



接続ロギング

次のトピックでは、モニタ対象ネットワークでホストから実行される接続を記録するよう Firepower システムを設定する方法について説明します。

- [接続ロギングについて, 1 ページ](#)
- [接続ロギング ストラテジー, 2 ページ](#)
- [SSL ルールによる復号可能接続のロギング, 10 ページ](#)
- [セキュリティ インテリジェンスによる接続のロギング, 11 ページ](#)
- [アクセス制御ルールによる接続のロギング, 12 ページ](#)
- [ポリシーのデフォルト アクションによる接続のロギング, 13 ページ](#)
- [長い URL のロギングの制限, 14 ページ](#)

接続ロギングについて

システムは管理対象デバイスで検出された接続のログを生成できます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティ インテリジェンス イベントと呼ばれる特別な接続イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によってブラックリストに登録（ブロック）された接続を表します。

接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求される URL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性

- どの設定がトラフィックを処理したか、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など、接続がログに記録された理由に関するメタデータ



(注) エクスポートした NetFlow レコードから生成された接続データを使い、管理対象デバイスで収集された接続ログを補うことができます。これは、Firepower システムの管理対象デバイスでモニタできないネットワーク上に NetFlow 対応ルータやその他のデバイスを配置した場合に特に有効です。

接続ロギング戦略

部門のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワークトラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。



ヒント 接続データの詳細な分析を実行するため、シスコはクリティカルな接続の終了を Firepower Management Center データベースに記録することを推奨します。

システムは1つの接続をさまざまな理由でロギングすることがあるため、1ヵ所でロギングを無効にしても、一致する接続がロギングされないとは限りません。また、接続イベントストレージを無効にしない限り、システムが自動でロギングする接続もあります。検出したファイル、マルウェア、侵入、インテリジェント アプリケーションバイパス (IAB) に関連する接続がその例です。

8000 シリーズのファーストパス ルールでファーストパスされた接続をロギングすることはできません。

設定可能な接続ロギング

重要な接続のみがロギングされるように、ルールごとの接続ロギングを有効にします。あるルールに対し接続ロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

また、ポリシーのデフォルトアクションにより処理された接続をロギングすることもできます。ルールやデフォルトアクションにより (アクセス制御の場合は、ルールのインスペクション設定により)、ロギングのオプションは異なります。

SSL ポリシー：ルールとデフォルトアクション

SSL ルールまたは SSL ポリシーのデフォルトアクションに一致する接続をロギングすることができます。

ブロックされた接続の場合、システムは即座にセッションを終了し、イベントを生成します。監視対象の接続やアクセスコントロールルールに渡す接続の場合、システムはセッションが終了するとイベントを生成します。

アクセスコントロールポリシー：セキュリティインテリジェンスによる判断

接続がレピュテーションベースのセキュリティインテリジェンス機能によってブラックリスト登録（ブロック）される場合は、その接続をログに記録できます。

オプションで、セキュリティインテリジェンスフィルタリングにはモニタ専用設定を使用できません。パッシブ展開環境では、この設定が推奨されます。この設定では、ブラックリスト登録されるはずの接続をシステムがさらに分析できるだけでなく、ブラックリストと一致する接続をログに記録することもできます。セキュリティインテリジェンスモニタリングによって、セキュリティインテリジェンス情報を使用してトラフィックプロファイルを作成することもできます。

セキュリティインテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティインテリジェンスイベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析することができ、また個別に保存、ブルーニングされます。接続でブラックリスト登録されたIPアドレスを特定できるように、IPアドレスの横にあるホストアイコンは、ブラックリスト登録されたIPアドレスとモニタされたIPアドレスではイベントビューアで少々異なる表示になっています。

アクセスコントロールポリシー：ルールとデフォルトアクション

アクセスコントロールルールまたは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に一致する接続をロギングすることができます。

自動接続ロギング

接続イベントのストレージを無効にしない限り、システムは他のロギング設定に関係なく、Firepower Management Center データベースに次の接続終了イベントを保存します。

侵入に関連付けられた接続

システムは、接続が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で処理されなければ、侵入イベントに関連付けられた接続を自動的にログに記録します。

アクセスコントロールのデフォルトアクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録しません。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

