



アクセスコントロールルール

次の各トピックでは、アクセスコントロールルールの設定方法について説明します。

- [アクセスコントロールルールの概要 \(1 ページ\)](#)
- [アクセス制御ルール カテゴリの追加 \(8 ページ\)](#)
- [アクセスコントロールルールの作成および編集 \(9 ページ\)](#)
- [アクセスコントロールルールの有効化と無効化 \(11 ページ\)](#)
- [アクセスコントロールルールの配置 \(12 ページ\)](#)
- [アクセスコントロールルールのアクション \(13 ページ\)](#)
- [アクセスコントロールルールのコメント \(16 ページ\)](#)

アクセスコントロールルールの概要

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きめ細かい制御方法が提供されます。

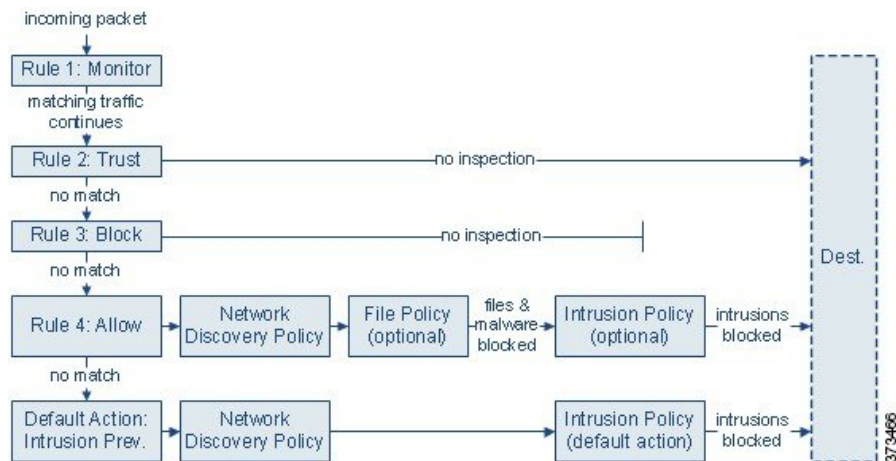


- (注) アクセスコントロールルールがネットワークトラフィックを評価する前に、プレフィルタ評価/8000 シリーズ高速パス、セキュリティインテリジェンスのフィルタリング、SSL インспекション、ユーザの識別、および一部の復号と前処理が発生します。

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。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニタ、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、 익스プロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセスコントロールルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- ルール1：モニタ**はトラフィックを最初に評価します。モニタールールはネットワークトラフィックを追跡してログに記録しますが、トラフィックフローには影響しません。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、許可するか拒否するかを決定します。
- ルール2：信頼**はトラフィックを2番目に評価します。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宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しないトラフィックは、引き続き次のルールと照合されます。
- ルール3：ブロック**はトラフィックを3番目に評価します。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ブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- ルール4：許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- デフォルトアクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。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を割り当てることもあります。(デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。)

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によって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザーデータについてネットワーク検出ポリシーによるインスペクションの対象になります。検出は明示的には有効にしません、拡張したり無効にしたりすることができます。ただし、トラフィックを許可することで、検出データの収

集が自動的に保証されるものではありません。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、ディスクバリアを実行します。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、または SSL インスペクションが設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセスコントロールルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、暗号化ペイロードの侵入およびファイル検査を、システムは無効化します。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。

アプリケーション制御に関する推奨事項

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーションアクセスを許可またはブロックするには、アクセスコントロールルールで**ポート**(選択された宛先ポート)条件を使用します。

たとえば、インターネット(安全性が低い)から内部ネットワーク(安全性が高い)への ICMP トラフィックを許可します。

- ユーザグループによってアクセスされるアプリケーションを許可またはブロックするには、アクセスコントロールルールで**アプリケーション**条件を使用します。

たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。



(注) アクセスコントロールルールを適切に設定しないと、ブロックする必要があるトラフィックを含め、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセスコントロールリスト内の順位を低くする必要があります。

