Cisco Threat Intelligence Director（TID）

この章のトピックでは、Firepower システムで TID を設定および使用する方法について説明します。

Cisco Threat Intelligence Director（TID） の概要

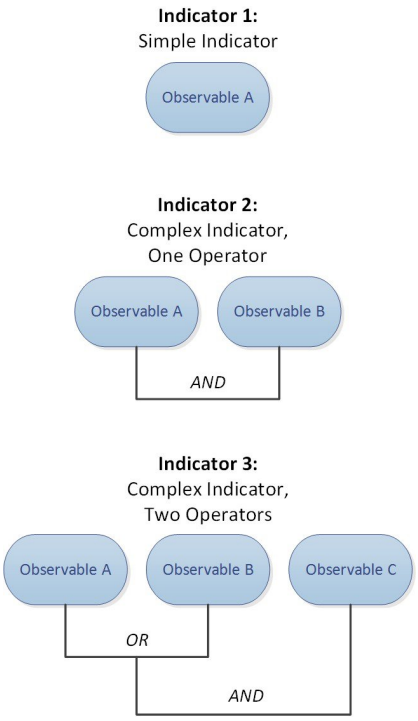
Cisco Threat Intelligence Director（TID） は脅威インテリジェンス データを操作可能にし、インテリジェンスデータの集約、防衛アクションの設定、環境内の脅威の分析を支援します。この機能は、Firepower の他の機能を補完するもので、脅威に対する追加の防衛線を提供します。

TID をホスティング プラットフォームに設定すると、脅威インテリジェンス ソースからデータが取り込まれ、設定されたすべての管理対象デバイス（要素）にそのデータが公開されます。このリリースでサポートされているホスティングプラットフォームと要素の詳細については、プラットフォーム、要素、およびライセンスに関する要件 （5 ページ） を参照してください。

ソースには、オブザーバブルを含むインジケータが含まれています。インジケータは、脅威に関連するすべての特性を伝達し、個々のオブザーバブルは、その脅威に関連付けられた個々の特性（例えば、SHA-256 値）を表します。単純なインジケータには単一のオブザーバブルが含まれ、複合インジケータには 2 つ以上のオブザーバブルが含まれます。

オブザーバブルとそれらの間の AND/OR 演算子は、次の例に示すように、インジケータのパターンを形成します。

図 *1:* 例：インジケータ パターン



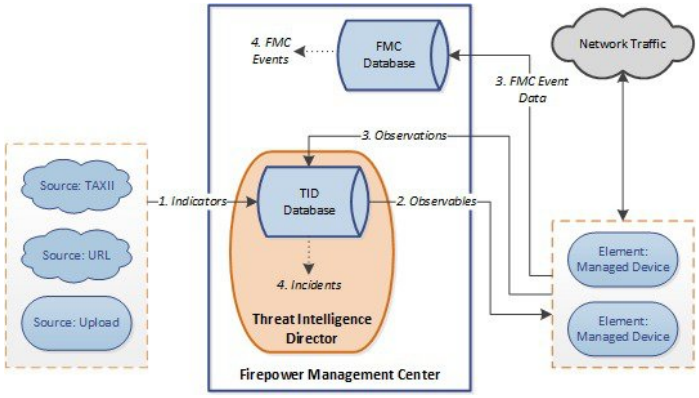
オブザーバブルが要素に公開された後、要素はトラフィックをモニタし、システムがトラフィック内のオブザーバブルを識別すると、Firepower Management Center にオブザベーションを報告します。

Firepower Management Center は、すべての要素からのオブザベーションを収集し、TID インジケータに対してオブザベーションを評価して、オブザーバブルの親インジケータに関連付けられたインシデントを生成または更新します。

インシデントは、インジケータのパターンが満たされたときに完全に実現されます。トラフィックがインジケータ内の 1 つまたは複数のオブザーバブルに一致するが、パターン全体では一致しない場合、インシデントは部分的に実現されます。詳細については、監視とインシデント生成 （18 ページ）を参照してください。

次の図に、サンプルの Firepower システム構成におけるデータ フローを示します。

図 *2 : Firepower Management Center* のデータ フロー



TIDインシデントが完全または部分的に実現されると、システムは設定されたアクション（モニタ、ブロック、部分的なブロック、またはアクションなし）を実行します。詳細は、アクションに影響を与える要因 （32 ページ）を参照してください。

TID およびセキュリティ インテリジェンス

アクセス コントロール ポリシーの一部として、セキュリティ インテリジェンスではレピュテーション インテリジェンスを使用して、IP アドレス、URL、およびドメインとの間の接続をすばやくブロックします。セキュリティ インテリジェンスは、Cisco Talos Security Intelligence and Research Group（Talos）からの業界をリードする脅威インテリジェンスへのアクセスを一意に提供します。セキュリティ インテリジェンスの詳細については、セキュリティ インテリジェンスについてを参照してください。

TID は、サードパーティのソースからのセキュリティ インテリジェンスに基づいて接続をブロックするシステムの機能を次のように拡張します。

- **TIDは、追加のトラフィック フィルタリング基準をサポート**：セキュリティインテリジェンスは、IP アドレス、URL、および（DNS ポリシーが有効な場合は）ドメイン名に基づいてトラフィックをフィルタリングできるようにします。TIDでも、これらの基準によるフィルタリングをサポートし、SHA-256ハッシュ値に基づくフィルタリングのサポートを追加します。

- **TID は、追加のインテリジェンス取り込み方法をサポート**：セキュリティ インテリジェンスおよびTIDの両方を使用して、フラット ファイルを手動でアップロードするか、サードパーティ ホストからフラット ファイルを取得するようにシステムを構成することで、システムに脅威インテリジェンスをインポートできます。TIDは、これらのフラットファイルの管理における柔軟性を向上させます。また、TID は Structured Threat Information eXpression（STIX™）形式で提供されるインテリジェンスを取得して取り込むことができます。

- **TID は、フィルタリング処理のきめ細かい制御を提供**：セキュリティ インテリジェンスにより、ネットワーク、URL、または DNS オブジェクトによるフィルタリング基準を指定できます。セキュリティインテリジェンス オブジェクト（特にリストおよびフィード）には、複数の IP アドレス、URL、DNS ドメイン名を含めることができますが、ブラック

リストまたはホワイトリストに含めることができるのは、オブジェクトの個別のコンポーネント単位ではなく、オブジェクト単位です。TIDを使用すると、個別の基準（つまり簡易インジケータまたは個別のオブザーバブル）に対するフィルタリング処理を構成できます。

- **TID 構成の変更には再展開は不要**：アクセス コントロール ポリシーでセキュリティ インテリジェンス設定を変更したら、管理対象デバイスに変更された構成を再展開する必要があります。TID では、管理対象デバイスへのアクセス コントロール ポリシーの初期展開後に、ソース、インジケータ、およびオブザーバブルを再展開せずに構成でき、システムによって新しい TID データが要素に自動的に公開されます。

セキュリティ インテリジェンスまたは TID が特定のインシデントに対処できるときに、システムがどのように機能するかについては、TID-Firepower Management Center のアクションの優先順位付け （27 ページ）を参照してください。

Threat Intelligence Director のパフォーマンスへの影響

Firepower Management Center

いくつかのケースで、次のような場合があります。

- 特に大きな STIX ソースを取り込んでいる間にシステムのパフォーマンスがわずかに低下することがあり、取り込みが完了するまでに時間がかかることがあります。
- 新しいまたは変更された TID データを要素に公開するまでに、最大 15 分かかることがあります。

管理対象デバイス（Managed Device）

例外的なパフォーマンスの影響はありません。TID は、Firepower Management Center セキュリティ インテリジェンスの機能と同じようにパフォーマンスに影響します。

Cisco Threat Intelligence Director（TID） およびハイ アベイラビリティ構成

ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

詳細は、TID データのバックアップおよび復元について （17 ページ）を参照してください。

Threat Intelligence Director の要件

プラットフォーム、要素、およびライセンスに関する要件

ホスティング プラットフォーム

次の物理および仮想 Firepower Management Center で TID をホスティングできます。

- Firepower システムのバージョン 6.2.2 以降を実行している。
- 最小 15 GB のメモリで構成されている。
- REST API アクセスが有効な状態で構成されている。REST API アクセスの有効化を参照してください。

要素

デバイスが Firepower システムのバージョン 6.2.2 以降を実行している場合は、任意の Firepower Management Center 管理対象デバイスを TID 要素として使用できます。

ライセンシング

SHA-256 のオブザーバブルの公開用のファイル ポリシーを設定する場合は、Firepower システムにマルウェア ライセンス（従来またはスマート）が必要です。

詳細については、TID をサポートするためのポリシーの設定 （8 ページ）およびFirepower の機能ライセンスについてを参照してください。

ソース要件

ソース タイプの要件：

STIX

ファイルは、STIX バージョン 1.0、1.1、1.1.1、または 1.2 であり、STIX ドキュメントのガイドライン（http://stixproject.github.io/documentation/suggested-practices/）に準拠していなければなりません。

STIX ファイルには複雑なインジケータを含めることができます。

フラット ファイル（Flat File）

ファイルは、1 行に 1 つのオブザーバブル値を持つ ASCII テキスト ファイルでなければなりません。

フラットファイルには、簡易インジケータ（インジケータごとに1つのオブザーバブル）しか含まれていません。

TID では、以下はサポートされません。

- オブザーバブル値を区切る区切り文字（たとえば、`observable,` は無効です）。
- オブザーバブル値を囲む囲み文字（たとえば、`"observable"` は無効です）。

各ファイルには、コンテンツ タイプを 1 つしか含めることができません。

- `SHA-256`：SHA-256 ハッシュ値。
- `Domain`：RFC 1035 で規定されているドメイン名。
- `URL`：RFC 1738 で規定されている URL。

（注） TIDは、ポート、プロトコル、または認証情報を含むURLを正規化し、インジケータを検出するときに正規化されたバージョンを使用します。たとえば、TID は次の URL を正規化します。

```
http://google.com/index.htm
http://google.com:8080/index.htm
google.com:8080/index.htm
google.com/index.htm
```

as:

```
google.com/index.htm
```

または、TID はたとえば次の URL を正規化します。

```
http://abc@google.com:8080/index.htm
```

これを次のように更新します。

```
abc@google.com/index.htm/
```

- `IPv4`：RFC 791 で規定されている IPv4 アドレス。

  TID は CIDR ブロックを受け入れません。

- `IPv6`：RFC 4291 で規定されている IPv6 アドレス。

  TID はプレフィックス長を受け入れません。

ソースの配信要件：

アップロードするファイルとしては、500 MB 以下のものが可能です。

ソース コンテンツの制限事項

システムにより、URL オブザーバブルの最初の 1000 文字のみが取り込まれ、照合されます。

Cisco Threat Intelligence Director（TID） のセットアップ方法

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

（注） TID の設定や操作中に問題が発生した場合は、Cisco Threat Intelligence Director（TID） のトラブルシューティング （52 ページ）を参照してください。

