ネットワーク トラフィックの接続のロギング

管理対象デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。また、アクセス コントロール ルールの特定のロギング設定では、接続に関連するファイル イベントとマルウェア イベントをログに記録するかどうかも決定します。

ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。接続をログに記録すると、システムによって*接続イベント*が生成されます。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、*セキュリティ インテリジェンス イベント*と呼ばれる特別な種類の接続イベントをログに記録することもできます。

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
- ポリシーがどのアクセス コントロール ルール（または他の設定）で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るかどうか、暗号化された接続および復号化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

組織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。アクセス コントロールに到達する前にデバイス レベルで高速パス処理される接続を除く**すべての**接続をログに記録できます。

接続イベントを Defense Center データベースに保存すると、FireSIGHT 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。接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）を参照してください。または、外部システム ログ（syslog）または SNMP トラップ サーバに接続データを送信できます。

管理対象デバイスで収集された接続データを補うために、NetFlow 対応デバイスによって生成されたレコードを使用して接続イベントを生成できます。これは、FireSIGHT システム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 対応デバイスを配置した場合に特に有効です。

(注) NetFlow のデータ収集はアクセス コントロールにリンクされていないため、ロギングする NetFlow 接続については、きめ細かい制御ができません。FireSIGHT システムの管理対象デバイスは NetFlow 対応デバイスによってエクスポートされるレコードを検出し、それらのレコードのデータに基づいて単一方向の接続終了イベントを生成し、最終的にそのイベントをデータベースに記録するために Defense Center へ送信します。NetFlow レコードはセキュリティ インテリジェンス イベントを生成できず、外部サーバにも記録できません。詳細については、NetFlow について (45-18 ページ) を参照してください。

接続データのロギングの詳細については、以下を参照してください。

- どの接続をログに記録するかの決定 (38-2 ページ)
- セキュリティ インテリジェンス (ブラックリスト登録) の決定のロギング (38-13 ページ)
- 暗号化された接続のロギング (38-15 ページ)
- アクセス コントロールの処理に基づく接続のロギング (38-18 ページ)
- 接続で検出された URL のロギング (38-22 ページ)

どの接続をログに記録するかの決定

ライセンス: 任意 (Any)

アクセス コントロール ポリシーと SSL ポリシーのさまざまな設定を使用して、デバイスがモニタする非高速パス接続をログに記録できます。ほとんどの場合、接続の開始または終了、またはその両方で接続をロギングできます。しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

接続イベントをログに記録するときに、Defense Center データベースにそれを保存し、FireSIGHT システムを使用してさらなる分析を行うことができます。または、外部 syslog または SNMP トラップ サーバに接続データを送信できます。

ヒント FireSIGHT システムを使用して接続データの詳細な分析を実行するには、クリティカルな接続の終了を Defense Center データベースに記録することを Cisco で は推奨しています。

詳細については、以下を参照してください。

- クリティカルな接続のロギング (38-3 ページ)
- 接続の開始または終了のロギング (38-5 ページ)
- Defense Center または外部サーバへの接続のロギング (38-6 ページ)
- アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて (38-7 ページ)
- 接続ロギングのライセンスおよびモデル要件 (38-11 ページ)

クリティカルな接続のロギング

ライセンス：任意（Any）

組織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。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。

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。

設定するロギングに加えて、禁止されたファイル、マルウェア、または侵入の試みをシステムが検出した場合には、ほとんどの接続を自動的にログに記録します。他のロギング設定に関係なく、システム ポリシーを使用して接続イベント ストレージを完全に無効にしない限り、システムはこれらの接続終了イベントを Defense Center データベースに保存し、さらなる分析に使用します。すべての接続イベントは、自動的にログ記録された理由を [アクション（Action）] および [理由（Reason）] フィールドを使用して反映します。操作（39-5 ページ）および理由（Reason）（39-9 ページ）を参照してください。

セキュリティ インテリジェンス ブラックリスト登録の決定（オプション）

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」設定を使用できます。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 ロギングを有効にすると、ブラックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが生成されます。セキュリティ インテリジェンス 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できるだけでなく、個別に保存およびプルーニングできます。詳細については、セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-13 ページ）を参照してください。

暗号化された接続（任意）

SSL ポリシーの設定に従ってシステムが暗号化されたセッションをブロックしたときの接続をログに記録できます。また、トラフィックを復号化するかどうかにかかわらず、またシステムがトラフィックを後でどのように処理または検査するかにかかわらず、アクセス コントロール ルールによるさらなる評価のためにシステムが渡す接続をログに記録するように強制することもできます。クリティカルな接続のみをログに記録するように、このロギングは SSL ルールごとに設定します。詳細については、暗号化された接続のロギング（38-15 ページ）を参照してください。