特定の条件(ネットワークや IP アドレスなど)を使用するアクセスコントロールルールは、一般的な条件(アプリケーションなど)を使用するルールの前にオーダーする必要があります。オープンシステム相互接続(OSI)モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および3(物理、データリンク、およびネットワーク)の条件を持つルールは、アクセスコントロールルールで最初に注文する必要があります。レイヤ5、6、および7(セッション、プレゼンテーション、およびアプリケーション)の条件は、アクセスコントロールルールの後で順序付ける必要があります。OSIモデルの詳細については、こちらの [Wikipedia の記事](#) を参照してください。

次の表に、アクセスコントロールルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	Users	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート (SSH など) を使用する場合の、安全性の低いネットワークから安全性の高いネットワークへのアプリケーション	お客様の選択 (この例では [許可 (Allow)])	任意 (Any)	任意 (Any)	設定しない	使用可能なポート : SSH [選択した宛先ポート (Selected Destination Port)] に追加	任意 (Any)	ISE/ISE-PIC でのみ使用。	任意 (Any)
アプリケーションがポートを使用していない場合 (ICMP など)、安全性の低いネットワークへのアプリケーション	お客様の選択 (この例では [許可 (Allow)])	任意 (Any)	任意 (Any)	設定しない	選択された宛先ポートプロトコル : ICMP タイプ : Any	設定しない	ISE/ISE-PIC でのみ使用。	任意 (Any)
ユーザグループによるアプリケーションアクセス	お客様の選択 (この例では [ブロック (Block)])	お客様の選択	ユーザグループ (この例では契約業者グループ) を選択。	アプリケーションの名前 (この例では [Facebook]) を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

アクセスコントロールルールの管理

アクセスコントロールポリシーエディタの[ルール (Rules)]タブでは、編集中のポリシーのアクセスコントロールルールの追加、編集、分類、検索、移動、有効化、無効化、削除、その他の管理が行えます。

ポリシーエディタでは、各アクセスコントロールルールに対してルールの名前、条件の概要、ルールアクションが表示され、さらにルールのインスペクションオプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- 侵入ポリシー オプション (🛡️)
- ファイルポリシー オプション (📁)
- セーフサーチ オプション (🔒)
- YouTube EDU オプション (📧)
- ロギング オプション (📄)
- 発信元クライアント オプション (📡)
- コメント (💬)
- 警告 (⚠️)
- エラー (❗)
- 重要な情報 (ℹ️)

無効なルールはグレー表示され、ルール名の下に[(無効) ((disabled))] というマークが付きます。

ルールを作成または編集するには、アクセスコントロールルールエディタを使用します。次の操作を実行できます。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。



- (注) アクセスコントロールルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセスコントロールポリシーインターフェイスにはルールに対する強力な警告およびエラーのフィードバックシステムがあります。

関連トピック

[アクセスコントロールルールのコンポーネント](#) (6 ページ)

[カスタムユーザロールの作成](#)

[ルールのパフォーマンスに関するガイドライン](#)

アクセスコントロールルールのコンポーネント

一意の名前に加え、各アクセスコントロールルールには次の基本コンポーネントがあります。

状態 (State)

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

アクセスコントロールポリシー内の各ルールには、1から始まる番号が付きます。ポリシー継承を使用する場合、ルール1は再外部ポリシーの1番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。モナルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセスコントロールルールの整理に役立つように、アクセスコントロールポリシーには、システムで用意されている2つのルールセクションとして「必須 (Mandatory)」と「デフォルト (Default)」があります。アクセスコントロールルールをさらに細かく整理するため、「必須 (Mandatory)」セクション内と「デフォルト (Default)」セクション内にカスタムルールカテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須 (Mandatory)」セクションと「デフォルト (Default)」セクションの間にネストされます。

条件 (Conditions)

条件は、ルールで処理する特定のトラフィックを指定します。条件には単純なものと複雑なものがあり、ライセンスによって用途が異なります。

操作 (Action)

ルールのアクションによって、一致したトラフィックの処理方法が決まります。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。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行されません。

インスペクション (Inspection)

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のもは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1つのルールに一致するトラフィックのレコードを1つ保持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システムログ (Syslog) または SNMP トラップサーバに記録できます。

説明

アクセスコントロールルールで変更を保存するたびに、コメントを追加できます。

関連トピック

- [ルールのパフォーマンスに関するガイドライン](#)
- [アクセスコントロールルールの管理 \(5 ページ\)](#)
- [アクセスコントロールルールの作成および編集 \(9 ページ\)](#)
- [ルール条件タイプ](#)
- [アクセスコントロールルールのアクション \(13 ページ\)](#)
- [ディープインスペクションについて](#)
- [接続のロギングのベストプラクティス](#)
- [アクセスコントロールルールのコメント \(16 ページ\)](#)

