



侵入ポリシーとファイルポリシーを使用したアクセス制御

次の各トピックでは、侵入ポリシーとファイルポリシーを使用するようにアクセスコントロールポリシーを設定する方法について説明します。

- [ディープインスペクションについて, 1 ページ](#)
- [アクセスコントロールトラフィック処理, 2 ページ](#)
- [ファイルインスペクションおよび侵入インスペクションの順序, 4 ページ](#)
- [ファイル制御およびマルウェア保護のためのアクセスコントロールルールの設定, 5 ページ](#)
- [侵入防御のためのアクセスコントロールルールの設定, 7 ページ](#)

ディープインスペクションについて

侵入ポリシーとファイルポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイルポリシーは、システムのファイル制御と AMP for Firepower の機能を管理します。

アクセスコントロールはディープインスペクションの前に発生し、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のデフォルトアクションによって、侵入ポリシーおよびファイルポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイルポリシーをアクセスコントロールルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。



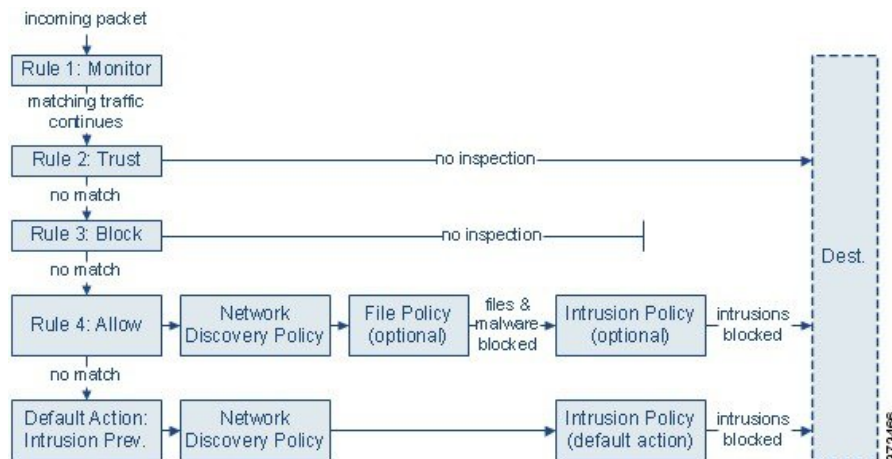
(注) デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセスコントロールルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

システムは、AMP クラウドからエンドポイント向け AMP データを受信し、このデータを任意の AMP for Firepower データと一緒に表示できます。

アクセスコントロールトラフィック処理

アクセスコントロールルールは、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を提供します。システムは、指定した順にアクセスコントロールルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワークトラフィックを処理します。アクセスコントロールルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致したトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

次の図は、4つの異なるタイプのアクセスコントロールルールとデフォルトアクションを含むアクセスコントロールポリシーによって制御されている、インラインの侵入防御と AMP for Firepower の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の3つのアクセスコントロールルール（モニタ、信頼およびブロック）は一致するトラフィックを検査できません。モニタルールはネットワークトラフィックの追跡とログングを行いますますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。信頼ルールおよびブロックルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセスコントロールルールに照合されます。

ポリシー内の4番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ：ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリデータの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的にディスカバリを有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可しても、ディスカバリデータ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニタされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。
- **AMP for Firepower とファイル制御：ファイルポリシー**：システムは、トラフィックがディスカバリによって検査された後、トラフィックの禁止ファイルやマルウェアを検査できます。AMP for Firepower は、PDF、Microsoft Office 文書など多数のファイルタイプに潜むマルウェアを検出し、オプションでブロックできます。部門がマルウェアファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイルタイプの伝送についてネットワークトラフィックをモニタし、ファイルをブロックまたは許可することができます。
- **侵入防御：侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。
- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブブロックルール（この図には表示されていません）には、許可ルールと同じインスペクションオプションがあります。これにより、あるユーザが警告ページをクリックスルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