手順

ステップ 1 インストールしたものが TID を実行するための要件を満たしていることを確認します。

参照先： プラットフォーム、要素、およびライセンスに関する要件 （5 ページ）

ステップ 2 管理対象デバイスごとに、TIDをサポートするために必要なポリシーを設定し、それらのポリシーをデバイスに展開します。

TID をサポートするためのポリシーの設定 （8 ページ）を参照してください。

インテリジェンス データ ソースを取り込む前または後で要素を設定できます。

ステップ 3 TID で取り込むインテリジェンス ソースを設定します。

ソース要件 （5 ページ）とデータ ソースを取り込むためのオプション （9 ページ）の下のトピックを参照してください。

ステップ 4 要素にデータをまだ公開していない場合は、公開します。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。

次のタスク

- 定期的にスケジュールされたバックアップに TID を含めます。TID データのバックアップおよび復元について （17 ページ）を参照してください。

  Firepower Management Center の展開がハイ アベイラビリティ構成である場合は、Cisco Threat Intelligence Director（TID） およびハイ アベイラビリティ構成も参照してください。

- （オプション）必要に応じて、TID 機能に管理アクセスを付与します。TID アクセス権を持つユーザ ロール （17 ページ）および管理アクセス用のユーザ アカウントを参照してください。
- 操作中に必要に応じて、設定を微調整します。たとえば、誤検出インシデントを生成するオブザーバブルをホワイトリストに登録します。Cisco Threat Intelligence Director（TID）設定の表示および変更 （33 ページ）を参照してください。

TID をサポートするためのポリシーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

Firepower Management Center から管理対象デバイス（要素）に TID データを公開するには、アクセス コントロール ポリシーを設定する必要があります。さらに、最大限のオブザベーションおよび Firepower Management Center イベント生成を行うためにアクセス コントロール ポリシーを設定することを推奨します。

TID をサポートする各管理対象デバイスに対し、次の手順を実行して、関連付けられたアクセス コントロール ポリシーを設定します。

データが公開された後に TID を使用するように設定されている要素は、現在公開されているすべてのオブザーバブルを自動的に受信します。

手順

ステップ 1 アクセス コントロール ポリシーの [詳細設定（Advanced Settings）] タブで、[Threat Intelligence Director を有効にする（Enable Threat Intelligence Director）] チェックボックスがオンになっていることを確認します。このオプションは、デフォルトで有効です。

詳細については、アクセス コントロール ポリシーの詳細設定を参照してください。

ステップ 2 ルールがまだない場合は、アクセス コントロール ポリシーにルールを追加します。TID では、アクセス コントロール ポリシーが少なくとも 1 つのルールを指定する必要があります。

詳細については、基本的なアクセス コントロール ポリシーの作成を参照してください。

ステップ 3 アクセス コントロール ポリシーのデフォルト アクションとして [侵入防御（Intrusion Prevention）] を選択し、TID 検出のためにトラフィックを復号する場合は、SSL ポリシーをアクセス コントロール ポリシーに関連付けます。アクセス制御への他のポリシーの関連付けを参照してください。

ステップ 4 SHA-256 オブザーバブルにオブザベーションおよび Firepower Management Center イベントを生成させる場合：

a) 1 つ以上の [マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ルールを含むファイル ポリシーを作成します。

詳細については、ファイル制御および AMP を実行するアクセス コントロール ルールの設定を参照してください。

b) このファイル ポリシーを、アクセス コントロール ポリシーの 1 つ以上のルールと関連付けます。

ステップ 5 [IPv4]、[IPv6]、[URL]、または [ドメイン名（Domain Name）] のオブザベーションで接続およびセキュリティ インテリジェンスイベントを生成する場合は、アクセス コントロール ポリシーで接続およびセキュリティ インテリジェンスのロギングを有効にします。

a) ファイル ポリシーを呼び出したアクセス コントロール ルールで、[接続の終了時にロギング（Log at End of Connection）] および [ファイル イベント：ログファイル（File Events: Log Files）] を有効にします（まだ有効になっていない場合）。

詳細については、アクセス制御ルールによる接続のロギングを参照してください。

b) セキュリティ インテリジェンス設定でデフォルトのロギング（[DNS ポリシー（DNS Policy）]、[ネットワーク（Networks）]、および [URL（URLs）]）が有効になっていることを確認します。

詳細については、セキュリティ インテリジェンスによる接続のロギングを参照してください。

ステップ 6 設定変更を展開します。設定変更の展開を参照してください。

次のタスク

残りの項目を入力します。 Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ）

データ ソースを取り込むためのオプション

使用するデータ タイプと配信メカニズムに基づいて構成オプションを選択します。

これらのデータ タイプの詳細については、ソース要件 （5 ページ） を参照してください。

表 *1:* データ ソースを取り込むためのオプション

データ タイプ	取り込みオプション
STIX	• TAXII サーバからの STIX フィードの取り込み： 参照先： ソースとして使用する TAXII フィードの取得 （10 ページ） • URL からの STIX データのダウンロード： 参照先： URL からのソースの取得 （12 ページ） • STIX ファイルのアップロード： 参照先： ソースとして使用するローカル ファイルのアップロード（13 ページ）
フラット ファイル	• URL からのデータのダウンロード： 参照先： URL からのソースの取得 （12 ページ） • フラット ファイルのアップロード： 参照先： ソースとして使用するローカル ファイルのアップロード（13 ページ）

ソースとして使用する TAXII フィードの取得

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

TID の設定や操作中に問題が発生した場合は、を参照してください。 Cisco Threat Intelligence Director（TID） のトラブルシューティング （52 ページ）

手順

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （5 ページ）

ステップ 2 **[インテリジェンス（Intelligence）]** > **[ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（＋）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [TAXII] を選択します。

ステップ 5 情報を入力します。

- ホスト サーバで暗号化された接続が必要な場合は、TID ソースの SSL 設定の構成 （15 ページ） の説明に従って [SSL 設定（SSL Settings）] を構成します。
- TAXII ソースの [アクション（Action）] 選択を変更することはできません。

  STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、TAXII ソースの `Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。
- フィードのリストが読み込まれるまでには時間がかかることがあります。
- [更新頻度（Update Every）] 間隔は、TID が TAXII ソースから更新を取得する頻度を指定します。

  データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。
- [TTL] に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）] スライダ（  ）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソースデータとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- TAXII フィードには大量のデータが含まれている可能性があるため、システムがすべてのデータを取り込むまでに時間がかかることがあります。取り込みステータスを表示するには、[ソース（Sources）] ページを更新します。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ） に戻ります。

URL からのソースの取得

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

TID でホストからファイルを取得する場合は、URL ソースを設定します。

TID の設定や操作中に問題が発生した場合は、を参照してください。 Cisco Threat Intelligence Director（TID） のトラブルシューティング （52 ページ）

手順

ステップ 1 次の要件をソースが満たしていることを確認します。 ソース要件 （5 ページ）

ステップ 2 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（＋）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [URL] を選択します。

ステップ 5 フォームに入力します。

- フラット ファイルを取り込む場合は、ソース内に含まれるデータを記述する [コンテンツ（Content）] タイプを選択します。
- ホスト サーバで暗号化された接続が必要な場合は、TID ソースの SSL 設定の構成 （15 ページ） の説明に従って **SSL 設定**を構成します。
- 名前については、TIDインジケータに基づいてインシデントのソートと処理を簡略化するには、ソースすべてで一貫性のある命名方式を使用します。たとえば、<source>-<type> などです。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。
- STIX ファイルを取り込む場合は、STIX データに（システムがブロックできない）複雑なインジケータが含まれている可能性があるため、Block が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

ただし、取り込み後は、個々のオブザーバブルと、そのソースから取得した簡易インジケータをブロックすることができます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。

- データ ソースを更新する有効な更新頻度を設定します。たとえば、ソースを 1 日に 3 回更新する場合、更新間隔を 1440/3 または 480 分に設定して、定期的に最新データをキャプチャします。
- [TTL] 間隔に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のソース更新に含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）] スライダ（  ）が有効になっていることを確認します。

このオプションを有効にすると、システムは自動的に初期ソースデータとそれに続く変更を公開します。

詳細は、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）] ページを更新します。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ） に戻ります。

ソースとして使用するローカル ファイルのアップロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

この手順は、ローカル ファイルのワンタイム手動アップロードに使用します。

STIX ファイルを取り込むと、TID によって STIX ファイルの内容から単純または複雑なインジケータが作成されます。

フラット ファイルを取り込むと、TID によってファイル内のオブザーバブル値ごとに簡易インジケータが作成されます。

TID の設定や操作中に問題が発生した場合は、を参照してください。 Cisco Threat Intelligence Director（TID） のトラブルシューティング （52 ページ）

手順

ステップ 1 の要件をファイルが満たしていることを確認します。 ソース要件 （5 ページ）

ステップ 2 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 3 追加アイコン（＋）をクリックします。

ステップ 4 ソースの [配信（Delivery）] 方法として [アップロード（Upload）] を選択します。

ステップ 5 フォームに入力します。

- フラット ファイルをアップロードする場合は、ソース内に含まれるデータを記述する [コンテンツ（Content）] タイプを選択します。
- 名前については、TIDインジケータに基づいてインシデントのソートと処理を簡略化するには、ソースすべてで一貫性のある命名方式を使用します。たとえば、<source>-<type> などです。

  ソース名も追加すると、追加の情報やフィードバックのためにソースに返信することが簡単になります。

  一貫性のある名前を入力してください。たとえば、IPv4アドレスを含むソースの場合、常に IPV4 を使用します（IPv4、ipv4、IP_v4、IP_V4、ip-v4、IP-v4、IP-V4 などは使用しません）。
- STIX ファイルをアップロードする場合は、STIX データに複雑なインジケータが含まれている可能性があるため、`Block` が [アクション（Action）] オプションになりません。デバイス（要素）は、単一のオブザーバブルに基づいて保存してアクションを実行します。複数のオブザーバブルに基づいてアクションを実行することはありません。

  ただし、インジケータまたはオブザーバブル レベルで簡易インジケータをブロックすることはできます。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。
- [TTL] 間隔に指定された日数の経過後に、TID が以下のものを削除します。
  - 以降のアップロードに含まれないソースのインジケータのすべて。
  - 残ったインジケータによって参照されないすべてのオブザーバブル。