アクセスコントロールルールの順序

アクセスコントロールポリシー内の各ルールには、1から始まる番号が付きます。システムは、ルール番号の昇順で先頭から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。モニタールール（トラフィックをログに記録するが、トラフィックフローには影響しないルール）を除き、いずれかのルールとトラフィックが一致した後、システムは優先順位の低い追加ルールに対してトラフィックの評価を継続しません。

アクセスコントロールルールの整理に役立つように、アクセスコントロールポリシーには、システムで用意されている2つのルールセクションとして「必須 (Mandatory)」と「デフォルト (Default)」があります。さらに細かく整理するため、「必須 (Mandatory)」セクション内や「デフォルト (Default)」セクション内にカスタムルールカテゴリを作成することができます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須 (Mandatory)」ルールセクションと「デフォルト (Default)」ルールセクションの間にネストされます。ルール1は、現在のポリシーではなく、最外部ポリシーの1番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセスコントロールポリシーの変更を許可する定義済みユーザーロールによって、ルールのカテゴリ内またはカテゴリ間でアクセスコントロールルールを移動および変更することもできます。しかし、ユーザーがルールを移動および変更することを制限するには、カスタムロールを作成できます。アクセスコントロールポリシーの変更権限が割り当てられているユーザーは、制限なく、カスタムカテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。



ヒント

アクセスコントロールルールの順序を適切に設定することで、ネットワークトラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものです。ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

関連トピック

[ルールの順序指定のガイドライン](#)

アクセス制御ルール カテゴリの追加

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

アクセスコントロールポリシーの必須ルールセクションとデフォルトルールセクションをカスタムカテゴリに分割できます。カテゴリを作成した後は、そのカテゴリの削除と名前の変更に加え、カテゴリへのルールの挿入、ルールの削除、カテゴリ内またはカテゴリ間のルールの移動はできますが、カテゴリ自体の移動はできません。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

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、[カテゴリの追加 (Add Category)] をクリックします。
- ヒント** ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[新規カテゴリの挿入 (Insert new category)] を選択することもできます。
- ステップ 2** 名前を入力します。
- ステップ 3** [挿入 (Insert)] ドロップダウンリストから、カテゴリを追加する先を選択します。
- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内 (Into Mandatory)] または [デフォルトルール内 (into Default)] を選択します。
 - 既存のカテゴリの上に挿入するには、[カテゴリの上 (above category)] を選択した後、カテゴリを選択します。
 - アクセス制御ルールの上または下に挿入するには、[ルールの上 (above rule)] または [ルールの下 (below rule)] を選択した後、既存のルール番号を入力します。
- 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。

次のタスク

- 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。

アクセスコントロールルールの作成および編集

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)	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には、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加 (Add Rule)] をクリックします。
- 既存のルールを編集するには、編集アイコン (✎) をクリックします。

代わりに表示アイコン (🔍) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ2 名前を入力します。

ステップ3 以下のルールコンポーネントを設定するか、デフォルトを受け入れます。

- [有効 (Enabled)] : ルールを有効にするかどうかを指定します。
- [位置 (Position)] : ルールの位置を指定します。[アクセスコントロールルールの順序 \(7 ページ\)](#) を参照してください。
- [アクション (Action)] : ルールの [アクション (Action)] を選択します。[アクセスコントロールルールのアクション \(13 ページ\)](#) を参照してください。
- [条件 (Conditions)] : 追加する条件に対応するタブをクリックします。詳細は、[ルール条件タイプ](#) を参照してください。
- [ディープインスペクション (Deep Inspection)] : 許可ルールおよびインタラクティブロックルールの場合、侵入調査アイコン (🛡️) またはファイルおよびマルウェア調査アイコン (📁) をクリックして、ルールの [インスペクション (Inspection)] オプションを設定します。アイコンが淡色表示の場合、そのタイプのポリシーがルールに選択されていません。詳細については、[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](#) を参照してください。
- [コンテンツの制限 (Content Restriction)] : セーフサーチアイコン (🔒) または YouTube EDU アイコン (🎓) をクリックして、ルールエディタの [アプリケーション (Applications)] タブでコンテンツ制限設定を行います。アイコンが淡色表示の場合、ルールに対してコンテンツ制限は無効になっています。詳細については、[コンテンツ制限について](#) を参照してください。
- [ロギング (Logging)] : アクティブな (青の) ロギングアイコン (📄) をクリックして、[ロギング (Logging)] オプションを指定します。アイコンが淡色表示の場合、接続ロギングがそのルールで無効になっています。詳細については、[接続のロギングのベストプラクティス](#) を参照してください。
- [コメント (Comments)] : コメント列の数字をクリックして、[コメント (Comments)] を追加します。数字は、ルールにすでに含まれているコメントの数を示します。詳細については、[アクセスコントロールルールのコメント \(16 ページ\)](#) を参照してください。