アクセス コントロールの処理（オプション）

接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理される場合は、その接続をログに記録できます。クリティカルな接続のみをログに記録できるように、このロギングはアクセス コントロール ルールごとに設定します。詳細については、アクセス コントロールの処理に基づく接続のロギング（38-18 ページ）を参照してください。

侵入に関連付けられる接続（自動）

アクセス コントロール ルールによって呼び出された侵入ポリシー（アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照）が侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。

しかし、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（ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定（12-8 ページ）を参照）によって侵入イベントが生成された場合、システムは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に役立ちます。

侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）]、理由は [侵入ブロック（Intrusion Block）] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ヒント　シリーズ 3 または仮想デバイスでこの接続ロギングを無効にするには、CLI を使用します。log-ips-connections（D-35 ページ）を参照してください。

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（自動）

アクセス コントロール ルールによって呼び出されたファイル ポリシーが、禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を Defense Center データベースに自動的にロギングします。このロギングを無効にすることは**できません**。

（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。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイル モニタ（File Monitor）]（ファイル タイプまたはマルウェアが検出された）、あるいは [マルウェア ブロック（Malware Block）] または [ファイル ブロック（File Block）]（ファイルがブロックされた）です。

接続の開始または終了のロギング

ライセンス: 任意（Any）

システムが接続を検出すると、ほとんどの場合、その開始または終了をログに記録できます。

しかし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックまたはブラックリスト登録されたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。暗号化されたトラフィックをブロックする場合は例外です。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。

（注） 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。

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。接続の開始イベントまたは終了イベントのどちらかに基づいて相関ルールをトリガーできます。何らかの理由で接続をモニタすると、接続終了ロギングが強制されることに注意してください。モニタされた接続のロギングについて（38-7 ページ）を参照してください。

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 38-1　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）	システムが以下の場合 • 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	セキュリティ インテリジェンスまたはアクセス コントロール ルールによって評価されたすべての接続。ただし、すべての場所で接続終了ロギングを設定できるとは限らない可能性があります。	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るとは限らない可能性があります。
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）

表 38-1　接続開始イベントと接続終了イベントの比較（続き）

	接続開始イベント	接続終了イベント
次の場合に有用です	次のものをロギングする場合 • セキュリティ インテリジェンス ブラックリスト登録の決定を含む、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	次の操作をする場合 • 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

Defense Center または外部サーバへの接続のロギング

ライセンス：任意（Any）

接続イベントのログは、Defense Center データベースの他に、外部の syslog または SNMP トラップ サーバにも記録できます。外部サーバに接続データを記録する前に、そのサーバに *アラート応答* という接続を設定する必要があります。アラート応答の使用（43-2 ページ）を参照してください。

Defense Center データベースにロギングすると、FireSIGHT 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 Context Explorer 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。ダッシュボードの使用（55-1 ページ）および Context Explorer の使用（56-1 ページ）を参照してください。
- 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。接続およびセキュリティ インテリジェンスのデータの使用（39-1 ページ）を参照してください。
- 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。トラフィック プロファイルの作成（53-1 ページ）を参照してください。
- 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。相関ポリシーのルールの作成（51-3 ページ）を参照してください。

（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 Defense 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。

Defense Center が保存できる接続イベントおよびセキュリティ インテリジェンス イベントの数は、そのモデルによって異なります。それらの制限のリストおよび接続イベント ストレージの無効化については、データベース イベント制限の設定（63-16 ページ）を参照してください。

アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて

ライセンス：機能に応じて異なる

すべてのアクセス コントロールおよび SSL ルールには *アクション* があり、それによってシステムがルールに一致するトラフィックを検査および処理する方法だけでなく、一致するトラフィックに関する詳細をユーザがロギングできる時期と方法が決まります。

（注） アクセス コントロールと SSL ポリシーのデフォルト アクションによって許可された接続のロギングは、若干処理が異なります。アクセス コントロールのデフォルト アクションによって処理された接続のロギング（38-20 ページ）および暗号化された接続および復号できない接続のデフォルトのロギング設定（38-16 ページ）を参照してください。

詳細については、以下を参照してください。

- ルール アクションを使用したトラフィックの処理とインスペクションの決定（14-8 ページ）
- ルール アクションを使用した暗号化トラフィックの処理と検査の決定（21-9 ページ）
- モニタされた接続のロギングについて（38-7 ページ）
- 信頼されている接続のロギングについて（38-8 ページ）
- ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて（38-8 ページ）
- 許可された接続のロギングについて（38-9 ページ）
- 許可された接続のファイルおよびマルウェア イベント ロギングの無効化（38-10 ページ）

モニタされた接続のロギングについて

ライセンス：機能に応じて異なる

システムは、ルールのロギング設定や、後で接続を処理するデフォルト アクションとは関係なく、次の接続の終了を Defense Center データベースに常にロギングします。