ただし例外として、デフォルトアクションの接続開始ロギングを有効にした場合はその限りではありません。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録します。

ファイル イベントとマルウェア イベントに関連付けられた接続

システムは、ファイル イベントとマルウェア イベントに関連付けられた接続を自動的にログに記録します。



- (注) NetBIOS-ssn (SMB) トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

インテリジェント アプリケーション バイパスに関連付けられた接続

システムは、IAB に関連付けられたバイパスされた、およびバイパスされるはずだった接続をログに記録します。

接続開始のロギングと終了のロギングの比較

接続は、次の例外となるブロックされたトラフィックを除き、接続開始時あるいは終了時にログを記録することができます。

- ブロックされたトラフィック：ブロックされたトラフィックは、さらに検査されることなくすぐさま拒否されるため、通常、ブロックされたトラフィックやブラックリストに登録されたトラフィックについては、接続開始イベントのみ記録可能です。ログに記録される個々の接続終了はありません。
- ブロックされた暗号化トラフィック：SSL ポリシーで接続のロギングを有効にすると、システムは接続開始イベントではなく接続終了イベントをログに記録します。これは、システムは接続がセッション内で最初のパケットを使用して暗号化されているかどうかを判定できず、暗号化されたセッションを即座にブロックできないためです。

パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。何らかの理由で接続をモニタリングすると、接続終了ロギングが強制されます。単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

表 1: 接続開始イベントと接続終了イベントの比較

	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の状態の場合 <ul style="list-style-type: none"> • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合
次のものについてロギングが可能です	SSL ポリシーによってブロックされた接続を除くすべての接続	すべての接続。ただし、すべての場所で接続終了ロギングを設定できない場合があります。
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケット）で判定できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）
次の場合に有用です	次のものをロギングする場合 <ul style="list-style-type: none"> • ブロックされた接続。 • 接続終了情報はユーザにとって重要ではないので、接続の開始のみ 	目的 <ul style="list-style-type: none"> • SSL ポリシーによって処理される暗号化接続をロギングする場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合、またはその情報を使用して相関ルールをトリガーする場合 • カスタム ワークフローで接続の概要（集約接続データ）を表示する場合、グラフ形式で接続データを表示する場合、またはトラフィックプロファイルを作成して使用する場合

Firepower Management Center と外部ロギング

接続イベントとセキュリティ インテリジェンス イベントは Firepower Management Center データベースにロギングできます（Web インターフェイスの [イベント ビューア (Event Viewer)]）。Firepower Management Center に保存できるイベントの数はモデルによって異なります。アラート

応答と呼ばれる接続を設定し、それを使って外部 syslog や SNMP トラップサーバにイベントをロギングすることもできます。

Firepower Management Center データベースにロギングすると、Firepower システムのレポート、分析、およびデータ相関関係の多くの機能を活用できます。次に例を示します。

- ダッシュボードおよびコンテキストエクスプローラでは、システムによってロギングされた接続をグラフ形式によって一目で確認できます。
- イベントビューには、システムによってロギングされた接続の詳細情報が提示され、グラフ形式や表形式で表示したり、レポートに要約することもできます。
- トラフィック プロファイリングは、接続データを使用して正常なネットワーク トラフィックのプロファイルを作成します。ユーザはそのプロファイルを基準として使用して、異常な動作を検出および追跡できます。
- 相関ポリシーを使用して、イベントを生成し、特定のタイプの接続またはトラフィック プロファイルの変更に対する応答（アラートや外部修復など）をトリガーできます。



(注) これらの機能を使用するには、接続（ほとんどの場合、接続の開始ではなく接続の終了）を Firepower Management Center データベースにロギングする必要があります。システムがクリティカルな接続（ログに記録された侵入、禁止されたファイルおよびマルウェアに関連付けられているもの）を自動的にロギングするのはこのためです。

アクションと接続ロギング

接続ロギングを設定する場合、ルールアクションおよびポリシーのデフォルトアクションにより、一致するトラフィックをシステムがどのように検査、処理するのかわけだけでなく、一致するトラフィックの詳細をいつ、どのようにロギングするかが決まります。接続イベントには、接続がロギングされた理由を記述したメタデータが含まれています。メタデータにはトラフィックがどのように設定によって処理されたかなどの情報が含まれます。