ステップ4 ルールを保存します。

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。

次のタスク

- 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。

関連トピック

[ルールのパフォーマンスに関するガイドライン](#)

アクセスコントロールルールの有効化と無効化

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

アクセスコントロールルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。アクセスコントロールポリシーのルールリストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。



ヒント また、ルールエディタを使用してアクセスコントロールルールを有効化または無効化することもできます。

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、ルールを右クリックし、ルールの状態を選択します。

代わりに表示アイコン (🔍) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ2 [保存 (Save)]をクリックします。

次のタスク

- 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。

関連トピック

[アクセスコントロールルールのコンポーネント](#) (6 ページ)

アクセスコントロールルールの配置

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

既存のルールは、アクセスコントロールポリシー内で移動できますが、アクセスコントロールポリシー間では移動できません。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。



ヒント 複数のルールを一度に移動するには、移動するルールを選択し、右クリックメニューを使用してカットアンドペーストします。

手順

ステップ 1 アクセス制御ルール エディタには、次のオプションがあります。

- 新しいルールを追加する場合は、[挿入 (Insert)] ドロップダウンリストを使用します。
- 既存のルールを編集する場合、[移動 (Move)] をクリックします。

ステップ 2 ルールを移動またはルールを挿入する場所を選択します。

- [必須に挿入 (into Mandatory)] または [デフォルトに挿入 (into Default)] を選択します。
- [カテゴリに挿入 (into Category)] を選択して、ユーザ定義カテゴリを選択します。
- [ルールの上 (above rule)] または [ルールの下 (below rule)] を選択してから、適切なルール番号を入力します。

ステップ 3 [保存 (Save)] 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。

次のタスク

- 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。

アクセスコントロールルールのアクション

アクセスコントロールルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。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。

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は、モニタアクセスコントロールルール以外のどの条件にも一致しない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モニタアクション

モニタ アクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わりに、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタルール以外の一致する最初のルールが、トラフィックフローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルトアクションを使用します。

モニタルールの主な目的はネットワークトラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィック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、接続はログに記録されます。



- (注) ローカル内トラフィックがレイヤ3展開のモニタルールに一致する場合、そのトラフィックはインスペクションをバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で[ローカルルータトラフィックの検査 (Inspect Local Router Traffic)] を有効にします。

関連トピック

[モニタされた監視接続のロギング](#)

アクセスコントロールルールの信頼アクション

[信頼 (Trust)] アクションは、ディープインスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID条件およびレート制限の対象です。

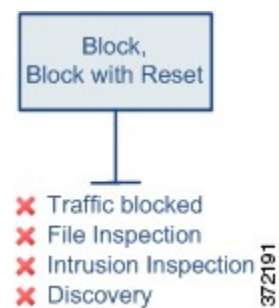


関連トピック

[信頼されている接続のロギング](#)

アクセスコントロールルールのブロックアクション

ブロックアクションおよびリセットしてブロックアクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。



[HTTP 応答 (HTTP response)] ページに一致する Web 要求を除き、リセットルールを持つブロックが接続をリセットします。これは、システムが Web 要求をブロックするときに表示されるように設定した応答ページは、接続がすぐにリセットされた場合は表示できないためです。詳細については、[HTTP 応答ページとインタラクティブなブロッキング](#)を参照してください。