- モニタに設定されたセキュリティ インテリジェンスのブラックリストに一致する接続
- SSL モニタ ルールに一致する接続
- アクセス コントロールのモニタ ルールに一致する接続

言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールまたはセキュリティ インテリジェンスのモニタ対象ブラックリストに一致すれば、必ず接続がロギングされます。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できます。セキュリティ インテリジェンス（ブラックリスト登録）の決定のロギング（38-13 ページ）を参照してください。

モニタ対象のトラフィックは、必ず後で別のルールまたはデフォルト アクションによって処理されるため、モニタ ルールが原因でロギングされる接続に関連するアクションは、決して [モニタ（Monitor）] にはなりません。代わりに、後で接続を処理するルールまたはデフォルト アクションの操作が反映されます。操作（39-5 ページ）を参照してください。

システムは、1 つの接続が 1 つの SSL またはアクセス コントロールのモニタ 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 ルールに一致する可能性があるため、Defense Center データベースにロギングされる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 アクセス コントロール ルールに関する情報だけでなく、最初の一致するモニタ SSL 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 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 ルールの情報が含まれます。

ヒント　接続ログ内のルール アクションは決して `Monitor` になりませんが、モニタ ルールに一致する接続での相関ポリシー違反をトリガーすることはできます。詳細については、相関ルール トリガー条件の指定（51-6 ページ）を参照してください。

信頼されている接続のロギングについて

ライセンス：機能に応じて異なる

信頼されている接続は、信頼アクセス 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 アクションによって処理される接続です。これらの接続の開始と終了をロギングできますが、暗号化されているかどうかにかかわらず、信頼されている接続は検出データ、侵入、または禁止されているファイルおよびマルウェアの有無について検査されないことに注意してください。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。

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 接続をロギングすることに注意してください。

- シリーズ 3 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 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 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、接続の開始および終了イベントを生成します。アクティブなモニタ 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およびインタラクティブにブロックされた接続のロギングについて

ライセンス：機能に応じて異なる

ブロックされた接続をロギングするとき、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。接続ログに基づいて相関ルールを設定する際にはこれを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。

- 復号化トラフィックまたは非暗号化トラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクション(インタラクティブなブロッキング ルールを含む)の場合、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。

アクセス コントロールまたは SSL ルールでブロックされたセッションの接続イベントには、アクション [ブロック(Block)] または [リセットしてブロック(Block with reset)] があります。ブロックされた暗号化接続には 理由 `SSL Block` があります。

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。許可された接続のロギングについて(38-9 ページ)を参照してください。

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)

インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。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。

許可された接続のロギングについて

ライセンス:機能に応じて異なる

[復号(Decrypt)] SSL ルール、[復号しない(Do not decrypt)] SSL ルール、および [許可(Allow)] アクセス コントロール ルールは、一致するトラフィックを許可し、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へと通過させます。

SSL ルールを使用して暗号化されたトラフィックを復号するかどうかにかかわらず、トラフィックはアクセス コントロール ルールによって引き続き評価されます。この SSL ルールにロギングを有効にすると、アクセス コントロール ルールまたはそれらを後で処理するデフォルト アクションのロギング設定に関係なく、システムは一致する接続の終了をロギングします。

アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー(またはその両方)を使用して、トラフィックをさらに検査し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックすることができます。ただし、デフォルトでは、ファイルおよび侵入のインスペクションは暗号化されたペイロードでは無効になっていることに注意してください。

許可アクセス コントロール ルールに一致するトラフィックの接続は次のようにロギングされます。

- アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を Defense Center データベースに自動的にロギングします。
- アクセス コントロール ルールによって呼び出されたファイル ポリシーが、禁止されたファイル(マルウェアを含む)を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を Defense Center データベースに自動的にロギングします。
- 任意で、システムが安全と見なすトラフィックや、侵入ポリシーまたはファイル ポリシーで検査をしないトラフィックなど、許可されたトラフィックに対して接続の開始および終了のロギングを有効にできます。

結果として生じるすべての接続イベントで、[アクション(Action)] および [理由(Reason)] フィールドにイベントがロギングされた理由が反映されます。操作(39-5 ページ)および理由(Reason)(39-9 ページ)を参照してください。次の点に注意してください。

- アクション [許可(Allow)] は、最終宛先に到達した明示的に許可されインタラクティブにユーザがバイパスしたブロックされた接続を表します。
- アクション [ブロック(Block)] は、アクセス コントロール ルールによって初めは許可されたが、侵入、禁止されたファイル、またはマルウェアが検出された接続を表します。