モニタされた監視接続のロギング

システムは常に、以下の設定と一致するトラフィックの接続終了をロギングします。このことは、トラフィックに一致する他のルールがなく、デフォルトアクションのロギングを有効にしている場合でも該当します。

- セキュリティ インテリジェンス：モニタするように設定されたブラックリスト（セキュリティ インテリジェンス イベントも生成されます）
- SSL ルール：[モニタ (Monitor)]アクション
- アクセス コントロールルール：[モニタ (Monitor)]アクション

システムは、1つの接続が1つのモニタールールに一致するたびに1つの別個のイベントを生成するわけではありません。1つの接続が複数のモニタールールに一致する可能性があるため、各接続イベントには、接続が一致する最初の8つのモニターアクセスコントロールルールに関する情報だけでなく、最初の一致するSSLモニタールールに関する情報を含めて表示することができます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは1つの接続が1つのモニタールールに一致するたびに1つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニタールールの情報が含まれます。

信頼されている接続のロギング

信頼されている接続の開始と終了をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- アクセスコントロールルール : [信頼する (Trust)] アクション
- アクセスコントロールのデフォルトアクション : [すべてのトラフィックを信頼する (Trust All Traffic)]

信頼されている接続には、ディープインスペクションまたはディスカバリは適用されません。したがって、信頼されている接続の接続イベントに含まれる情報は限られます。

システムは、接続を検出したデバイスに応じて異なる方法で、信頼アクセスコントロールルールによって処理された TCP 接続をロギングします。

- 7000 および 8000 シリーズ デバイスでは、信頼ルールによって最初のパケットで検出された TCP 接続は、すでに有効になっているモニタールールの有無に応じて異なるイベントを生成します。モニタールールがアクティブな場合、システムはパケットを評価し、接続開始および接続終了イベントを生成します。アクティブなモニタールールがない場合、システムは接続終了イベントだけを生成します。
- 他のすべてのモデルでは、信頼ルールによって最初のパケットで検出された TCP 接続は、接続終了イベントだけを生成します。システムは、最後のセッションパケットの1時間後にイベントを生成します。

ブロックされた接続のロギング

ブロックされた接続をロギングできます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- セキュリティ インテリジェンス : ブロックするブラックリストが設定されます (セキュリティ インテリジェンス イベントも生成されます)
- SSL ルール : [ブロック (Block)] および [リセットしてブロック (Block with reset)]
- SSL のデフォルトアクション : [ブロック (Block)] および [リセットしてブロック (Block with reset)]

- アクセスコントロールルール：[ブロック (Block)]、[リセットしてブロック (Block with reset)]、[インタラクティブブロック (Interactive Block)]
- アクセスコントロールのデフォルトアクション：[すべてのトラフィックをブロック (Block All Traffic)]

トラフィックをブロックできるデバイスは、インライン（つまり、ルーテッドインターフェイス、スイッチドインターフェイス、トランスペアレントインターフェイス、インラインインターフェイスのペア）で展開されているもののみです。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。



注意

サービス妨害 (DoS) 攻撃の間にブロックされた TCP 接続をロギングすると、システムパフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロックルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

ブロックされた接続の接続開始ロギングと接続終了ロギングとの比較

ブロックされた接続をロギングするときは、システムがその接続をどのようにロギングするかは接続がブロックされた理由によって異なります。これは、接続ログに基づいて関連ルールを設定する際に留意しておくことが重要です。

- 暗号化されたトラフィックをブロックする SSL ルールおよび SSL ポリシーのデフォルトアクションの場合、システムは接続終了イベントをロギングします。これは、システムが接続がセッション内で最初のパケットを使用して暗号化されているかどうかを決定できないためです。
- 他のブロッキングアクションについては、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

バイパスされるインタラクティブ ブロックのロギング

インタラクティブブロッキングアクセスコントロールルール（このルールではユーザが禁止されている Web サイトを参照するとシステムによって警告ページが表示されます）を使用すると、接続終了ロギングを設定できます。その理由は、警告ページをユーザがクリックスルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。

したがって、[インタラクティブブロック (Interactive Block)]ルールまたは[リセットしてインタラクティブブロック (Interactive Block with reset)]ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション[インタラクティブブロック (Interactive Block)]または[リセットしてインタラクティブブロック (Interactive Block with reset)]が関連付けられます。