ポリシー内のモニタ以外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は、デフォルトアクションによって処理されます。このシナリオでは、デフォルトアクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションが割り当てられている場合もあります。システムはデフォルトアクションによって許可されたトラフィックに対しディスカバリデータおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できない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ファイルポリシーを関連付けることはできません。



- (注) 場合によっては、接続がアクセスコントロールポリシーによって分析される場合、システムはトラフィックを処理するアクセスコントロールルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

ファイルインスペクションおよび侵入インスペクションの順序

アクセスコントロールポリシーで、複数の許可ルールとインタラクティブブロックルールを異なる侵入ポリシーおよびファイルポリシーに関連付けて、インスペクションプロファイルをさまざまなタイプのトラフィックに照合できます。



(注) 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセスコントロールのデフォルトアクションにファイルポリシーを関連付けることはできません。

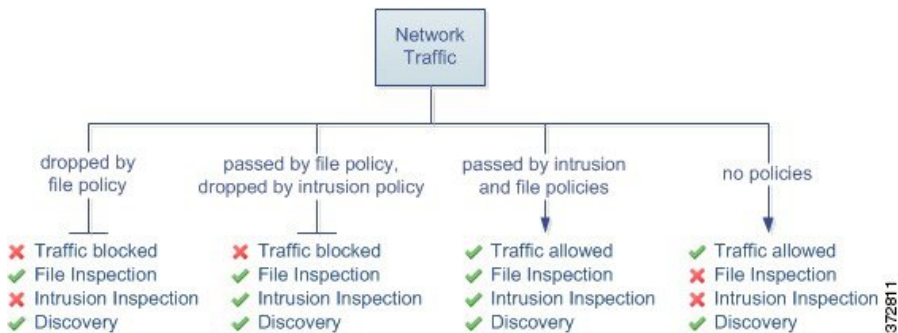
同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブブロックルールに一致する接続の場合：

- ファイルポリシーがない場合、トラフィックフローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィックフローはファイルポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます。



ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセスコントロールルール、またはユーザによりバイパスされた「インタラクティブブロック」アクセスコントロールルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイルポリシーの両方が1つのアクセスコントロールルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィックフローを図に示しています。



372811

アクセスコントロールルールによって処理される単一接続の場合、ファイルインスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイルポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェアインスペクションおよびブロッキングよりも優先されます。

たとえば、アクセスコントロールルールで定義された特定のネットワークトラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされたPDFのマルウェアインスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセスコントロールポリシーを作成し、それを侵入ポリシーとファイルポリシーの両方に関連付けます。ファイルポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含むPDFも検査およびブロックします。

- まず、システムはファイルポリシーで指定された単純なタイプマッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェアインスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされたPDFに対するマルウェアクラウドルックアップを実行します。マルウェアの性質を持つPDFはすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセスコントロールルールに関連付けられている侵入ポリシーを使用して、ファイルポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。



(注) ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

ファイル制御およびマルウェア保護のためのアクセスコントロールルールの設定

アクセスコントロールポリシーは、複数のアクセスコントロールルールをファイルポリシーに関連付けることができます。ファイルインスペクションを許可アクセスコントロールルールまたはインタラクティブブロックアクセスコントロールルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクションプロファイルがネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイルポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントをFirepower Management Center データベースに自動的にロギングします。ログファ

イルまたはマルウェア イベントが必要ない場合は、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。

また、システムは、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かかわらず、関連付けられた接続の終了を Firepower Management Center データベースにロギングします。

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

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 (ファイル制御) マルウェア (AMP)	保護 (ファイル制御) マルウェア (AMP)	任意 (Any)	任意 (Any)	Admin/Access Admin/Network Admin



注意

[ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] を選択、[ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] ルールで [ファイルの保存 (Store files)] または無効化、または [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)] ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE)]、[動的分析 (Dynamic Analysis)]、または [ローカルマルウェア分析 (Local Malware Analysis)]) またはファイルの保存オプション ([マルウェア (Malware)]、[不明 (Unknown)]、[正常 (Clean)]、または [カスタム (Custom)]) と結合する最初のファイルルールを追加または最後のファイルルールを削除すると、設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作](#)を参照してください。

