# Cisco Tetration Analytics リリース ノート、リリース 3.1.1.59

このマニュアルでは、Cisco Tetration Analytics ソフトウェアの機能、不具合、および制限について説明します。

Cisco Tetration Analytics は、サーバ、Cisco Nexus®スイッチ、エンドポイント デバイス（ラップトップ、デスクトップ、スマートフォンなど）から収集された豊富なトラフィック テレメトリを使用して、包括的にデータセンターの運用およびセキュリティの課題に対応するように設計されています。プラットフォームは、ホリスティックなワークロード保護プラットフォームを提供するためのアルゴリズムアプローチを使用して高度な分析を実行します。このアルゴリズム的アプローチには、人手を介さない機械学習技術や動作分析が含まれています。プラットフォームには、次の使用事例をサポートするすぐに使用可能なソリューションが用意されています。

- 許可リストポリシーの生成を自動化する動作ベースのアプリケーションインサイトを提供する
- アプリケーションのセグメンテーションを提供して、ゼロ信頼実績を効率とセキュリティを有効にする
- オンプレミス データセンター、およびプライベート クラウドとパブリック クラウドの環境全体で一貫性のあるポリシー適用を実現する
- プロセスの動作の違い、ソフトウェアの脆弱性、および攻撃対象領域を削減するへの公開を識別する
- アプリケーションの動作の変更やポリシーの遵守違反をほぼリアルタイムに特定する
- 異種環境での包括的なテレメトリ処理をサポートすることにより、実用的な情報を数分で提供する
- スイッチとサーバーの両方から収集されたテレメトリデータに基づいた包括的なネットワークのパフォーマンス メトリック
- 詳細なフォレンジック、分析、およびトラブルシューティングのデータを長期間保持する

Cisco Tetration Analytics プラットフォーム内でケースの様々な使用事例をサポートするため、プラットフォームではデータセンター インフラストラクチャ全体からの一貫したテレメトリ データが必要です。豊富な Cisco Tetration Analytics テレメトリはセンサーを使用して収集されます。さまざまなタイプのセンサーがあり、既存と新規の両方のデータセンターインフラストラクチャのサポートに使用できます。このリリースでは、次のセンサータイプがサポートされています。

- 仮想マシン、ベアメタル、またはコンテナホストにインストールされているソフトウェアセンサー
- Cisco Nexus 9000 cloudscale シリーズスイッチの内蔵ハードウェアセンサー
- コピーされたパケットから Cisco Tetration テレメトリを生成できる ERSPAN センサー
- Cisco Tetration 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 センサー
- 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からテレメトリを収集するための Cisco AnyConnect プロキシ

ソフトウェアセンサーもまた、アプリケーションセグメンテーションのポリシー施行ポイントとしても機能します。このアプローチを使用して、Cisco Tetration Analytics 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導入全体で一貫性のある適用を実現します。センサー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、でデータパスにセンサーを置く必要がなく、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、制限や警告に関する新しい情報によって更新される場合があります。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。

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

表 1 に、このドキュメントのオンライン変更履歴を示します。

**表 1 オンライン変更履歴**

| 日付 | 説明 |
|---|---|
| 2019 年 1 月 10 日 | リリース 3.1.1.59 が利用可能になりました。 |

# 目次

このマニュアルの構成は、次のとおりです。



# 新機能および変更された機能に関する情報

このセクションでは、このリリースで追加された機能と変更された機能を一覧表示しており、次の項目を含みます。



## 新しいソフトウェア機能

このパッチ リリースには、新しいソフトウェア機能は含まれていません。

# 動作における変更

このパッチ リリースには、次の動作における変更が含まれています。

- Cisco Tetration クラスタの外部から Kafka にアクセスするポートが、9093 から 443 に変更されました。この変更は、すべての 3.1.1.x リリースに適用されます。この変更により、Datasinks 証明書と Managed Data Tap（MDT）証明書を再度ダウンロードして、kafkaBrokerIps.txt ファイル内のポートの変更を含む最新の tar.gz ファイルを取得する必要があります。

# 警告

このセクションには、未解決および解決済みの警告と既知の動作のリストが含まれています。

- 未解決の警告
- 解決済みの不具合
- 既知の動作

# 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。不具合 ID をクリックして、不具合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 2 未解決の不具合**

| 不具合 ID | 説明 |
|---|---|
| CSCvn86706 | Lookout 注釈の場合、新しい rootscope が追加されると、UAS サービスが有効でない限り、その rootscope には、UAS/Bogon タグは追加されません。 |