- 複数の接続開始または終了イベント（ユーザが警告ページをクリックスルーし、要求した最初のページをロードした場合）。これらのイベントには [許可 (Allow)] アクションおよび理由 [ユーザ バイパス (User Bypass)] が関連付けられます。

許可された接続のロギング

許可された接続をロギングができます。ロギングには、以下のルールとアクションに一致するトラフィックを含めることができます。

- SSL ルール : [複合 (Decrypt)] アクション
- SSL ルール : [複合しない (Do not decrypt)] アクション
- SSL のデフォルトアクション : [複合しない (Do not decrypt)] アクション
- アクセス コントロール ルール : [許可 (Allow)] アクション
- アクセス コントロールのデフォルトアクション : [ネットワーク検出のみ (Network Discovery Only)] および任意の侵入防御オプション

これらの設定に対するロギングを有効にすると、接続が確実にロギングされると同時に、インスペクションおよびトラフィック処理の次のフェーズが許可（または指定）されます。SSL ロギングは常に接続終了ロギングですが、アクセス コントロール設定で接続開始ロギングも可能にすることができます。

アクセス コントロール ルールまたはデフォルトアクションでトラフィックを許可する場合、関連する侵入ポリシーを使用してトラフィックをさらに検査し、侵入をブロックすることができます。アクセス コントロール ルールでは、ファイル ポリシーを使用して、マルウェアを含む禁止されたファイルを検出し、ブロックすることもできます。接続イベントストレージを無効にしない限り、システムは、侵入イベント、ファイルイベント、マルウェアイベントに関連する許可された接続のほとんどを自動的にロギングします。詳細については、[自動接続ロギング](#)、(3 ページ) を参照してください。ペイロードが暗号化される接続には、ディープインスペクションは適用されません。したがって、暗号化接続の接続イベントに含まれる情報は限られることに注意してください。

許可された接続のファイルおよびマルウェア イベントのロギング

ファイルポリシーによってファイルが検出またはブロックされると、以下のいずれかのイベントが Firepower Management Center データベースにロギングされます。

- ファイル イベント : 検出またはブロックされたファイル（マルウェア ファイルを含む）を表します
- マルウェア イベント : 検出されたまたはブロックされたマルウェア ファイルのみを表します
- レトロスペクティブ マルウェア イベント : 以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます

このロギングは、アクセスコントロールルールごとが無効にすることができます。または、ファイルイベントおよびマルウェア イベント ストレージを完全に無効にすることもできます。



(注) Ciscoでは、ファイルイベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

SSL ルールによる復号可能接続のロギング

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)	すべて (NGIPSv を除く)	任意 (Any)	Admin/Access Admin/Network Admin

手順

- ステップ 1** SSL ポリシーエディタで、ロギングを設定するルールの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 2** [ロギング (Logging)] タブをクリックします。
- ステップ 3** [接続の終了時にロギングする (Log at End of Connection)] をオンにします。モニタ対象トラフィックに対して、接続の終了時のロギングが必要になります。
- ステップ 4** 接続イベントの送信先を指定します。
接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベントビューアに送信します。モニタ対象トラフィックに対して、これが必要になります。
- ステップ 5** [保存 (Save)] をクリックしてルールを保存します。
- ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

セキュリティインテリジェンスによる接続のロギング

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)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin

手順

- ステップ 1** アクセスコントロールポリシーエディタで、[セキュリティインテリジェンス (Security Intelligence)] タブをクリックします。
- ステップ 2** ロギングアイコン (📄) をクリックして、次の条件を使用するセキュリティインテリジェンスロギングを有効にします。
- IP アドレス別 : [ネットワーク (Networks)] の横にあるロギングアイコンをクリックします。
 - URL 別 : [URL (URLs)] の横にあるロギングアイコンをクリックします。
 - ドメイン名別 : [DNS ポリシー (DNS Policy)] ドロップダウンリストの横にあるロギングアイコンをクリックします。
- コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
- ステップ 3** [接続のロギング (Log Connections)] チェックボックスをオンにします。
- ステップ 4** 接続イベントとセキュリティインテリジェンスイベントの送信先を指定します。Firepower Management Center ベースの分析を実行する場合や、ブラックリストに登録されたオブジェクトをモニタ専用を設定する場合は、イベントをイベントビューアに送信します。
- ステップ 5** [OK] をクリックしてロギングオプションを設定します。
- ステップ 6** [保存 (Save)] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