ステップ 6 要素への公開をすぐに開始する場合は、[公開（Publish）] スライダ（  ）が有効になっていることを確認します。

取り込み時にソースを公開しない場合、後ですべてのソースインジケータを一度に公開することはできません。代わりに、各オブザーバブルを個別に公開する必要があります。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- 取り込みステータスを表示するには、[ソース（Sources）] ページを更新します。
- 初期の TID 設定を行っている場合は、Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ） に戻ります。

TID ソースの SSL 設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

ホスト サーバで暗号化された接続が必要な場合は、**SSL 設定**を構成します。

始める前に

- ソースとして使用する TAXII フィードの取得 （10 ページ） または URL からのソースの取得 （12 ページ） の説明に従って、`TAXII` または `URL` ソースの設定を開始します。

手順

ステップ 1 [ソースの編集（Edit Source）] ダイアログで、[SSL 設定（SSL Settings）] セクションを展開します。

ステップ 2 サーバ証明書が自己署名されている場合：

a) [自己署名証明書（Self-Signed Certificate）] を有効にします。

b) [SSL ホスト名検証（SSL Hostname Verification）] 方式を選択します。

- [厳格（Strict）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID は複数のサブドメインと一致することはできません。

- [ブラウザ互換性あり（Browser Compatible）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要があります。

  ホスト名にワイルドカードが含まれる場合、TID はすべてのサブドメインに一致します。

- [すべて許可（Allow All）]：TID では、ソース **URL** がサーバ証明書に指定されたホスト名と一致する必要はありません。

たとえば、`subdomain1.subdomain2.cisco.com` がソース **URL** で、`*.cisco.com` がサーバ証明書で指定されたホスト名である場合は、次のようになります。

- [厳格（Strict）] ホスト名検証は失敗します。
- [ブラウザ互換性あり（Browser Compatible）] ホスト名検証は成功します。
- [すべて許可（Allow All）] ホスト名検証では、ホスト名の値は完全に無視されます。

c) [サーバ証明書（Server Certificate）] の場合：

- PEM エンコードおよび自己署名されたサーバ証明書にアクセスできる場合は、テキスト エディタで証明書を開き、`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含むテキスト ブロック全体をコピーします。この文字列全体をフィールドに入力します。
- 自己署名されたサーバ証明書にアクセスできない場合は、フィールドを空白のままにします。ソースを保存すると、TID はサーバから証明書を取得します。

ステップ 3 サーバにユーザ証明書が必要な場合：

a) [ユーザ証明書（User Certificate）] を入力します。

テキスト エディタで PEM エンコードされた証明書を開いて、`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含むテキストのブロック全体をコピーします。この文字列全体をフィールドに入力します。

b) [ユーザ秘密キー（User Private Key）] を入力します。

テキスト エディタで秘密キー ファイルを開き、`BEGIN RSA PRIVATE KEY` および `END RSA PRIVATE KEY` 行を含むテキスト ブロック全体をコピーします。この文字列全体をフィールドに入力します。

次のタスク

- 証明書の有効期限を記録します。現在の証明書の有効期限が切れた後に、新しいサーバ証明書を入力するためのカレンダー通知を設定することもできます。
- ソースの設定を続けます。
  - ソースとして使用する TAXII フィードの取得 （10 ページ）
  - URL からのソースの取得 （12 ページ）

TID アクセス権を持つユーザ ロール

Firepower Management Center ユーザ アカウントを使用して、TID のメニューやページにアクセスすることができます。

- [管理者（Admin）] または [Threat Intelligence Director ユーザ（Threat Intelligence Director User）] のユーザ ロールを持つアカウント。
- [インテリジェンス（Intelligence）]権限を含むカスタム ユーザ ロールを持つアカウント。

さらに、[管理者（Admin）]、[アクセス管理者（Access Admin）]、または [ネットワーク管理者（Network Admin）] のユーザ ロールを持つ Firepower Management Center ユーザ アカウントを使用して、アクセス コントロール ポリシーでTIDを有効または無効にすることができます。

ユーザ アカウントの詳細については、管理アクセス用のユーザ アカウントを参照してください。

TID データのバックアップおよび復元について

Firepower Management Center を使用して、TID に必要なすべてのデータ（要素データ、セキュリティ インテリジェンス イベント、接続イベント、TID 構成、および TID データ）をバックアップおよび復元できます。

（注） ハイ アベイラビリティ構成のアクティブな Firepower Management Center で TID をホスティングする場合、システムは TID 構成と TID データをスタンバイ Firepower Management Center に同期しません。フェールオーバー後にデータを復元できるように、アクティブ Firepower Management Center で TID データの定期的なバックアップを実行することを推奨します。

表 *2 : TID* 関連のバックアップおよび復元ファイルの内容

TID 関連ファイルの内容	バックアップの選択	復元の選択
要素データ	バックアップ構成	設定データの復元（Restore Configuration Data）
Firepower Management Center イベント データ	イベントのバックアップ	イベント データの復元（Restore Event Data）
TID 構成および TID データ	Threat Intelligence Director のバックアップ	Threat Intelligense Director データの復元

詳細については、Firepower Management Center のバックアップおよびバックアップ ファイルからのアプライアンスの復元を参照してください。

TID インシデントおよびオブザベーション データの分析

TID要素によって生成されたインシデントおよびオブザベーションデータを分析するには、インシデント表およびインシデント詳細ページを使用します。

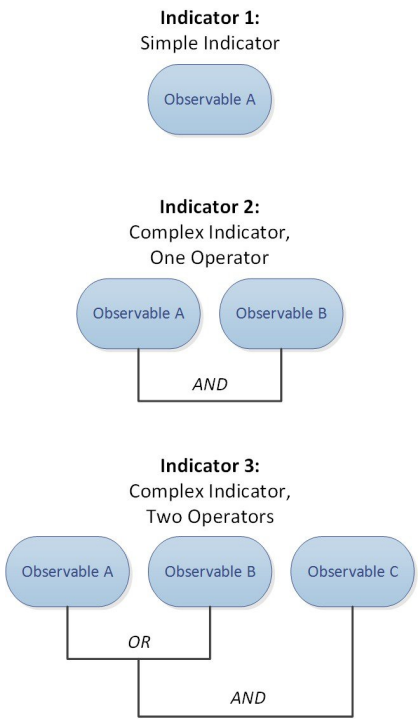
監視とインシデント生成

TIDは、インジケータに対する最初のオブザーバブルがトラフィックに見られたときにインシデントを生成します。単一の監視後、簡易インジケータが完全に実現されます。複雑なインジケータは、1 つ以上の追加の監視がそのパターンを実行するまで、部分的に実現されます。複雑なインジケータは、必ずしも単一のトランザクション中に達成される必要はありません。各オブザーバブルは、異なるトランザクションにより、時間の経過とともに個別に達成できます。

（注） TIDは、インジケータのパターンを評価するときに、サポートされていない、無効な、およびホワイトリストに登録されたオブザーバブルを無視します。

インシデントが完全に実現された後、その後の監視で新しいインシデントがトリガーされます。

図 *3:* 例：インジケータ パターン



TIDが上記の例からのオブザーバブルを取り込み、オブザーバブルが順番に確認されると、インシデント生成は次のように進行します。

1. システムがトラフィック中のオブザーバブル A を識別すると、TID は次のようになります。
   - インジケータ 1 に対して完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、部分的に実現されたインシデントを生成します。
2. システムがトラフィック中のオブザーバブル B を識別すると、TID は次のようになります。
   - インジケータ 2 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。
   - インジケータ 3 については、インシデントを [部分的に実現（partially-realized）] に更新します。
3. システムがトラフィック中のオブザーバブル C を識別すると、TID は次のようになります。
   - インジケータ 3 については、パターンが達成されたのでインシデントを [完全に実現（fully-realized）] に更新します。
4. システムがオブザーバブル A をもう一度識別すると、TID は次のようになります。
   - インジケータ 1 に対して新しい完全に実現されたインシデントを生成します。
   - インジケータ 2 とインジケータ 3 に対して、新しい部分的に実現されたインシデントを生成します。

特定のインジケータが複数のソースに存在する場合、重複インシデントが表示される場合があります。詳細については、Cisco Threat Intelligence Director（TID） のトラブルシューティング（52 ページ）を参照してください。

インシデントは実際のトラフィックによってのみ生成されることに注意してください。URL B のオブザーバブルがあり、ユーザが URL B へのリンクを表示する URL A にアクセスした場合は、ユーザが URL B のリンクをクリックしない限り、インシデントは発生しません。

インシデントの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

[インシデント（Incidents）] ページには、最大 110 万件の最新の TID インシデントに関する要約情報が表示されます。（インシデント サマリー情報 （21 ページ）を参照）。

始める前に

- Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ）の説明に従って機能を設定します。
- 監視とインシデント生成 （18 ページ）の説明を読んで、オブザベーションとインシデント生成について理解します。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]** の順に選択します。

ステップ 2 次のようにインシデントを確認します。

- 1 つ以上のフィルタを追加するには、[フィルタ（Filter）] アイコン（🔍）をクリックします。デフォルトのフィルタは6時間です。詳細については、テーブル ビューでの TID データのフィルタ処理 （43 ページ）を参照してください。
- TID でインシデントが最後に更新された日時を表示するには、[最終更新日（Last Updated）] 列内の値の上にカーソルを置きます。
- インシデントに関連付けられているインジケータについての詳細を表示するには、[インジケータ名（Indicator Name）] 列内のテキストをクリックします（インジケータの表示と管理 （38 ページ）を参照）。

ステップ 3 [インシデントID（Incident ID）] 列の値をクリックして、その他の詳細を表示します。

表示される詳細の説明については、インシデントの詳細 （22 ページ）を参照してください。

- インジケータの詳細を表示するには、ウィンドウ下部の [インジケータ（Indicator）] 見出しのインジケータ値（IP アドレスや SHA-256 の値など）をクリックします。
- オブザベーションの詳細を表示するには、[オブザベーション（Observations）] 見出しのすぐ下のオブザベーションの左にある矢印をクリックします。

- [Security Intelligence Events（セキュリティ インテリジェンス イベント）] ページでこのインシデントを表示するには、オブザベーション詳細セクションで [イベント（Events）] リンクをクリックします。

ステップ 4 （オプション）インシデント詳細ページで詳細情報を入力します。

ヒント：次のオプションの一貫性と有用性を最大化するには、方針を作成したうえで、命名規則、カテゴリの選択、および信頼度レベル基準を文書化します。

- [名前（Name）]、[説明（Description）] および [カテゴリ（Category）] フィールドに任意の値を入力します。
- [信頼度（Confidence）] の評価レベルをクリックします。
- インシデントの調査ステータスを指定するには、[ステータス（Status）] フィールドのドロップダウン リストから値を選択します。