許可された接続のファイルおよびマルウェア イベント ロギングの無効化

ライセンス: Protection または Malware

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

アクセス コントロール ルールで暗号化されていないトラフィックまたは復号化されたトラフィックを許可する場合、関連付けられたファイル ポリシーを使用して送信されたファイルをインスペクションし、そのトラフィックが宛先に到達する前に禁止されたファイルおよびマルウェアをブロックすることができます。侵入防御パフォーマンスの調整(18-10 ページ)を参照してください。DC500 で Malware ライセンスを使用したり、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることはできないので、これらのアプライアンスをマルウェア防御に使用できないことに注意してください。

システムが禁止されたファイルを検出すると、次のタイプのイベントの 1 つを Defense Center データベースに自動的にロギングします。

- *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

ファイル イベントまたはマルウェア イベントをロギングしない場合は、アクセス コントロール ルール エディタの [ロギング(Logging)] タブの [ログファイル(Log Files)] チェックボックスをオフにすることで、アクセス コントロール ルールごとにこのロギングを無効にできます。ファイルおよびマルウェアのイベント ストレージを完全に無効にする詳細については、データベース イベント制限の設定(63-16 ページ)を参照してください。

(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。

ファイル イベントおよびマルウェア イベントを保存するかどうかにかかわらず、ネットワーク トラフィックがファイル ポリシーに違反すると、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、システムは関連付けられた接続の終了を Defense Center データベースに自動的にロギングします。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（自動）（38-4 ページ）を参照してください。

接続ロギングのライセンスおよびモデル要件

ライセンス：機能に応じて異なる

アクセス コントロール ポリシーおよび SSL ポリシーで接続ロギングの設定を行うことで、これらのポリシーが正常に処理できる接続をすべてロギングすることができます。

Defense Center でのライセンスに関係なくアクセス コントロール ポリシーおよび SSL ポリシーを作成できます。ただし、アクセス コントロールのある側面では、ポリシーの適用前にターゲット デバイスで特定のライセンス交付対象の機能を有効にする必要があります。また、一部の機能は、特定のモデルでのみ使用できます。

Defense Center に含まれている FireSIGHT ライセンスを使用して、ホスト、ユーザおよびアプリケーションのデータを接続ログの情報に基づいてネットワーク マップに追加できます。また、接続イベントに関連付けられている侵害の兆候（IOC）情報を表示できます。DC500 以外では、接続に関連付けられている位置情報データ（送信元または宛先の国または大陸）を表示することもできます。

次の表では、アクセス コントロールを正常に設定し、アクセス コントロール ポリシーによって処理される接続をロギングするのに必要なライセンスについて説明します。

表 38-2　アクセス コントロール ポリシーにおける接続ロギングのライセンスおよびモデルの要件

次の接続をロギングするには	ライセンス	サポートされる Defense Center	サポートされるデバイス
ネットワーク、VLAN、ポートまたはリテラル URL 基準を使用して処理されるトラフィック用	Any	Any	任意（Any）、ただし次を除く。 • シリーズ 2デバイスは、URL フィルタリングを実行できません • ASA FirePOWER デバイスは、VLAN フィルタリングを実行できません
位置情報データを使用して処理されるトラフィック用	FireSIGHT	DC500 を除くいずれか	シリーズ 2 と X-シリーズを除くすべて

表 38-2　アクセス コントロール ポリシーにおける接続ロギングのライセンスおよびモデルの要件(続き)

次の接続をロギングするには	ライセンス	サポートされる Defense Center	サポートされるデバイス
関連付ける対象 • レピュテーションが低い IP アドレス(セキュリティ インテリジェンスのフィルタリング) • 暗号化されていないトラフィックまたは復号化されたトラフィックでの侵入または禁止されたファイル	Protection	Any	任意:例外として、シリーズ 2 デバイスではセキュリティ インテリジェンス フィルタリングを実行できません。
暗号化されていないトラフィックまたは復号化されたトラフィックで検出されたマルウェアに関連付けられる	Malware	DC500 を除くいずれか	シリーズ 2 と X-シリーズを除くすべて
ユーザ制御またはアプリケーション制御によって処理されるトラフィック用	Control	任意:例外として、DC500 ではユーザ制御を実行できません。	シリーズ 2 と X-シリーズを除くすべて
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングするトラフィック用、およびモニタ対象ホストによって要求される URL の URL カテゴリおよび URL レピュテーション情報を表示するため	URL フィルタリング(URL Filtering)	DC500 を除くいずれか	すべて(シリーズ 2 を除く)

次の表では、SSL インスペクションを正常に設定し、SSL ポリシーによって処理される接続をロギングするために必要なライセンスについて説明します。暗号化された接続が SSL ポリシーによってロギングされない(または検査さえされない)場合でも、他の理由で依然としてロギングされる場合があることに留意してください。

