	AWS フローログの子範囲のポリシー分析が機能しない
CSCwa23206	取り込みコネクタのリスニングポートを再設定すると、コネクタが非アクティブ状態になる。
CSCwa00954	ADM の会話モードでプロバイダーポートが 0 に設定されたポリシーが生成される
CSCwa19256	エラー：site_enable_strong_ciphers_sensor_vip が定義されていないために 3.6.1.5 へのアップグレードが失敗する
CSCvz95962	会話モード：会話モードの短時間の非 TCP フローでクライアントサーバーが切り替わることがある
CSCwa00947	エージェントが会話モードの場合、確立されていない TCP フローのポリシーが ADM で生成される
CSCwa07367	Windows ホストにおいて、3.6(1.5) エージェントのインストールスクリプトで 3.5(1.x) エージェントのパッケージをインストールできない
CSCwa11427	会話モード：適用が有効になっている場合、39RU クラスタで 50k のセンサーがサポートされないことがある。
CSCvz95023	FMC-CSW オーケストレータ：プロトコルが any に設定されている場合、CSW で IPv6 ホップバイホップがプッシュされる。

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 プラットフォームのデータシート
- Cisco Secure Workload のドキュメント

表 *9:* 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（Cisco Secure Workload）M5 クラスタハードウェア導入ガイド

ドキュメント	説明
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
Cisco Secure Workload アップグレードガイド	Cisco Secure Workload アップグレードガイド （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

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

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

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。