# 解決済みの不具合 (p.11)

次の表は、このリリースで解決済みの不具合のリストです。不具合 ID をクリックして、不具合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 3 解決済みの不具合**

| 不具合 ID | 説明 |
|---|---|
| CSCvm96270 | システム LVM モジュールでの低速なメモリリークにより、bmmgr で徐々にメモリがリークし、最終的に他のプロセスの分岐ができなくなることがあります。 |
| CSCvn52935 | ホストのネットワーク インターフェイスの名前がラテン文字以外で表されている場合、優れた可視性エージェントで 1 つのネットワーク インターフェイスからしかトラフィックがキャプチャされないことがあります。 |
| CSCvn79981 | パスワードにバックスラッシュが含まれている場合に、ユーザー名とパスワードを使用したアウトバウンド HTTP プロキシの設定が失敗していました。これにより、ログにパスワードが出力されていました。 |
| CSCvn90050 | 外部オーケストレータ データストレージのデータ保持期間が 48 時間から 1680 時間（または 40 GB）に延長されました。 |
| CSCvn90064 | 新しいセッションが作成されないように VMware vCenter のログインの動作が変更されました。 |

## 既知の動作

次のリストには、このリリースでの既知の動作が含まれています。

- 展開とアップグレード
  - Syslog (syslog サーバーおよび syslog ポート）の設定フィールドは、アップグレード/展開 GUI で廃止されています。これらのフィールドの変更は、TAN GUI でのみ行うことができます。
  - リモート CA の設定フィールド（remote CA、remote CA URL、remote CA username、remote CA password）は、物理および ESX フォームファクタではサポートされていません。
- TAN
  - ユーザーアプリケーションのアラートは、TAN 仮想アプライアンスではサポートされていません。
  - 大きなサイズのアラート（> 64k）は、UDP を介して syslog サーバに送信することはできません。
- データタップ/Kafka
  - 8 ラックユニットの展開と ESXi クラスタの設定では、Cisco Tetration は Kafka ブローカのインスタンスを 1 つだけ実行します。このため、インスタンスをホストしているベアメタルまたは VM の使用停止または再コミッションがある場合は、データが失われます。
- 施行
  - 施行を有効にしてから無効にすると、エージェントはすべてのルールをフラッシュし、キャッチオールを入力と出力の両方に許可したままにします。
  - エージェントは、最後に既知の正常なポリシーをバックエンドから保存し、サービスの再起動時にポリシーをリロードします。
  - ネットワークポリシーの更新中、Linux のエージェントは、ipset のコンテンツをフラッシュおよび再プログラミングではなく新しいコンテンツとスワップすることにより、ipset リストをよりアトミックな方法で再プログラミングします。これにより、トラフィックがドロップされる可能性が低くなります。

- ネットワークポリシーの更新中に、Windows のエージェントは、最初に Windows ファイアウォールのインバウンドおよびアウトバウンドのデフォルトポリシーを設定し、現在のルールを削除し、新しいルールをプログラミングし、ネットワークポリシー設定によって指定されたポリシーに従って、インバウンドおよびアウトバウンドのデフォルトをプログラミングします。これにより、拒否キャッチオールポリシーの場合にトラフィックがドロップされる可能性が低くなります。
- 適用されたワークスペースで適用が停止されるたびに、ユーザは施行が停止してから約15分間、そのワークスペースのオブジェクトを削除してはなりません。これにより、パイプラインがそのワークスペースの状態を更新するのに十分な時間が確保されます。削除されたアプリケーションによって参照されるユーザーインベントリフィルタまたは範囲は、アプリケーションの削除後 15 ~ 20 分間は削除されません。

- データリーク
  - データリーク検出には 5 分間の遅延があるため、データリークスコアにはデータリークイベント時間と比べて 5 分の遅延があります。
  - データリークイベントは、現在、フォレンジック分析ページには表示されていません。
- プロセスハッシュの異常
  - 周波数分析（つまり、出力スコア）は、rootscope レベルでのみ実行されます。
  - 分析は1時間に1回実行されます。
- AnyConnect
  - 複数の AnyConnect プロキシが同じ AnyConnect エンドポイントマシンからデータを取得することは推奨されません。このモードを必要とする使用事例がある場合は、Cisco にご連絡ください。
  - エンドポイントが異なるプロキシ間で反転しない限り、同じエンドポイントが異なる時点で異なるプロキシに接続できます。反転が発生した場合、AnyConnect プロキシは、このような反転が発生したときに少なくとも7日が必要になるようにシナリオを制限します。エンドポイントが2つの異なるプロキシ間で交互に接続されている反転の使用事例がある場合は、Cisco にお問い合わせください。
- Kafka でのポリシー公開
  - この機能を使用するクライアントアプリケーションの場合、この設定には Kafka ブローカーのインスタンスが 1 つしかないため、8 ラックユニットの導入と ESXi クラスタの設定を使用することは推奨されません。アプリケーションをホストしているベアメタルまたは VM の廃止/再コミッションがない場合、作成されたポリシーストリームは正しく回復されず、動作不能になります。代わりに、39ラックユニットのクラスタ設定を使用して、ポリシーストリームの可用性を高めます。
- ADM
  - ADM の実行は、現在のアプリケーションで手動で作成されたポリシーによってすでにカバーされているフローのポリシーを生成しなくなります。
  - クラスタを提供サービスとして使用することはできなくなりました。公開としてマークされ、外部アプリケーションによって参照される既存のクラスタは、インベントリフィルタに変換されます。インベントリフィルタは、範囲またはアプリケーションによって提供されるサービスを示す唯一の方法になります。
  - クラスタがインベントリフィルタに昇格されると、そのクラスタは会話ビューから削除されます。更新された IP アドレスとフィルタのマッピングを生成するには、新しい ADM を実行する必要があります。
  - 除外フィルタは、ADM の実行をまたいで実行されます。クラスタが除外フィルタの一部として使用されている場合、フローはアプリケーションがプライマリの場合にのみ削除されます。
  - Citrix ロードバランサー設定の SLB アップロードでは、ポート範囲として * を使用することはできません。設定では、1 つのポートを設定で指定する必要があります。