表 38-3　SSL ポリシーにおける接続ロギングのライセンスおよびモデルの要件

次の接続をロギングするには	ライセンス	サポートされる Defense Center	サポートされるデバイス
ゾーン、ネットワーク、VLAN、ポート、または SSL 関連の基準を使用して処理される暗号化トラフィック用	Any	Any	シリーズ 3
地理位置情報データを使用して処理される暗号化トラフィック用	FireSIGHT	任意(DC500 を除く)	シリーズ 3
アプリケーションまたはユーザの基準を使用して処理される暗号化トラフィック用	Control	任意:例外として、DC500 ではユーザ制御を実行できません。	シリーズ 3
URL カテゴリおよびレピュテーション データを使用してシステムがフィルタリングする暗号化トラフィック用	URL フィルタリング(URL Filtering)	DC500 を除くいずれか	シリーズ 3

セキュリティ インテリジェンス(ブラックリスト登録)の決定のロギング

ライセンス: Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:DC500 を除くいずれか

悪意のあるインターネット コンテンツに対する第一の防衛ラインとして、FireSIGHT システムにはセキュリティ インテリジェンス機能があります。これを使用すると、接続を最新のレピュテーション インテリジェンスに基づいて即座にブラックリスト登録(ブロック)することができるため、リソースを集中的に消費する詳細な分析が不要になります。このトラフィック フィルタリングは、他のすべてのポリシー ベースのインスペクション、分析、またはトラフィック処理よりも**先**に行われます(ただし高速パスなどのハードウェア レベルの処理の後に発生します)。

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」設定を使用できます。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。

(注) セキュリティ インテリジェンス情報に基づいてトラフィック プロファイルを作成する場合、または接続終了イベントのセキュリティ インテリジェンス情報を使用して相関ルールをトリガーする場合は、この情報を Defense Center データベースにロギングする**必要があります**。最初に、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。次に、モニタ専用のセキュリティ インテリジェンス オブジェクトを使用して、ブラックリストを作成します。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録 (13-1 ページ)を参照してください。

セキュリティ インテリジェンスのロギングを有効にすると、アクセス コントロール ポリシーのターゲット デバイスによって処理されるすべてのブロックされた接続およびモニタされた接続がロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。

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できます。どちらのタイプのイベントも、[アクション(Action)] および [理由(Reason)] フィールドを使用して、ブラックリストの一致を反映します。さらに、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。

ブロックされたブラックリスト登録された接続のロギング

ブロックされた接続の場合、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブラックリスト登録されたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続の終了イベントはありません。これらのイベントの場合、アクションは [ブロック(Block)]、理由は [IP ブロック(IP Block)] です。

[IP ブロック(IP Block)] 接続イベントのしきい値は、開始側と応答側の固有のペアあたり 15 秒です。つまり、システムは接続をブロックしてイベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、別の接続イベントを生成しません。

モニタされブラックリスト登録された接続のロギング

セキュリティ インテリジェンスによってモニタされた(ブロックではなく)接続の場合、システムは接続終了セキュリティ インテリジェンス イベントと接続イベントを Defense Center データベースにロギングします。このロギングは、接続が後で SSL ポリシー、アクセス コントロール ルール、またはアクセス コントロールのデフォルト アクションによってどのように処理されるかにかかわらず発生します。

これらの接続イベントの場合、アクションは接続の最終的な傾向によって異なります。[理由(Reason)] フィールドには、[IP モニタ(IP Monitor)] と、接続がロギングされている可能性がある他の理由が含まれています。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルト アクションでのロギング設定によっては、接続開始イベントが生成されることもあります。

ブラックリスト登録された接続をログに記録する方法:

アクセス: Admin/Access Admin/Network Admin

手順 1　[ポリシー(Policies)] > [アクセス制御(Access Control)] を選択します。

[アクセス コントロール ポリシー(Access Control Policy)] ページが表示されます。

手順 2　設定するアクセス コントロール ポリシーの横にある編集アイコン( )をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[セキュリティ インテリジェンス(Security Intelligence)] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

手順 4　ロギング アイコン( )をクリックします。

[ブラックリスト オプション(Blacklist Options)] ポップアップ ウィンドウが表示されます。

手順 5　[ログ接続(Log Connections)] チェックボックスをオンにします。

手順 6　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。次の選択肢があります。

- イベントを Defense Center に送信する場合は、[Defense Center] を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン( )をクリックします。Syslog アラート応答の作成(43-5 ページ)を参照してください。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ(SNMP Trap)] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン( )をクリックして SNMP アラート応答を追加することもできます(SNMP アラート応答の作成(43-4 ページ)を参照)。

ブラックリスト登録されたオブジェクトをモニタ専用に設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の Defense Center ベースの分析を行う場合は、イベントを Defense Center に送信することが**必須**となります。詳細については、Defense Center または外部サーバへの接続のロギング(38-6 ページ)を参照してください。