インシデント サマリー情報

[インシデント（Incidents）] ページには、すべての TID インシデントのサマリー情報が表示されます。

表 *3*: インシデント サマリー情報

フィールド	説明
最終更新日	システムまたはユーザが最後にインシデントを更新してからの日数。更新の日時を表示するには、この列の値にマウスオーバーします。
[インシデント ID（Incident ID）]	インシデントの固有識別子。この ID の形式は次のとおりです。 `<type>-<date>-<number>` • `<type>`：インシデントに関係するインジケータまたはオブザーバブルのタイプ。単純なインジケータの場合、この値はオブザーバブルのタイプ（`IP`（IPv4 または IPv6）、`URL`（URL）、`DOM`（ドメイン）、または `SHA`（SHA-256））を示します。複雑なインジケータの場合、この値は `COM` です。 • `<date>`：インシデントが作成された日付（*yyyymmdd*）。 • `<number>`：インシデント番号。これは、1 日に作成されたインシデントの中での順序を示す番号です。この順序は 0 で始まることに注意してください。たとえば、`DOM-20170828-10` はその日に作成された 11 番目のインシデントです。 識別子の隣には、インシデントが部分的に実現された（）か、完全に実現された（）かを示すアイコンが表示されます。詳細については、監視とインシデント生成 （18 ページ）を参照してください。

フィールド	説明
[インジケータ名（Indicator Name）]	インシデントに関係するインジケータの名前。インジケータの追加情報を表示するには、この列の値をクリックします。インジケータの表示と管理 （38 ページ）を参照してください。
タイプ（Type）	インシデントに関係するインジケータのタイプ。 • 単一のオブザーバブルを含むインジケータでは、データ型（`URL`、`SHA-256` など）が表示されます。 • 2 つ以上のオブザーバブルを含むインジケータは、`Complex` として表示されます。
[実施アクション（Action Taken）]	インシデントに関してシステムが実行するアクション。詳細については、インシデントの詳細 （22 ページ）を参照してください。
ステータス	インシデントに関する調査のステータスです。詳細については、インシデントの詳細 （22 ページ）を参照してください。
	このアイコンをクリックすると、インシデントが完全に削除されます。

インシデントの詳細

[インシデントの詳細（Incident Details）] ウィンドウには、単一の TID インシデントに関する情報が表示されます。このウィンドウは、2 つのセクションで構成されています。

- インシデントの詳細：基本情報 （22 ページ）
- インシデントの詳細：インジケータとオブザベーション （23 ページ）

インシデントの詳細：基本情報

[インシデントの詳細（Incident Details）] ウィンドウの上部セクションでは、次の情報が提供されます。

表 *4*：基本的なインシデント情報フィールド

フィールド	説明
IncidentID または *IncidentID*	インシデントのステータス（部分的に実現または完全に実現）およびインシデントの一意の ID を示すアイコン。 （注） TID は、インシデントのステータスを決定するときに、サポートされていない、無効な、およびホワイトリストに登録されたオブザーバブルを無視します。
[既読（Opened）]	インシデントが最後に更新された日時。

フィールド	説明
[名前（Name）]	手動で入力するオプションのカスタム インシデント名。 ヒント：[説明（Description）]フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントに名前を付けます。
説明	手動で入力するオプションのカスタム インシデント説明。 ヒント：[説明（Description）]フィールド（ウィンドウの下部）にソースからの情報がある場合は、そのフィールドの情報を使用してインシデントについて説明します。
[オブザベーション（Observations）]	インシデント内のオブザベーションの数。
信頼性（Confidence）	インシデントの相対的な重要度を示すために手動で選択できるオプションの評価。
[実施アクション（Action Taken）]	システムによって実行されるアクション：[モニタ済み（Monitored）]、[ブロック済み（Blocked）]、または [部分的にブロック済み（Partially Blocked）]。 [部分的にブロック済み（Partially Blocked）] は、インシデントに [モニタ済み（Monitored）] と [ブロック済み（Blocked）] の両方のオブザベーションが含まれていることを示します。 （注） [実施アクション（Action Taken）] は、システムによって実行されるアクションを示しますが、必ずしも TID で選択されているアクションではありません。詳細については、TID-Firepower Management Center のアクションの優先順位付け （27 ページ）を参照してください。
カテゴリ（Category）	インシデントに手動で追加するオプションのカスタム タグまたはキーワード。
ステータス	インシデントの分析の現在の段階を示す値。すべてのインシデントは、[ステータス（Status）]を初めて変更するまでは [新規（New）] です。 このフィールドは任意です。組織のニーズに応じて、以下のステータス値を使用することを検討してください。 • [新規（New）]：インシデントには調査が必要ですが、まだ調査を開始していません。 • [オープン（Open）]：現在インシデントを調査しています。 • [クローズ済み（Closed）]：インシデントを調査し、対処しました。 • [却下（Rejected）]：インシデントを調査し、実行するアクションはないと判断しました。
🗑	このアイコンをクリックすると、このインシデントが完全に削除されます。

インシデントの詳細：インジケータとオブザベーション

[インシデントの詳細（Incident Details）] ウィンドウの下部セクションには、インジケータとオブザベーションの詳細情報が表示されます。この情報は、[インジケータ（Indicator）]フィー

ルド、インジケータ パターン、および [オブザベーション（Observations）] フィールドとして編成されています。

[インジケータ（Indicator）] セクション

インジケータの詳細を初めて表示するときには、このセクションにはインジケータ名のみが表示されます。

[インジケータ（Indicator）] ページでインジケータを表示するには、インジケータ名をクリックします。

インジケータ名の隣にある下矢印をクリックすると、インシデントを閉じることなくインジケータの詳細を表示できます。詳細フィールドには、次のものがあります。

表 5: インジケータのフィールド

フィールド	説明
説明	ソースから提供されたインジケータの説明。
ソース（Source）	インジケータが含まれていたソース。このリンクをクリックすると、完全なソースの詳細にアクセスできます。
[有効期限（Expires）]	ソースの [TTL] 値に基づく、インシデントが期限切れになる日時。
[操作（Action）]	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集（46 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開（48 ページ）を参照してください。
[STIX のダウンロード（Download STIX）]	ソース タイプが `STIX` の場合は、このボタンをクリックして STIX ファイルをダウンロードします。

[インジケータ パターン（Indicator Pattern）]

インジケータ パターンは、インジケータを構成するオブザーバブルおよび演算子のグラフィカル表示です。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は [AND] 演算子で示されます。OR 関係は、**OR** 演算子、または複数のオブザーバブルの緊密なグループ化によって示されます。

パターンのオブザーバブルがすでに観測されている場合、オブザーバブル ボックスは白色です。オブザーバブルがまだ観測されていない場合、オブザーバブル ボックスは灰色です。

インジケータ パターンで、次のようにします。

- ホワイトリスト アイコン（）をクリックして、オブザーバブルをホワイトリストに追加します。このアイコンは、白色と灰色の両方のオブザーバブル ボックスに表示されます。詳細については、TID オブザーバブルのホワイトリスト登録について （50 ページ）を参照してください。
- 白色のオブザーバブル ボックスにマウスオーバーすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示されます。
- 白色のオブザーバブル ボックスをクリックすると、[オブザベーション（Observations）] セクションで関連するオブザベーションが強調表示され、そのオブザベーションがスクロールされて表示されて（複数のオブザベーションが存在する場合）、そのオブザベーションの詳細表示が展開されます。
- インジケータ パターンで灰色のオブザーバブル ボックスをマウスオーバーまたはクリックした場合、[オブザベーション（Observations）] セクションに変化はありません。これは、オブザーバブルがまだ観測されていないため、表示するオブザベーションの詳細がないためです。

[オブザベーション（Observations）] セクション

デフォルトでは、[オブザベーション（Observations）] セクションには、次のような概要情報が表示されます。

- オブザベーションをトリガーしたオブザーバブルのタイプ（たとえば、[ドメイン（Domain）]）
- オブザーバブルを構成するデータ
- オブザベーションが最初のオブザベーションか、それ以降のオブザベーションか（たとえば、[最初の（1st）] または [3 つ目（3rd）]）

（注） 1 つのオブザーバブルが 3 回以上観測された場合、TID では最初と最後のオブザベーションの詳細を表示します。中間のオブザベーションの詳細は表示されません。

- オブザベーションの日時
- オブザーバブルに設定されているアクション

[オブザベーション（Observations）] セクションでオブザベーションにマウスオーバーすると、インジケータ パターンの関連するオブザーバブルが強調表示されます。

[オブザベーション（Observations）] セクションでオブザベーションをクリックした場合は、インジケータ パターンで関連するオブザーバブルが強調表示され、関連する最初のオブザーバブルがスクロールされて表示されます（複数のオブザーバブルが存在する場合）。また、オブザベーションをクリックすると、[オブザベーション（Observations）] セクションのオブザベーションの詳細が展開されます。

オブザベーションの詳細には、次のようなフィールドがあります。

表 6: オブザベーションの詳細のフィールド

フィールド	説明
[送信元（SOURCE）]	オブザベーションをトリガーしたトラフィックの送信元 IP アドレスおよびポート。
DESTINATION	オブザベーションをトリガーしたトラフィックの宛先 IP アドレスおよびポート。
[その他の情報（ADDITIONAL INFORMATION）]	オブザベーションをトリガーしたトラフィックに関連する DNS および認証情報。
イベント	このクリッカブル リンクは、オブザベーションによって接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントが生成された場合に表示されます。リンクをクリックして、Firepower Management Center イベント テーブルでイベントを表示します。接続イベントについてを参照してください。

TID オブザベーションのイベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

TID オブザベーションによって生成される Firepower Management Center イベントについて詳しくは、Firepower Management Center イベントでの TID オブザベーション （27 ページ） を参照してください。

TID 関連のイベントについてログに記録されるシステム アクションは、TID の相互作用やその他の Firepower Management Center 機能によって異なります。アクションの優先順位付けについて詳しくは、TID-Firepower Management Center のアクションの優先順位付け （27 ページ）を参照してください。

始める前に

- Cisco Threat Intelligence Director（TID） のセットアップ方法 （7 ページ）の説明に従って機能を設定します。

- TID をサポートするためのポリシーの設定 （8 ページ）の説明に従って、アクセス コントロール ポリシーで TID に必要なイベント ロギングを有効にしたことを確認します。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]** の順に選択します。