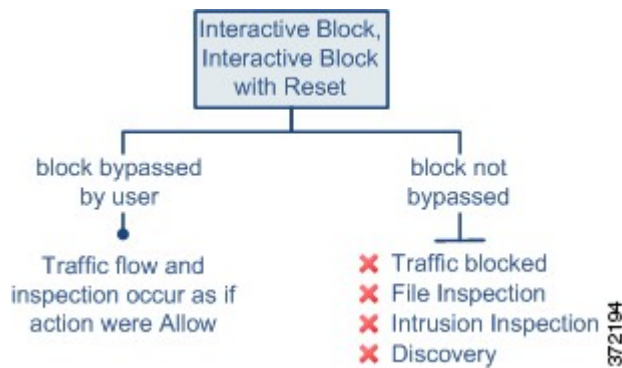
関連トピック

[ブロックされた接続のロギング](#)

[HTTP 応答ページについて](#)

アクセスコントロールルールインタラクティブブロックアクション

詳細については、[HTTP 応答ページとインタラクティブなブロッキング](#)を参照してください。



ユーザがブロックをバイパスしている場合、ルールは許可ルールを模倣します。したがって、インタラクティブブロックルールをファイルポリシーと侵入ポリシーに関連付けることができるため、一致するトラフィックもネットワーク検出の対象となります。

ユーザがブロックをバイパスしない（できない）場合は、ルールはブロックルールを模倣します。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。

インタラクティブブロックを有効にした場合は、ブロックされているすべての接続をリセットできません。これは、接続がすぐにリセットされた場合は応答ページを表示できないためです。[リセットしてインタラクティブブロック（Interactive Block with reset）]アクションを（非インタラクティブに）Web以外のすべてのトラフィックをリセットしてブロックしても、Web要求についてはインタラクティブブロックは有効になっています。

詳細については、[HTTP 応答ページとインタラクティブなブロッキング](#)を参照してください。

関連トピック

[許可された接続のロギング](#)

[TLS/SSL ルールのブロックアクション](#)

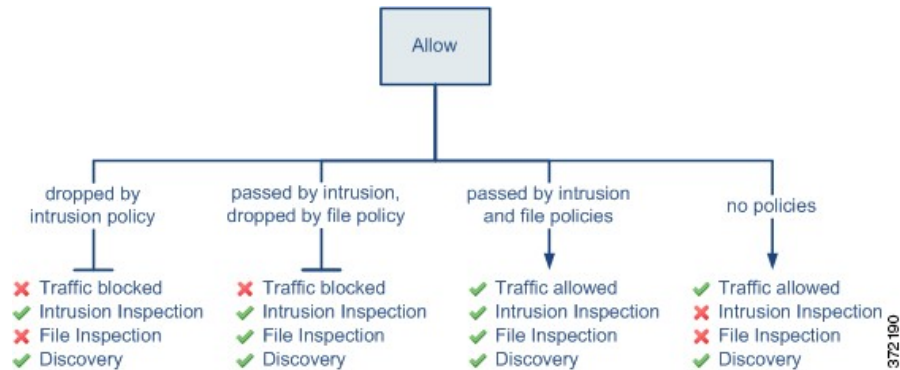
アクセスコントロールルールの許可アクション

[許可（Allow）]アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワークトラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。
- ファイルポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザが特定のアプリケーションプロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ネットワークベースの高度なマルウェア保護（AMP）もファイルポリシーを使用して実行できます。ネットワーク向け AMP はファイルのマルウェアを調べ、検出したマルウェアを設定に応じてブロックします。

下の図は、許可ルールの条件（またはユーザによりバイパスされるインタラクティブブロックルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



シンプルにするために、この図では、侵入ポリシーとファイルポリシーの両方がアクセスコントロールルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィックフローを示しています。ただし、どちらか1つだけを設定することも可能です。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が決定します。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が決定します。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可しても、ディスカバリ検査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。また、アプリケーション検出は、暗号化されたセッションに限定されます。

関連トピック

[許可された接続のロギング](#)

アクセスコントロールルールのコメント

アクセスコントロールルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

関連トピック

[アクセスコントロールポリシーの設定の構成](#)

アクセス制御ルールへのコメントの追加

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

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、[コメント (Comments)] タブをクリックします。
- ステップ2** [New Comment] をクリックします。
- ステップ3** コメントを入力し、[OK] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。
- ステップ4** [保存 (Save)] 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。

次のタスク

- 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。