手順 7　[OK] をクリックしてロギング オプションを設定します。

[セキュリティ インテリジェンス(Security Intelligence)] タブが再表示されます。

手順 8　[保存(Save)] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。

暗号化された接続のロギング

ライセンス：SSL

サポートされるデバイス：シリーズ 3

アクセス コントロールの一部として、*SSL インスペクション*機能を使用することで、SSL ポリシーを使用してアクセス コントロール ルールによるさらなる評価のために暗号化されたトラフィックを復号できます。システムがトラフィックを後でどのように処理または検査するかにかかわらず、これらの復号された接続のログを記録するようにシステムに強制できます。また、暗号化されたトラフィックをブロックするとき、または復号せずにトラフィックがアクセス コントロール ルールに渡されることを許可するときに、接続をロギングすることもできます。

暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。クリティカルな接続のみをログに記録するように、SSL ポリシーの暗号化されたセッションの接続ロギングは SSL ルールごとに設定します。

詳細については、次の項を参照してください。

- SSL ルールによる復号可能接続のロギング（38-15 ページ）
- 暗号化された接続および復号できない接続のデフォルトのロギング設定（38-16 ページ）

SSL ルールによる復号可能接続のロギング

ライセンス：SSL

サポートされるデバイス：シリーズ 3

SSL ポリシー内では、*SSL ルール*は複数の管理対象デバイス間で暗号化されたトラフィックを処理する詳細な方法を提供します。クリティカルな接続のみをロギングできるように、SSL ルールごとに接続ロギングを有効にします。あるルールに対して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るすべての接続をロギングします。

SSL ポリシーによって検査される暗号化された接続の場合、接続イベントのログを Defense Center データベース、または外部の syslog や SNMP トラップ サーバに記録できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）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。
- モニタ対象の接続（[モニタ（Monitor）]）およびアクセス コントロール ルールに渡す接続（[復号する（Decrypt）]、[復号しない（Do not decrypt）]）の場合、アクセス コントロール ルールまたはそのセッションを後で処理するデフォルト アクションのロギング設定に関係なく、システムはセッション終了時にイベントを生成します。

詳細については、アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（38-7 ページ）を参照してください。

復号できる接続をログに記録するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin/Security Approver

手順 1　[ポリシー（Policies）] > [SSL] を選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

手順 2　編集する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示され、[ルール（Rules）] タブにフォーカスが移動します。

手順 3　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。

SSL ルール エディタが表示されます。

手順 4　[ロギング(Logging)] タブを選択します。

[ロギング(Logging)] タブが表示されます。

手順 5　[接続の終了時点でロギングを行う(Log at End of Connection)] を選択します。

手順 6　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、**[Defense Center]** を選択します。ルール アクションが [モニタ(Monitor)] である場合は、接続をDefense Centerにロギングする必要があります。
- イベントを外部の syslog に送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン( )をクリックします。Syslog アラート応答の作成(43-5 ページ)を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ(SNMP Trap)] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン( )をクリックして SNMP アラート応答を追加することもできます(SNMP アラート応答の作成(43-4 ページ)を参照)。

これらの接続イベントで Defense Center ベースの分析を実行するには、Defense Center にイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング(38-6 ページ)を参照してください。

手順 7　[追加(Add)] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ)を参照してください。

暗号化された接続および復号できない接続のデフォルトのロギング設定

ライセンス:SSL

サポートされるデバイス:シリーズ 3

SSL ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録できます。これらのロギング設定では、システムが復号できないセッションをどのようにログに記録するかも管理されます。

SSL ポリシーのデフォルト アクションは、ポリシー内のどの SSL ルール(トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く)にも一致しない暗号化されたトラフィックをシステムがどのように処理するかを決定します。SSL ポリシーに SSL ルールが含まれていない場合、デフォルト アクションは、ネットワーク上のすべての暗号化セッションがどのようにログに記録されるかを決定します。詳細については、暗号化トラフィックに対するデフォルトの処理とインスペクションの設定(20-4 ページ)を参照してください。

接続イベントを Defense Center データベース、または外部の syslog や SNMP トラップ サーバにロギングするように SSL ポリシーのデフォルト アクションを設定できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[ブロック（Block）]、[リセットしてブロック（Block with reset）]）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。
- 暗号化されていない接続をアクセス コントロール ルールに渡すことを許可する接続の場合（[復号しない（Do not decrypt）]、システムはセッションの終了時にイベントを生成します。

SSL ポリシーのデフォルト アクションのロギングを無効にしても、接続が以前に少なくとも 1 つの SSL モニタ ルールに一致していた場合、または後でアクセス 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場合は、接続終了イベントが引き続き Defense Center データベースにロギングされる可能性があることに注意してください。

暗号化されたトラフィックおよび復号できないトラフィックのデフォルトの処理を設定するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin/Security Approver