ステップ 2 インシデントの [インシデント ID（Incident ID）] 値をクリックします。

ステップ 3 [インジケータ（Indicator）] セクションでオブザベーションをクリックして、オブザベーション ボックスを表示します。

ステップ 4 オブザベーション ボックスの左上隅にある矢印をクリックしてボックスを展開します。

ステップ 5 オブザベーション情報で [イベント（Events）] リンクをクリックします。セキュリティ インテリジェンスの表示内容について詳しくは、接続イベントについてを参照してください。

Firepower Management Center イベントでの TID オブザベーション

アクセス コントロール ポリシーを完全に制御する場合、TID オブザベーションによって、次の Firepower Management Center イベントが生成されます。

表 *7:* オブザベーションによって生成される *Firepower Management Center* イベント

オブザベーションの内容	接続イベントの表	セキュリティ インテリジェンス イベントの表	ファイル イベントの表	マルウェア イベントの表
SHA-256	[はい（Yes）]	[いいえ（No）]	○	○（判定結果がマルウェアまたはカスタム検出の場合）。
[ドメイン名（Domain Name）]、[URL]、または [IPv4/IPv6]	○ TID 関連の接続イベントは、TID 関連の [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] 値によって識別されます。	○ TID 関連のセキュリティ インテリジェンス イベントは、TID 関連の [セキュリティ インテリジェンス イベント（Security Intelligence Category）] 値により識別されます。	[いいえ（No）]	[いいえ（No）]

TID-Firepower Management Center のアクションの優先順位付け

このセクションでは、複数の Firepower 機能を特定の 1 つのオブザーバブルに適用可能な場合のシステムの動作について説明します。たとえば、アクセス コントロール ポリシーでセキュ

リティインテリジェンスとTIDの両方を有効にした場合は、システムがトラフィックをセキュリティインテリジェンス基準でフィルタリングしてから、TID基準でフィルタリングします。

TID のオブザーバブル アクションが Firepower Management Center のポリシー アクションと競合する場合は、システムが次のようにアクションに優先順位を付けます。

表 *8 : TID URL* または *IPv4/IPv6* 監視可能アクション対セキュリティ インテリジェンス アクション

設定：セキュリティ インテリジェンス アクション	設定：**TID URL** または **IPv4/IPv6** 監視可能アクション	**TID** インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティ インテリジェンス カテゴリ（**Security Intelligence Category**）	理由（**Reason**）
WHITELIST	[モニタ（Monitor）] または [ブロック（Block）]	（インシデント生成なし）	許可（Allow）	（なし）	（なし）
ブロック（Block）	[モニタ（Monitor）] または [ブロック（Block）]	ブロック	ブロック（Block）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション	[IP ブロック（IP Block）] または [URL ブロック（URL Block）]
モニタ（Monitor）	モニタ（Monitor）	監視対象	許可（Allow）	システム分析により決定（を参照） セキュリティ インテリジェンス オプション	[IP モニタ（IP Monitor）] または [URL モニタ（URL Monitor）]
	ブロック（Block）	ブロック	ブロック（Block）	[TID IP ブロック（TID IP Block）] または [TID URL ブロック（TID URL Block）]	[IP ブロック（IP Block）] または [URL ブロック（URL Block）]

表 *9 : TID* ドメイン名の監視可能アクション対 *DNS* ポリシー アクション

設定：**DNS** ポリシー アクション	設定：**TID** ドメイン名の監視可能アクション	**TID**インシデント フィールド：実行されるアクション	セキュリティ インテリジェンス イベントのフィールド：		
			操作	セキュリティインテリジェンス カテゴリ（**Security Intelligence Category**）	理由（**Reason**）
WHITELIST	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	許可（Allow）	システム分析により決定（を参照）セキュリティインテリジェンス オプション	DNS モニタ（DNS Monitor）
モニタ（Monitor）	モニタ（Monitor）	監視対象	許可（Allow）	システム分析により決定（を参照）セキュリティインテリジェンス オプション	DNS モニタ（DNS Monitor）
	ブロック（Block）	ブロック	ブロック（Block）	TID ドメイン名ブロック	DNS ブロック（DNS Block）
[ドロップ（Drop）]、[見つからないドメイン（Domain Not Found）]、[Sinkhole—ログ（Sinkhole—Log）]、または [Sinkhole—ブロックおよびログ（Sinkhole—Block and Log）]	モニタ（Monitor）	ブロック	ブロック（Block）	システム分析により決定（を参照）セキュリティインテリジェンス オプション	DNS ブロック（DNS Block）
	ブロック（Block）			TID ドメイン名ブロック	

表 *10 : TID SHA-256* 監視可能アクション対マルウェア クラウド ルックアップ ファイル ポリシー

ファイル傾向（**File Disposition**）	**TID SHA-256** 監視可能アクション	**TID** インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
クリーン（Clean）	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
マルウェア	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外

ファイル傾向（File Disposition）	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
カスタム（Custom）	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。	• SHA-256 がカスタム検出リストにない場合は、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）]。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出（Custom Detection）]。
不明	[モニタ（Monitor）] または [ブロック（Block）]	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外

（注） TID の一致は、システムが動的分析用にファイルを送信する前に発生します。

表 *11 : TID SHA-256* 監視可能アクション対マルウェア ブロック ファイル ポリシー

ファイル傾向（File Disposition）	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[正常（Clean）] または [不明（Unknown）]	モニタ（Monitor）	監視対象	マルウェア クラウド ルックアップ（Malware Cloud Lookup）	適用対象外
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

ファイル傾向（File Disposition）	TID SHA-256 監視可能アクション	TID インシデントで行われるアクション	ファイルイベントでのアクション	マルウェアイベントでのアクション
[マルウェア（Malware）] または [カスタム（Custom）]	モニタ（Monitor）	ブロック	マルウェア ブロック（Block Malware）	マルウェア ブロック（Block Malware）
	ブロック（Block）	ブロック	• SHA-256 がカスタム検出リストにない場合は、[TID ブロック（TID Block）]。 変更されたファイル性質は [カスタム（Custom）] です。 • SHA-256 がカスタム検出リストにある場合は、[カスタム検出ブロック（Custom Detection Block）]。	TID ブロック（TID Block） 変更されたファイル性質は [カスタム（Custom）] です。

アクションに影響を与える要因

システムがアクションを取るタイミングや、TID オブザーバブルと一致するトラフィックを検出したときにシステムが取るアクションは多くの要因によって決定されます。

- セキュリティインテリジェンスのような機能は、TID がアクションを起こす前にアクションを起こします。詳細は、TID-Firepower Management Center のアクションの優先順位付け（27 ページ）を参照してください。
- 実行されるアクションは一般に、オブザーバブルに対して構成されたアクション（親インジケータまたはソースに対して構成されたアクションとは異なる可能性がある）となります。
- STIX ソースには複雑なインジケータが含まれている可能性があるため、ソースのアクション設定は [モニタ（Monitor）] にのみ設定できます。ただし、STIX フィードまたはファイルに含まれている個々の簡易インジケータまたはオブザーバブルは [ブロック（Block）] に設定できます。
- インジケータおよびオブザーバブルのアクション設定は、継承するかまたは継承をオーバーライドするように個別に設定できます。TID 設定における継承 （44 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。

- それ以外の場合、アクション可能なトラフィックはホワイトリストに登録される可能性があります。詳細は、TID オブザーバブルのホワイトリスト登録 （51 ページ）を参照してください。
- 設定されたアクションは、部分的および完全に実現されたインシデントの両方に対して実行されます。
- 複雑なインジケータに基づくインシデントは部分的にブロックできます。これは、インジケータにモニタ対象のオブザーバブルとブロックされたオブザーバブルの両方が含まれている場合に発生する可能性があります。
- 公開の一時停止は、システムが実行するアクションに影響します。公開の一時停止について （47 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。
- TID機能を一時停止すると、すべての操作ができなくなります。この機能を再開した後、実行可能なデータが以前と異なる場合があります。詳細は、TID の一時停止と要素からの TID データの消去 （48 ページ）を参照してください。

Cisco Threat Intelligence Director（TID） 設定の表示および変更

必要に応じて、次の情報を使用して設定を見直し、微調整します。

要素（管理対象デバイス）の TID ステータスの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

管理対象デバイスとして Firepower Management Center に登録されているすべてのデバイスは、[要素（Elements）] ページに自動的に表示されます。すべての（TID をサポートするためのポリシーの設定 （8 ページ） で指定されたとおりに）適切に構成された要素は、要素が追加される前に取り込まれたものを含めて、現在公開されているすべてのオブザーバブルを受信します。

手順

ステップ 1 **[インテリジェンス（Intelligence）]** > **[要素（Elements）]** を選択します。

ステップ 2 設定した要素を確認します。

- [名前（Name）] の横にあるアイコンは、その要素が接続されて TID が有効になっているかどうかを示します。
- TID が有効化されてこのデバイスに展開されたときのアクセス コントロール ポリシーを確認するには、[アクセス コントロール ポリシー（Access Control Policy）] 列を調べます。詳細については、TID をサポートするためのポリシーの設定 （8 ページ）を参照してください。

ソースの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

[ソース（Sources）]ページには、設定済みのすべてのソースに関する概要情報が表示されます（ソース サマリー情報 （35 ページ）を参照）。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 ソースを次のように表示します。

- ページに表示されるソースをフィルタリングするには、[フィルタ（Filter）]アイコン（🔍）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （43 ページ）を参照してください。
- 詳細な取り込みステータスを表示するには、[ステータス（Status）] 列のテキストの上にカーソルを移動します。詳細については、ソース ステータスの詳細 （36 ページ）を参照してください。

ステップ 3 ソースを次のように管理します。

- [アクション（Action）] 設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。固定されているアクションがある場合、ソースの[タイプ（Type）]には、そのアクションだけがサポートされます。

- [公開（Publish）] 設定を編集するには、スライダ（）をクリックします。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。
- TID によるソースの更新を一時停止または再開する場合は、[更新の一時停止（Pause Updates）] または [更新の再開（Resume Updates）] をクリックします。更新を一時停止すると、更新は中断されますが、既存のインジケータとオブザーバブルは TID 内に残ります。
- ソースを削除するには、削除アイコン（）をクリックします。ソースが現在処理中の場合、このアイコンはグレー表示になります。ソースを削除すると、そのソースに関連付けられているすべてのインジケータも削除されます。関連付けられているオブザーバブルも削除される可能性があります。ただし、システム内に残っているインジケータに関連付けられたオブザーバブルは保持されます。