- TIM の設定
  - 高可用性モードで F5 が設定されている場合は、次のようになります。
    - TIM F5 プラグインは、設定されたホストのリストから 1 つの F5 のみから設定を取得します。この設定がプライマリおよびスタンバイの REST エンドポイント間で異なる F5 のすべての機能は、TIM が新しいプライマリに接続するまで、スイッチオーバー後に遅延が発生する可能性があります。
  - Netscale が HA モードで設定されているときの Citrix 設定。
    - TIM Citrix プラグインは、設定されているホストのリストから 1 つの Netscaler から設定を取得します。この設定がプライマリおよびセカンダリの REST エンドポイント間で異なる NetScaler のすべての機能は、TIM が新しいプライマリに接続するまで、スイッチオーバー後に遅延が発生する可能性があります。
  - VMware vCenter HA モードがアクティブな場合は、次のようになります。
    - TIM VMware vCenter プラグインは、一度に 1 つの VMware vCenter エンドポイントからのみ設定を取得します。VMware vCenter HA モードと TIM VMware vCenter プラグインの動作はテストされていません。

# 互換性に関する情報

このパッチを使用するには、Cisco Tetration のソフトウェアリリース 3.1.1.53、3.1.1.54、または 3.1.1.55 を実行している必要があります。

3.1.1.53 リリースの詳細については、次のリリースノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html

3.1.1.54 リリースの詳細については、次のリリースノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_54.html

3.1.1.55 リリースの詳細については、次のリリースノートを参照してください。

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_55.html

# 使用上のガイドライン

ここでは、Cisco Tetration 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40.0.0 以降を使用する必要があります。
- このリリースでは、Cisco Nexus 9300-EX スイッチのハードウェア センサーからのテレメトリと分析の収集がサポートされています。ただし、収集ルールを定義する必要があります。
- DNS を設定した後、Cisco Tetration Analytics クラスタの URL（https://<cluster.domain>）を参照します。

# 検証済みスケーラビリティの制限値

検証済みスケーラビリティの制限値については、次の URL にある『*Cisco Tetration Analytics*、*リリース 3.1.1.53*、*リリース ノート*』[英語] を参照してください。

https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_1_1_53.html

# 関連資料

Cisco Tetration Analytics のマニュアルには、次の web サイトからアクセスできます。

**Cisco Tetration プラットフォーム データシート：**
https://www.cisco.com/c/en/us/products/security/tetration/datasheet-listing.html

**一般的なドキュメント：**https://www.cisco.com/c/en/us/support/security/tetration/tsd-products-support-series-home.html

このマニュアルには、インストール情報とリリースノートが含まれています。

**表 4 インストールドキュメント**

| ドキュメント | 説明 |
|---|---|
| *Cisco Tetration Analytics クラスタ展開ガイド* | M4 ベース Cisco Tetration (39-RU) プラットフォームと Cisco Tetration-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。<br><br>ドキュメントリンク：<br>https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-Analytics-Cluster-Hardware-Deployment-Guide.html<br><br>M5 ベース Cisco Tetration (39-RU) プラットフォームと Cisco Tetration-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。<br><br>https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html |
| *Cisco Tetration Cloud 導入ガイド* | Amazon Web Services での Cisco Tetration Cloud の導入について説明します。<br><br>ドキュメント リンク：<br>http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/nexus9000/hw/Tetration/b_tetration_cloud_setup.pdf |
| *Cisco Tetration クラスターアップグレードガイド* | ドキュメントリンク：<br>https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html |
| *最新の脅威データソース* | https://updates.tetrationcloud.com/ [英語] |

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。

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。