手順 1　[ポリシー（Policies）] > [SSL] を選択します。

[SSL ポリシー（SSL Policy）] ページが表示されます。

手順 2　編集する SSL ポリシーの横にある編集アイコン（ ）をクリックします。

SSL ポリシー エディタが表示され、[ルール（Rules）] タブにフォーカスが移動します。

手順 3　[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。

[ロギング（Logging）] ポップアップ ウィンドウが表示されます。

手順 4　[接続の終了時点でロギングを行う（Log at End of Connection）] を選択して、接続イベントのロギングを有効にします。

手順 5　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、**[Defense Center]** を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、追加アイコン（ ）をクリックすることで、syslog アラート応答を設定できます。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（ ）をクリックすることで、SNMP アラート応答を設定できます。SNMP アラート応答の作成（43-4 ページ）を参照してください。

これらの接続イベントで Defense Center ベースの分析を実行するには、Defense Center にイベントを送信する**必要があります**。しかし、SSL ポリシーのデフォルト アクションによって処理されるトラフィックは、侵入、マルウェア、または検出データの有無についてさらなる検査が行われないことに注意してください。詳細については、Defense Center または外部サーバへの接続のロギング（38-6 ページ）を参照してください。

手順 6　[OK] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

アクセス コントロールの処理に基づく接続のロギング

ライセンス: 任意（Any）

アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法が提供されます。クリティカルな接続のみをロギングできるように、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対して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るすべての接続をロギングします。

また、アクセス コントロール ポリシーのデフォルト アクションによって処理されたトラフィックの接続もロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール 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まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。

すべてのアクセス コントロール ルールおよびデフォルト アクションのロギングを無効にしても、接続がアクセス コントロール ルールに一致し、しかも侵入試行、禁止されたファイル、またはマルウェアが含まれている場合、あるいは接続がシステムで復号化され、しかも SSL ポリシーで接続のロギングが有効になっている場合には、接続終了イベントが引き続き Defense Center データベースにロギングされる場合があることに注意してください。

ルールまたはデフォルトのポリシー アクション、および設定した関連するインスペクション オプションによって、ロギング オプションは異なります。詳細については、以下を参照してください。

- アクセス コントロール ルールに一致する接続のロギング（38-18 ページ）
- アクセス コントロールのデフォルト アクションによって処理された接続のロギング（38-20 ページ）

アクセス コントロール ルールに一致する接続のロギング

ライセンス: 任意（Any）

クリティカルな接続のみをロギングするには、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対し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。

ルール アクションおよびそのルールの侵入およびファイルのインスペクション設定によって、ロギング オプションは異なります。アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（38-7 ページ）を参照してください。また、アクセス コントロール ルールに対してロギングを無効にしても、接続が以下に該当する場合は、そのルールに一致する接続の接続終了イベントが引き続き Defense Center データベースにロギングされる場合があることに注意してください。

- 侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合
- SSL ポリシーによって検査され、ログに記録された場合
- 以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合

接続、ファイル、およびマルウェア情報をログに記録するアクセス コントロール ルールを設定する方法：

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　変更するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示され、[ルール（Rules）] タブに焦点が置かれています。

手順 3　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。

アクセス コントロール ルール エディタが表示されます。

手順 4　[ロギング（Logging）] タブを選択します。

[ロギング（Logging）] タブが表示されます。

手順 5　接続の開始/終了時点でのロギングを示す [接続開始時にロギング（Log at Beginning of Connection）] または [接続終了時にロギング（Log at End of Connection）] を選択します。

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。

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。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、ブロック ルールの接続開始イベントのみをログに記録できます。

また、モニタ ルールの目的は一致するトラフィックをロギングすることなので、Defense Center データベースへの接続終了ロギングは自動的に有効になっており、無効にできないことに注意してください。詳細については、接続の開始または終了のロギング（38-5 ページ）を参照してください。

手順 6　接続に関連しているファイル イベントとマルウェア イベントをすべてログに記録するかどうか指定するには、[ログ ファイル（Log Files）] チェック ボックスを使用します。

ユーザがファイル ポリシーをルールに関連付けてファイル制御または AMP を実行すると、システムはこのオプションを自動的に有効にします。Cisco 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。許可された接続のファイルおよびマルウェア イベント ロギングの無効化（38-10 ページ）を参照してください。

手順 7　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、[**Defense Center**] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

接続イベントで Defense Center ベースの分析を実行するには、データベースにイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング（38-6 ページ）を参照してください。

手順 8　[保存(Save)] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用(12-17 ページ) を参照してください。

アクセス コントロールのデフォルト アクションによって処理された接続のロギング

ライセンス:任意(Any)

アクセス コントロール ポリシーのデフォルト アクションによって処理されたトラフィックの接続をロギングできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール 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まります(トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く)。ネットワーク トラフィックに対するデフォルトの処理とインスペクションの設定(12-8 ページ)を参照してください。