はじめる前に

- AMP を含むファイル制御をアクセスコントロールルールで実行するためには、[適応型プロファイルの設定](#) で説明されているように、アダプティブプロファイルを有効にする必要があります。

手順

- ステップ 1 アクセス コントロール ルール エディタで、[許可 (Allow)]、[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)] の [アクション (Action)] を選択します。
- ステップ 2 [インスペクション (Inspection)] タブをクリックします。
- ステップ 3 アクセス コントロール ルールに一致するトラフィックを検査する場合は [マルウェア ポリシー (Malware Policy)] (ファイル ポリシー) を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [なし (None)] を選択します。
- ステップ 4 (オプション) [ロギング (Logging)] タブをクリックし、[ログ ファイル (Log Files)] チェック ボックスをオフにして、一致する接続のファイルまたはマルウェア イベントのロギングを無効にします。
(注) シスコでは、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。
- ステップ 5 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。

侵入防御のためのアクセス コントロール ルールの設定

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセスコントロールルールまたはインタラクティブブロックアクセスコントロールルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セットを使用します。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。



ヒント

システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを強く推奨します。少なくとも、デフォルトセットにあるデフォルトの変数を変更します。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

Firepower システムには複数の侵入ポリシーが付属しています。システム提供の侵入ポリシーを使用することで、Cisco Talos Security Intelligence and Research Group (Talos) の経験を活用できます。これらのポリシーでは、Talos が侵入ルールおよびプリプロセッサルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタムポリシーのベースとして使用できます。カスタムポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。

接続イベントおよび侵入イベントのロギング

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すると、侵入イベントを生成し、そのイベントを Firepower Management Center に保存します。また、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、侵入が発生した接続の終了を Firepower Management 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の設定と侵入ポリシー

ユーザが独自に作成するカスタム侵入ポリシーに加え、初期インラインポリシーと初期パッシブポリシーの2つのカスタムポリシーがシステムで用意されています。これらの2つの侵入ポリシーは、ベースとして **Balanced Security and Connectivity** 侵入ポリシーを使用します。両者の唯一の相違点は、[インライン時にドロップ (Drop When Inline)] 設定です。インラインポリシーではドロップ動作が有効化され、パッシブポリシーでは無効化されています。

1つのアクセスコントロールポリシーで使用可能な固有の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有のペアはすべて、1つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの許可ルールおよびインタラクティブブロックルール（およびデフォルトアクション）と関連付けることができますが、ターゲットデバイスが設定されたとおりに検査を実行するのに必要なリソースが不足している場合は、アクセスコントロールポリシーを展開できません。

侵入防御を実行するアクセスコントロールルールの設定

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

**注意**

アクセスコントロールポリシーによって使用される侵入ポリシーの総数の変更 設定の変更を展開すると **Snort** プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort®の再起動によるトラフィックの動作](#)を参照してください。現在使用されていない侵入ポリシーを追加するか、侵入ポリシーの最後のインスタンスを削除することで、侵入ポリシーの総数を変更します。アクセスコントロールルールで侵入ポリシーをデフォルトのアクションまたはデフォルトの侵入ポリシーとして使用できます。

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、新しいルールを作成するか、既存のルールを編集します。[アクセスコントロールルールのコンポーネント](#)を参照してください。
- ステップ 2** ルールアクションが [許可 (Allow)]、[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)] に設定されていることを確認します。
- ステップ 3** [削除インスペクション タブ] を選択します。
- ステップ 4** システムによって提供されるまたはカスタムの侵入ポリシーを選択するか、またはアクセスコントロールルールに一致するトラフィックに対する侵入インスペクションを無効にするには [なし (None)] を選択します。
- ステップ 5** 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット (Variable Set)] ドロップダウン リストから値を選択します。
- ステップ 6** [保存 (Save)] をクリックしてルールを保存します。
- ステップ 7** [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。