ソース サマリー情報

[ソース（Sources）]ページには、設定されているすべてのソースの概要情報が表示されます。次の表で、概要表示に含まれるフィールドについて簡単に説明します。これらのフィールドの詳細については、ソースの関連設定トピックの説明を参照してください。データ ソースを取り込むためのオプション （9 ページ） を参照してください。

表 *12:* ソース サマリー情報

フィールド	説明
[名前（Name）]	ソース名。
タイプ（Type）	ソースのデータ形式（[STIX] または [フラットファイル（Flat File）]）。
配信	TID がソースを取得するのに使用する手法。
操作（Action）	このソースに含まれるデータと一致するトラフィックに対してシステムで実行するように設定されているアクション（[ブロック（Block）] または [モニタ（Monitor）]）。 可用性、継承、および継承のオーバーライドを含む TID のアクションの詳細については、アクションに影響を与える要因 （32 ページ） を参照してください。
パブリッシュ	[オン（On）] または [オフ（Off）] トグル。登録されている要素（TID をサポートするために設定された管理対象デバイス）に TID がソースからのデータを公開するかどうかを指定します。 インジケータは親ソースから [公開（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [公開（Publish）] 設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。
最終更新日	TID が最後にソースを更新した日時。

フィールド	説明
ステータス	ソースの現在のステータス。 • [新規（New）]：ソースは新規に作成されます。 • [スケジュール済み（Scheduled）]：初回のダウンロードまたはその後の更新がスケジュールされていますが、まだ進行中ではありません。 • [ダウンロード 中（Downloading）]：TID が初回のダウンロードまたは更新を処理中です。 • [解析中（Parsing）] または [処理中（Processing）]（）：TID がソースを取り込んでいます。 • [完了（Completed）]（）：TID はソースの取り込みを終了しました。 • [完了（エラーあり）（Completed with Errors）]（）：TID はソースの取り込みを終了しましたが、一部のオブザーバブルがサポートされていないか無効です。 • [エラー（Error）]（）：TID による処理にエラーが発生しました。[更新間隔（Update Frequency）] が指定された TAXII ソースまたは URL ソースの場合、更新が一時停止でなければ、 TID はスケジュールされている次回の更新で再試行します。 ページを更新してステータスを更新します。
	このアイコンをクリックすると、ソースの設定を編集できます。
	このアイコンをクリックすると、ソースが完全に削除されます。

ソース ステータスの詳細

ソースの概要ページに表示されるソースの [ステータス（Status）] 値にマウスオーバーすると、TID は次の詳細情報を表示します。

データ	説明
ステータス メッセージ	ソースの現在のステータスを簡単に説明します。
最終更新日（Last Updated）	TID が最後にソースを更新した日時を表示します。
次回更新日（Next Update）	TAXII および URL ソースの場合、この値は TID が次にソースを更新する時期を指定します。

データ	説明
インジケータ（Indicators）	インジケータ カウントを表示します。 • [使用済み（Consumed）]：最近のソース更新中に TID が処理したインジケータの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのインジケータを表します。 • [破棄済み（Discarded）]：最近の更新でシステムが TID に追加しなかった無効なインジケータの数。 （注） `TAXII` ソースの場合、 TID は [最終更新（Last Update）] と [合計（Total）] とに分けてインジケータ数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのインジケータの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、TID は [最終更新（Last Update）] の値のみを表示します。 あるインジケータのオブザーバブルがすべて [無効（Invalid）] の場合、 TID はそのインジケータを破棄します。
オブザーバブル（Observables）	オブザーバブルの数を表示します。 • [使用済み（Consumed）]：最近のソース更新中に TID が処理したオブザーバブルの数。この数値は、取り込みや破棄が行われたかどうかに関係なく、その更新に含まれていたすべてのオブザーバブルを表します。 • [サポート対象外（Unsupported）]：最近の更新でシステムが TID に追加しなかったサポートされないオブザーバブルの数。 サポートされているオブザーバブルのタイプに関する詳細については、ソース要件 （5 ページ） でコンテンツ タイプに関する情報を参照してください。 • [無効（Invalid）]：最近の更新でシステムが TID に追加しなかった無効なオブザーバブルの数。 オブザーバブルが正しく作成されていない場合は無効になります。たとえば、`10.10.10.10.123` は有効な IPv4 アドレスではありません。 （注） `TAXII` ソースの場合、 TID は [最終更新（Last Update）] と [合計（Total）] とに分けてオブザーバブル数を表示します。これは、TAXII の場合、既存のデータを置換する形式ではなく、増分データを追加する形式で更新が行われるからです。他のソース タイプのオブザーバブルの場合、これらのソースの更新では既存のデータ セットが完全に置換されるので、TID は [最終更新（Last Update）] の値のみを表示します。

インジケータの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

インジケータは、取り込まれたソースから自動的に生成されます。このページの詳細については、インジケータ サマリー情報 （39 ページ） を参照してください。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 [インジケータ（Indicators）] をクリックします。

ステップ 3 現在のインジケータを次のように表示します。

- ページに表示されるインジケータをフィルタリングするには、[フィルタ（Filter）]アイコン（🔍）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （43 ページ）を参照してください。
- インジケータの詳細情報（関連付けられているオブザーバブルなど）を表示するには、インジケータ名をクリックします。詳細については、インジケータの詳細 （40 ページ）を参照してください。
- インジケータに関連付けられているインシデントについての情報を表示するには、[インシデント（Incidents）]列内の番号をクリックします。また、アイコンの上にカーソルを移動すると、インシデントが完全に実現されたか、部分的に実現されたかを確認できます。
- ソースからのインジケータの調査が TID で完了したかどうかを判別するには、[ステータス（Status）] 列を確認します。

ステップ 4 現在のインジケータを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。固定されているアクションがある場合、ソースの[タイプ（Type）]には、そのアクションだけがサポートされます。
- [公開（Publish）]設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。
- インジケータの 1 つ以上のオブザーバブルをホワイトリストに入れるには、インジケータ名をクリックして [インジケータの詳細（Indicator Details）] ページにアクセスします。詳

細については、TID オブザーバブルのホワイトリスト登録について （50 ページ）を参照してください。

インジケータ サマリー情報

[インジケータ（Indicators）]ページには、設定されたソースに関連付けられているすべてのインジケータの概要情報が表示されます。

表 *13*：インジケータ サマリー情報

フィールド	説明
タイプ（Type）	• 1 つオブザーバブルを持つインジケータには、そのオブザーバブルのデータ タイプがリストされます（URL、SHA-256 など）。 • 2 つ以上のオブザーバブルを持つインジケータは、[複合（Complex）] としてリストされます。 特定のオブザーバブルを確認するには、タイプの上にカーソルを移動します。
[名前（Name）]	インジケータ名。
ソース（Source）	インジケータが含まれていたソース（親ソース）。
[インシデント（Incidents）]	インジケータに関連付けられたすべてのインシデントに関する情報。 • インシデントが部分的に実現（）されるか、完全に実現（）されるかを指定するアイコン。 • インジケータに関連付けられたインシデント数。
操作（Action）	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。 インジケータは親ソースから[アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。 インジケータは親ソースから[公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから[公開（Publish）]設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。

フィールド	説明
最終更新日	TID が最後にインジケータを更新した日時。
ステータス	インジケータの現在のステータス。 • [保留中（Pending）]（）：TID はインジケータのオブザーバブルを取り込み中です。 • [完了（Completed）]（）：TID はインジケータのオブザーバブルをすべて正常に取り込みました。 • [完了（エラーあり）（Completed With Errors）]（）：TID はインジケータを取り込みましたが、一部のオブザーバブルがサポートされていないか無効です。

インジケータの詳細

[インジケーターの詳細（Indicator Details）] ページには、インシデントのインジケータとオブザーバブル（監視可能）データが表示されます。

表 *14*：インジケータの詳細情報

フィールド	説明
[名前（Name）]	インジケータ名。
説明	ソースから提供されたインジケータの説明。
ソース（Source）	このインジケータを含んでいたソース。
有効期限	ソースの [TTL] 値に基づく、インジケータが期限切れになる日時。
[操作（Action）]	インジケータに関連付けられたアクション。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。 インジケータは親ソースから [アクション（Action）] 設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。
パブリッシュ	インジケータのパブリッシュ設定。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。 インジケータは親ソースから [パブリッシュ（Publish）] 設定を継承でき、オブザーバブルは親インジケータから [パブリッシュ（Publish）] 設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。

フィールド	説明
インジケータのパターン（Indicator Pattern）	インジケーターのパターンを形成するオブザーバブルと演算子。演算子はインジケーター内のオブザーバブルをリンクします。AND 関係は [AND] 演算子で示されます。OR 関係は、[OR] 演算子で示されるか、いくつかのオブザーバブルの密接なグループ化により示されます。 必要に応じて、ホワイトリスト アイコン（）をクリックし、オブザーバブルをホワイトリストに入れます。詳細については、TID オブザーバブルのホワイトリスト登録について （50 ページ）を参照してください。

オブザーバブルの表示と管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

[オブザーバブル（Observables）] ページには、正常に取り込まれたすべてのオブザーバブルが表示されます（オブザーバブル サマリー情報 （42 ページ）を参照）。

始める前に

- ソースとして使用する TAXII フィードの取得 （10 ページ）、URL からのソースの取得 （12 ページ）、またはソースとして使用するローカル ファイルのアップロード （13 ページ）の説明に従って 1 つ以上のソースを設定します。

手順

ステップ 1 **[インテリジェンス（Intelligence）] > [ソース（Sources）]** の順に選択します。

ステップ 2 [オブザーバブル（Observables）] をクリックします。

ステップ 3 現在のオブザーバブルを次のように表示します。

- ページに表示されるオブザーバブルをフィルタリングするには、[フィルタ（Filter）] アイコン（）をクリックします。詳細については、テーブル ビューでの TID データのフィルタ処理 （43 ページ）を参照してください。
- [値（Value）] 列の情報が途切れている場合は、値の上にカーソルを移動します。
- そのオブザーバブルを含むインジケータを表示するには、[インジケータ（Indicators）] 列内の番号をクリックします。[インシデント（Incidents）] ページが開き、オブザーバブルの値がフィルタとして適用されます。詳細については、インジケータの表示と管理 （38 ページ）を参照してください。

ステップ 4 現在のオブザーバブルを次のように管理します。

- [アクション（Action）] を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。
- オブザーバブルの[公開（Publish）]設定を編集するには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。
- オブザーバブルの有効期限を変更するには、親ソースの[TTL]を変更します。詳細については、ソースの表示と管理 （34 ページ）を参照してください。
- オブザーバブルをホワイトリストに入れるには、[ホワイトリスト（Whitelist）] アイコン（）をクリックします。詳細については、TID オブザーバブルのホワイトリスト登録について （50 ページ）を参照してください。