ポリシーのデフォルト アクションによって処理された接続のメカニズムとオプションは、次の表で示すように、個々のアクセス コントロール ルールによって処理された接続のロギング オプションとほとんど同じです。つまり、ブロックされたトラフィックを除き、接続の開始と終了をログに記録でき、接続イベントを Defense Center データベース、または外部の syslog や SNMP トラップ サーバに送信できます。

表 38-4　アクセス コントロールのデフォルト アクションのロギング オプション

デフォルト アクション	比較対象	参照先
アクセス コントロール:すべてのトラフィックをブロック(Access Control: Block All Traffic)	ブロック ルール	ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて(38-8 ページ)
アクセス コントロール:すべてのトラフィックを信頼(Access Control:Trust All Traffic)	信頼ルール	信頼されている接続のロギングについて(38-8 ページ)
侵入防御(Intrusion Prevention)	関連付けられた侵入ポリシーを持つ許可ルール	許可された接続のロギングについて(38-9 ページ)
ネットワーク検出のみ(Network Discovery Only)	関連付けられた侵入ポリシーを持たない許可ルール	

しかし、アクセス コントロール ルールによって処理された接続のロギングとデフォルト アクションによって処理された接続のロギングにはいくつかの違いがあります。

- デフォルト アクションにはファイル ロギング オプションはありません。デフォルト アクションを使用して、ファイル制御または AMP を実行できません。
- 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**。これは、接続データをログに記録する必要のない、侵入検知および防御のみを行う展開で役立ちます。

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。

デフォルト アクションに対してロギングを無効にしても、接続が以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合、または SSL ポリシーによって検査およびロギングされた場合は、そのルールに一致する接続の接続終了イベントが引き続き Defense Center データベースにロギングされる場合があることに注意してください。

アクセス コントロールのデフォルト アクションによって処理されたトラフィックの接続をログに記録するには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　変更するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示され、[ルール（Rules）] タブに焦点が置かれています。

手順 3　[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。

[ロギング（Logging）] ポップアップ ウィンドウが表示されます。

手順 4　接続の開始/終了時点でのロギングを示す [接続開始時にロギング（Log at Beginning of Connection）] または [接続終了時にロギング（Log at End of Connection）] を選択します。

パフォーマンスを最適化するためには、これらの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。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。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、[すべてのトラフィックをブロック（Block All Traffic）] デフォルト アクションの接続開始イベントのみをログに記録できます。

手順 5　接続イベントの送信先を指定します。次の選択肢があります。

- 接続イベントを Defense Center に送信する場合は、**[Defense Center]** を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。オプションで、syslog アラート応答を追加するには、追加アイコン（  ）をクリックします。Syslog アラート応答の作成（43-5 ページ）を参照してください。
- イベントを SNMP トラップ サーバに送信する場合は、[SNMP トラップ（SNMP Trap）] を選択し、ドロップダウンリストから SNMP アラート応答を選択します。オプションで、追加アイコン（  ）をクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成（43-4 ページ）を参照）。

接続イベントで Defense Center ベースの分析を実行するには、データベースにイベントを送信する**必要があります**。詳細については、Defense Center または外部サーバへの接続のロギング（38-6 ページ）を参照してください。

手順 6　[保存（Save）] をクリックして、ポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

接続で検出された URL のロギング

ライセンス：FireSIGHT

HTTP トラフィックで、接続終了イベントのログを Defense Center データベースに記録する場合、システムはセッション中にモニタ対象のホストが要求した URL を記録します。

デフォルトでは、システムは URL の最初の 1024 文字を接続ログに保管します。ただし、URL ごとに最大 4096 文字を保管するようにシステムを設定して、モニタ対象のホストが要求する完全な URL が取り込まれるようにすることができます。または、アクセスされた個々の URL を知る必要がない場合は、保管する文字数をゼロに設定して、URL の保管を無効にすることもできます。ネットワーク トラフィックによっては、URL の保管を無効にするか、あるいは保管する URL の文字数を制限すると、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 のロギングを無効にしても、URL フィルタリングには影響しません。アクセス コントロール ルールにより、要求された URL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々の URL を記録しないだけです。詳細については、URL のブロッキング（16-10 ページ）を参照してください。

保存する URL の文字数をカスタマイズするには、次の手順を実行します。

アクセス：Admin/Access Admin/Network Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

手順 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

手順 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

手順 4　[全般設定（General Settings）] の横にある編集アイコン（）をクリックします。

[全般設定（General Settings）] ポップアップ ウィンドウが表示されます。

手順 5　**接続イベントで保存する URL の最大文字数**を入力します。

0 ～ 4096 の値を指定できます。保管する文字数をゼロにすると、URL フィルタリングを無効にすることなく URL の保管が無効になります。

手順 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

手順 7　[保存（Save）] をクリックして、ポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。