アクセス制御ルールによる接続のロギング

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)	任意 (Any)	Admin/Access Admin/Network Admin

ルールアクションと詳細検査のオプションの選択によって、ロギングオプションは異なります。
[アクションと接続ロギング](#)、[\(6 ページ\)](#) を参照してください。

手順

-
- ステップ 1** アクセス コントロール ポリシー エディタで、ロギングを設定するルールの横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 2** [ロギング (Logging)] タブをクリックします。
- ステップ 3** [接続の開始時にロギングする (Log at Beginning of Connection)] または [接続の終了時にロギングする (Log at End of Connection)] を指定します。
- パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。
- ステップ 4** (オプション) [ファイルのロギング (Log Files)] チェックボックスをオンにして、接続に関連付けられているファイル イベントとマルウェア イベントをロギングします。
- シスコは、このオプションを有効のままにすることを推奨します。
- ステップ 5** 接続イベントの送信先を指定します。
- 接続イベントに対し、Management Center ベースの分析を実行する場合や、ルールアクションが [モニタ (Monitor)] の場合は、イベントを Firepower Management Center に送信します。
- ステップ 6** [保存 (Save)] をクリックしてルールを保存します。
-

次の作業

- 設定変更を展開します。[設定変更の導入](#) を参照してください。

ポリシーのデフォルトアクションによる接続のロギング

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)	任意 (Any)	Admin/Access Admin/Network Admin

ポリシーのデフォルトアクションにより、システムがポリシー内のルールのいずれにも一致しないトラフィックを処理する方法が決定されます（ただし、トラフィックの照合およびロギングを実行し、トラフィックの処理や調査は実行しないモニタールールを除きます）。

また、システムが複合化できないセッションをロギングする方法は、SSL ポリシーのデフォルトアクションのロギング設定でも制御されます。

手順

-
- ステップ 1** ポリシーエディタで、[デフォルトアクション (Default Action)] ドロップダウンリストの横にあるロギングアイコン (📄) をクリックします。
- ステップ 2** 一致する接続をロギングするタイミングを指定します。
- 接続の開始時にロギングする：SSL のデフォルトアクションではサポートされていません。
 - 接続の終了時にロギングする：アクセス制御の [すべてのトラフィックをブロック (Block All Traffic)] デフォルトアクションを選択するとサポートされなくなります。
- パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。
- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。アクセスコントロールポリシーでは、設定が先祖ポリシーから継承されることもあります。
- ステップ 3** 接続イベントの送信先を指定します。
接続イベントについて Firepower Management Center ベースの分析を実行する場合は、イベントをイベントビューアに送信します。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [保存 (Save)] をクリックしてポリシーを保存します。
-

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

長い URL のロギングの制限

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)	任意 (Any)	Admin/Access Admin/Network Admin

HTTP トラフィックの接続の終了イベントは、監視対象ホストによって要求された URL を記録します。URL の保管を無効にすることや保管する URL 文字数を制限することで、システムパフォーマンスが向上する可能性があります。URL のロギングを無効化しても（保管する文字数を 0 にしても）、URL フィルタリングには影響しません。システムは、要求された URL に基づいてトラフィックをフィルタリングします。それらの URL を記録しない場合も同じです。

手順

-
- ステップ 1** アクセス コントロール ポリシー エディタで、[詳細 (Advanced)] タブをクリックして、[一般設定 (General Settings)] の横にある編集アイコン (✎) をクリックします。
- 代わりに表示アイコン (🔍) が表示される場合、設定は先祖ポリシーから継承され、先祖ドメインに属しており、設定を変更する権限がありません。設定がロック解除されている場合は、[ベースポリシーから継承する (Inherit from base policy)] をオフにして、編集を有効にします。
- ステップ 2** [接続イベントで保存する URL の最大文字数 (Maximum URL characters to store in connection events)] を入力します。
- ステップ 3** [OK] をクリックします。
- ステップ 4** [保存 (Save)] をクリックしてポリシーを保存します。
-

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。