オブザーバブル サマリー情報

[オブザーバブル（Observables）]ページには、取り込まれたすべてのオブザーバブルの概要情報が表示されます。

表 *15*：オブザーバブル サマリー情報

フィールド	説明
タイプ（Type）	オブザーバブル（監視可能）データのタイプ：`SHA-256`、`Domain`、`URL`、`IPv4`、または `IPv6`。
値	オブザーバブルを構成するデータ。
インジケータ（Indicators）	オブザーバブルを含む親インジケータの数。
操作（Action）	オブザーバブルに対して設定されている操作。詳細については、ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）を参照してください。 インジケータは親ソースから[アクション（Action）]設定を継承でき、オブザーバブルは親インジケータから [アクション（Action）] 設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。
パブリッシュ	オブザーバブルのパブリッシュ設定（ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照）。 インジケータは親ソースから[公開（Publish）]設定を継承でき、オブザーバブルは親インジケータから[公開（Publish）]設定を継承できます。詳細については、TID 設定における継承 （44 ページ）を参照してください。

フィールド	説明
更新時刻（Updated At）	TID が最後にオブザーバブルを更新した日時。
有効期限	親インジケータの [TTL] に基づいて、オブザーバブルが TID から自動的に消去される日付。
	このアイコンをクリックすると、オブザーバブルがホワイトリストに入ります（TID オブザーバブルのホワイトリスト登録について（50 ページ）を参照）。

テーブル ビューでの TID データのフィルタ処理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

手順

ステップ 1 次のいずれかの TID テーブル ビューを選択します。

- **[インテリジェンス（Intelligence）] > [インシデント（Incidents）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [オブザーバブル（Observables）]**

ステップ 2 フィルタ アイコン（🔍）をクリックし、フィルタ属性を選択します。

ステップ 3 そのフィルタ属性の値を選択または入力します。

フィルタでは大文字/小文字が区別されます。

ステップ 4 （オプション）複数の属性でフィルタリングするには、フィルタ アイコン（🔍）をクリックし、手順 2 と手順 3 を繰り返します。

ステップ 5 前回フィルタを適用してから行った変更を取り消すには、[キャンセル（Cancel）] をクリックします。

ステップ 6 フィルタを適用してテーブルを更新するには、[適用（Apply）] をクリックします。

ステップ 7 フィルタ属性を個別に削除するには、フィルタ属性の横にある削除アイコン（✕）をクリックし、[適用（Apply）] をクリックしてテーブルを更新します。

TID 設定における継承

TIDはソースからインテリジェンスデータを取り込むと、そのソースの子オブジェクトとしてインジケータとオブザーバブルを作成します。作成時に、これらの子オブジェクトは、親設定から [アクション（Action）] および [公開（Publish）] 設定を継承します。

インジケータは、親ソースからこれらの設定を継承します。インジケータは、親ソースを1つしか持てません。

オブザーバブルは、親インジケータからこれらの設定を継承します。オブザーバブルは、複数の親インジケータを持つことができます。

詳細については、以下を参照してください。

- 複数の親からの TID 設定の継承 （44 ページ）
- 継承された TID 設定の上書きについて （45 ページ）

複数の親からの TID 設定の継承

オブザーバブルに複数の親インジケータがある場合、システムはすべての親から継承した設定を比較し、オブザーバブルに最もセキュアなオプションを割り当てます。つまり、

- [アクション（Action）] : [ブロック（Block）] は [モニタ（Monitor）] よりもセキュアです。
- [公開（Publish）] : [オン（On）] は [オフ（Off）] よりもセキュアです。

たとえば、SourceA は IndicatorA と関連する ObservableA に関与する可能性があります。

設定	SourceA	IndicatorA	ObservableA
操作（Action）	ブロック（Block）	ブロック（Block）	ブロック（Block）
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）

SourceB が後で ObservableA を含む IndicatorB に関与する場合、システムは ObservableA を次のように変更します。

設定	SourceB	IndicatorB	ObservableA
操作（Action）	モニタ（Monitor）	モニタ（Monitor）	[ブロック（Block）]（IndicatorA から継承）

設定	SourceB	IndicatorB	ObservableA
パブリッシュ	オン	オン	[オン（On）]（IndicatorB から継承）

この例では、ObservableA には 2 つの親があります。1 つは [アクション（Action）] 設定の親で、もう 1 つは [公開（Publish）] 設定の親です。オブザーバブルの設定を手動で編集してから設定を元に戻した場合、[アクション（Action）] 設定が IndicatorA 値に設定され、[公開（Publish）] 設定が IndicatorB 値に設定されます。

継承された TID 設定の上書きについて

継承された設定を上書きするには、子レベルで設定を変更します。ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集 （46 ページ）およびソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。継承された設定を上書きすると、親オブジェクトに変更にかかわらず、子オブジェクトではその設定が保持されます。

たとえば、上書きを設定せずに、次の元の設定で開始するとします。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オフ（Off）	オフ（Off）	オフ（Off）

IndicatorA の設定を上書きした場合、設定は次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン	オン	オン

この場合、SourceA の [公開（Publish）] 設定への変更は、IndicatorA に自動的にはカスケードされなくなります。ただし、オブザーバブルの設定は現在値を上書きするようには設定されていないため、IndicatorA から ObservableA1 および ObservableA2 への継承は続行されます。

後から ObservableA1 の設定を上書きする場合は、次のようになります。

設定	SourceA	IndicatorA	ObservableA1	ObservableA2
パブリッシュ	オフ（Off）	オン	オフ（Off）	オン

IndicatorA の [公開（Publish）] 設定への変更は、ObservableA1 に自動的にはカスケードされなくなります。ただし、ObservableA2 は上書き値には設定されていないため、これらの変更は引き続き ObservableA2 にカスケードされます。

オブザーバブル レベルでは、上書き設定から継承された設定に戻すことができ、システムは、親インジケータからそのオブザーバブルへの設定変更のカスケードを自動的に再開します。

ソース、インジケータ、またはオブザーバブル レベルでの TID アクションの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

（注）

- 親のアクションを編集すると、すべての子に対しアクションが設定されます。ソース レベルでアクションを編集すると、そのすべてのインジケータにアクションが設定されます。インジケータ レベルでアクションを編集すると、そのオブザーバブルのすべてに対してアクションが設定されます。
- 子のアクションを編集すると、継承が中断されます。インジケータ レベルでアクションを編集し、続いてソース レベルで編集すると、個々のインジケータのアクションを編集するまで、インジケータのアクションが保持されます。監視可能レベルでアクションを編集し、続いてインジケータ レベルで編集すると、個々のオブザーバブルのアクションを編集するまで、オブザーバブルのアクションが保持されます。監視可能レベルでは、親インジケータのアクションに自動的に復元できます。継承の詳細については、TID設定における継承 （44 ページ）を参照してください。

他の アクションに影響を与える要因 （32 ページ） を確認することもできます。

手順

ステップ 1 次のいずれかを選択します。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**

  （注） TID は、ソース レベルでの TAXII ソースのブロックをサポートしていません。TAXII ソースに簡易インジケータが含まれている場合、インジケータ レベルまたは監視可能レベルでブロックすることができます。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ （Indicators）]**

  （注） TIDは、複雑なインジケータのブロックをサポートしていません。代わりに、複雑なインジケータ内で個々のオブザーバブルをブロックします。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [オブザーバブル（Observables）]**

ステップ 2 [アクション（Action）] ドロップダウンを使用して、[モニタ（Monitor）]（）または [ブロック（Block）]（）を選択します。

ステップ 3 （オブザーバブルのみ）親インジケータからアクション設定を継承し直すには、オブザーバブルの [アクション（Action）] 設定の横にある復元アイコン（）をクリックします。

公開の一時停止について

- 機能レベルで公開を一時停止すると、要素に保存されているすべての TID オブザーバブルが消去されます。つまり、TID は脅威を検出、監視、ブロックすることはできません。システム上の他のセキュリティ機能は影響を受けません。
- ソース、インジケータ、またはオブザーバブル レベルで公開を一時停止すると、システムは一時停止された TID オブザーバブルを要素から削除し、トラフィックと一致しないようにします。
- 親のパブリケーションを一時停止すると、すべての子が一時停止します。ソース レベルで公開を一時停止すると、そのすべてのインジケータの公開が一時停止されます。インジケータ レベルで公開を一時停止すると、そのすべてのオブザーバブルの公開が一時停止されます。
- 子のパブリケーションを一時停止すると、継承が中断されます。インジケータ レベルで公開を一時停止し、その後にソース レベルで公開すると、インジケータの個別設定を変更するまで、インジケータの公開は一時停止されたままになります。監視可能レベルで公開を一時停止し、その後にインジケータ レベルで公開すると、オブザーバブルの個別設定を変更するまで、オブザーバブルの公開は一時停止されたままになります。監視可能レベルでは、親インジケータの公開ステータスに自動的に復元できます。継承の詳細については、TID 設定における継承 （44 ページ）を参照してください。
- アップロードされたソースの公開は、インジケータ レベルでのみ一時停止することができます。
- オブザーバブルのホワイトリスト化と公開の一時停止の比較については、TID オブザーバブルのホワイトリスト登録について （50 ページ） を参照してください。
- 個々のオブザーバブルまたはインジケータに対して公開または一時停止の設定を指定した場合、更新プログラムに同じオブザーバブルまたはインジケータが含まれている場合、ソースの更新によってその設定が変わることはありません。
- オブジェクト管理ページで公開を無効にすることができます。オブザーバブルのパブリケーション頻度の変更 （50 ページ）を参照してください。
- 更新を一時停止する [ソース（Sources）] ページ上のオプションは、要素へのデータの公開には関連しません。フィードから Firepower Management Center 上のソースを更新する場合に適用されます。

TID の一時停止と要素からの TID データの消去

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

注意 この設定により、すべての要素への公開が一時停止され、要素に保存されたすべてのTIDオブザーバブルが消去され、TID 機能を使用したトラフィックの検査が停止されます。

より細かいレベルでオブザーバブルを無効にするには、ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ） を参照してください。

管理センター上のデータ（既存のインシデントと設定済みのソース、インジケータ、オブザーバブル、およびソースの取り込み）は、この設定の影響を受けません。

手順

ステップ 1 **[インテリジェンス（Intelligence）]** > **[設定（Settings）]** の順に選択します。

ステップ 2 [一時停止（Pause）] をクリックします。

次のタスク

要素へのTIDデータの同期とオブザベーションの生成を再開する準備ができたら、このページから手動で公開を [再開（Resume）] します。管理センター上の既存のオブザーバブルがすべての要素に公開されます。

ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

ソース レベルで公開が有効になっている場合、システムは最初のソース データとそれに続く以下のような変更を自動的に公開します。

- 定期的なソースの更新からの変更
- システム アクションに起因する変更（**TTL** の有効期限など）
- ユーザが開始した変更（インジケータやオブザーバブルの [アクション（Action）] 設定の変更など）

（注） デバイス（要素）から一度にすべての TID オブザーバブルを消去するには、TID の一時停止と要素からの TID データの消去 （48 ページ） を参照してください。

始める前に

公開を一時停止する前に、公開の一時停止について （47 ページ） に記載されている影響を把握してください。

手順

ステップ 1 次のいずれかを選択します。

- **[インテリジェンス（Intelligence）] > [ソース（Sources）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [インジケータ（Indicators）]**
- **[インテリジェンス（Intelligence）] > [ソース（Sources）] > [オブザーバブル（Observables）]**

ステップ 2 [公開（Publish）] スライダ（）を検索して、要素への公開を切り替えるために使用します。

ステップ 3 （オブザーバブルのみ）親インジケータからパブリケーション設定を継承し直す場合は、オブザーバブルの [公開（Publish）] 設定の横にある復元アイコン（）をクリックします。

次のタスク

- 要素が変更を受け取るまで少なくとも 10 分間待機します。大規模なソースが含まれる変更には時間がかかります。
- （オプション）オブザーバブル レベルで TID データのパブリケーション頻度を変更します。オブザーバブルのパブリケーション頻度の変更 （50 ページ） を参照してください。

オブザーバブルのパブリケーション頻度の変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

デフォルトでは、監視可能データ（オブザーバブル）がTID要素に5分ごとに公開されます。この間隔を別の値に設定するには、次の手順を実行します。

始める前に

- 監視可能レベルでTIDデータのパブリケーションを有効にします。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。

手順

ステップ1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。

ステップ2 **[セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク フィードとリスト（Network Feeds and Lists）]** を選択します。

ステップ3 [Cisco-TID フィード（Cisco-TID-Feed）] の横にある編集アイコンをクリックします。

ステップ4 [更新間隔:（Update Frequency）] ドロップダウンリストから値を選択します。

- 監視可能なデータの要素への公開を停止するには、[無効（Disable）] を選択します。
- その他の値を選択して、監視可能なパブリケーションの間隔を設定します。

ステップ5 [保存（Save）] をクリックします。

TID オブザーバブルのホワイトリスト登録について

指定された [アクション（Action）] から簡易インジケータ内の1つのオブザーバブルを除外する（モニタリング/ブロッキングなしでトラフィックを通過させる）には、オブザーバブルをホワイトリストに入れることができます。

複雑なインジケータでは、TIDはトラフィックを評価するときにホワイトリスト登録されたオブザーバブルを無視しますが、そのインジケータ内の他のオブザーバブルは引き続き評価されます。たとえば、インジケータにAND演算子でリンクされているオブザーバブル1とオブザーバブル2が含まれていて、オブザーバブル1をホワイトリストに入れると、TIDはオブザーバブル2が認識されたときに完全に実現されたインシデントを生成します。

これに対して、同じ複雑なインジケータで、オブザーバブル 1 をホワイトリスト登録するのではなく、その公開を無効にすると、TID はオブザーバブル 2 が認識されたときに部分的に実現されたインシデントを生成します。

（注） オブザーバブルをホワイトリストに追加する場合、オブザーバブルの設定が継承されるか上書き値であるかにかかわらず、ホワイトリストが常に [アクション（Action）] 設定より優先されます。

更新プログラムに同じオブザーバブルが含まれている場合、ソースの更新は個々のオブザーバブルのホワイトリスト設定に影響しません。

TID オブザーバブルのホワイトリスト登録

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	グローバル	管理/Threat Intelligence Director（□ID）ユーザ

ホワイトリスト登録の詳細については、TID オブザーバブルのホワイトリスト登録について（50 ページ） を参照してください。

ヒント ホワイトリストのアイコン（）は、Web インターフェイスの複数の場所に表示できます。アイコンをクリックすることで、それらの場所のいずれかでオブザーバブルをホワイトリストに登録することができます。

手順

ステップ 1 [インテリジェンス（Intelligence）]>[ソース（Sources）]>[オブザーバブル（Observables）] をクリックします。

ステップ 2 無視するオブザーバブルに移動します。

ステップ 3 そのオブザーバブルのホワイトリストのアイコン（）をクリックします。

次のタスク

（オプション）ホワイトリストからオブザーバブルを削除する必要がある場合は、アイコンをもう一度クリックします。

STIX ソース ファイルの表示

手順

ステップ 1 [インテリジェンス（Intelligence）]>[ソース（Sources）]>[インジケータ（Indicators）] を選択します。

ステップ 2 インジケータ名をクリックします。

ステップ 3 [STIXのダウンロード（Download STIX）] をクリックします。

ステップ 4 テキスト エディタでこのファイルを開きます。

Cisco Threat Intelligence Director（TID）のトラブルシューティング

以下のセクションでは、TIDの一般的な問題について、可能な解決策と軽減策を説明します。

フラット ファイル ソースを取得またはアップロードするとエラーが発生する

システムがフラットファイル ソースを取得またはアップロードできない場合は、フラットファイル内のデータが [インテリジェンス（Intelligence）] > [ソース（Sources）] ページの [タイプ（Type）] 列と一致することを確認してください。

TAXII または URL のソース アップデートでエラーが発生する

TAXII またはURL のソース アップデートでソース ステータス エラーが発生した場合は、サーバ証明書の期限が切れていないことを確認してください。証明書の有効期限が切れている場合は、新しい**サーバ証明書**を入力するか、または既存の**サーバ証明書**を削除して、TIDが新しい証明書を取得できるようにします。詳細については、TID ソースの SSL 設定の構成 （15 ページ）を参照してください。

インジケータまたはソースに対して「ブロック」アクションは使用できず、「モニタ」アクションのみを使用できます。

インジケータまたはソースの個々のオブザーバブルのアクションを変更できます。

TID テーブル ビューで「結果なし」と表示される

テーブル ビューには、[ソース（Sources）]、[インジケータ（Indicators）]、[オブザーバブル（Observables）]、および [インシデント（Incidents）] ページが含まれます。

いずれかの TID テーブル ビューにデータが表示されない場合：

- テーブル フィルタを確認し、[最終更新日（Last Updated）] フィルタ属性の時間枠を拡大することを検討します（テーブル ビューでの TID データのフィルタ処理 （43 ページ）を参照）。
- ソースが正しく設定されていることを確認します（データ ソースを取り込むためのオプション （9 ページ）を参照）。
- TIDをサポートするのに必要なアクセス コントロール ポリシー、および関連するポリシーが設定されていることを確認します（TID をサポートするためのポリシーの設定 （8 ページ）を参照）。たとえば、SHA 256 オブザーバブルがオブザベーションを生成していない場合、展開されているアクセス コントロール ポリシーに、[マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイル ポリシーを呼び出すアクセス制御ルールが 1 つ以上含まれていることを確認します。
- TID をサポートするアクセス コントロール ポリシーおよび関連するポリシーが要素に展開されていることを確認します（設定変更の展開を参照）。
- 機能レベルでTIDデータ パブリケーションを一時停止していないことを確認します（TID の一時停止と要素からの TID データの消去 （48 ページ）を参照）。

システムが低速またはパフォーマンス低下を起こしている

パフォーマンスの影響の詳細については、Threat Intelligence Director のパフォーマンスへの影響 （4 ページ） を参照してください。

Firepower Management Center テーブル ビューに TID データが表示されない

オブザーバブルを要素に公開しても、接続、セキュリティ インテリジェンス、ファイル、またはマルウェア イベントのテーブルに TID データが表示されない場合は、要素に展開されたアクセス コントロール ポリシーとファイル ポリシーを確認してください。詳細については、TID をサポートするためのポリシーの設定 （8 ページ）を参照してください。

1 つまたは複数の要素が TID データによって圧倒される

TID データが 1 つまたは複数のデバイスを圧倒している場合は、TID による要素に保存されているデータの公開と消去を一時停止することを検討してください。詳細については、TID の一時停止と要素からの TID データの消去 （48 ページ）を参照してください。

システムが TID ブロックの代わりにマルウェア クラウド ルックアップを実行している

これは設計によるものです。詳細については、TID-Firepower Management Center のアクションの優先順位付け （27 ページ）を参照してください。

システムが TID アクションではなく、セキュリティ インテリジェンスまたは DNS ポリシー アクションを実行している

これは設計によるものです。詳細については、TID-Firepower Management Center のアクションの優先順位付け （27 ページ）を参照してください。

TID が無効化されている

- アプライアンスにメモリを追加します。Threat Intelligence Director を使用するには、少なくとも 15 GB のメモリをアプライアンスに搭載する必要があります。
- Firepower Management Center の REST API アクセスを有効化します。詳細については、REST API アクセスの有効化を参照してください。

システムが TID インシデントを生成しないか、または予期される TID アクションを実行しない

- すべての管理対象デバイスが TID に対し適切に有効になっており、設定されていることを確認します。要素（管理対象デバイス）の TID ステータスの表示 （33 ページ）および TID をサポートするためのポリシーの設定 （8 ページ）を参照してください。
- 変更内容が要素に公開されるまでには少なくとも 5 ～ 10 分かかり、大規模なデータ フィードを公開する場合は、かかる時間がそれよりも著しく長くなります。
- オブザーバブルに対するアクション設定を確認します。オブザーバブルの表示と管理 （41 ページ）を参照してください。
- システムが実行する TID アクションに影響を与える他の要因のリストについては、アクションに影響を与える要因 （32 ページ） を参照してください。
- 要素（管理対象デバイス）に、予想していた脅威データが含まれていない可能性があります。公開の一時停止について （47 ページ）を参照してください。

特定の脅威との一度の遭遇によって、複数のインシデントが生成される

これは、単一のインジケータが複数のソースに含まれている場合に発生します。

- フラット ファイル ソースからのインジケータ：インジケータの各インスタンスがインシデントを生成するため、特定の脅威を一度検出すると複数のインシデントを生成する場合があります。
- STIX ソースからのインジケータ：異なる STIX ソースからのインジケータが同じ ID を共有している場合、含んでいるソースの数にかかわらず、そのインジケータに対して 1 つのインシデントのみが生成されます。

今後の重複インシデントを回避するには、重複インジケータの 1 つを除くすべてのインジケータの公開を一時停止します。ソース、インジケータ、またはオブザーバブル レベルでの TID データの一時停止または公開 （48 ページ）を参照してください。