SCADA の前処理の設定

ネットワーク分析ポリシーに Supervisory Control and Data Acquisition（SCADA）プリプロセッサを設定します。これによりトラフィックに対して、侵入ポリシーで有効になっているルールを使用した検査を実行できるようになります。詳細については、ネットワーク分析ポリシーおよび侵入ポリシーについて（23-1 ページ）を参照してください。

SCADA プロトコルは、製造、水処理、配電、空港、輸送システムなど、工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。FireSIGHT システムは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

注意 カスタム ユーザ ロールを持つ一部のユーザは、標準メニュー パス（[ポリシー（Policies）] > [アクセス制御（Access Control）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）からネットワーク分析ポリシーにアクセスできません。これらのユーザは、侵入ポリシーを介してネットワーク分析ポリシーにアクセスできます（[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] > [ネットワーク分析ポリシー（Network Analysis Policy）]）。カスタム ユーザ ロールの詳細については、カスタム ユーザ ロールの管理（61-56 ページ）を参照してください。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、Modbus または DNP3 プロセッサがその現在の設定で自動的に使用されます。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。詳細については、Modbus キーワード（36-81 ページ）および DNP3 キーワード（36-83 ページ）を参照してください。

詳細については、次の各項を参照してください。

- Modbus プリプロセッサの設定（28-1 ページ）
- DNP3 プリプロセッサの設定（28-3 ページ）
- CIP プリプロセッサの設定（28-5 ページ）

Modbus プリプロセッサの設定

ライセンス：Protection

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、Modbus キーワード（36-81 ページ）を参照してください。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

イベントを生成するには、次の表に示す Modbus プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-23 ページ）を参照してください。

表 28-1　Modbus プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

Modbus プリプロセッサの使用について、ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

Modbus プリプロセッサがモニタするポートを変更するには、次の手順を用いることができます。

Modbus プリプロセッサを設定するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

手順 4　[SCADA プリプロセッサ（SCADA Preprocessors）] の [Modbus の設定（Modbus Configuration）] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Modbus の設定（Modbus Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　オプションで、プリプロセッサが Modbus トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

手順 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

DNP3 プリプロセッサの設定

ライセンス：Protection

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発された SCADA プロトコルです。DNP3 も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。詳細については、DNP3 キーワード（36-83 ページ）を参照してください。

イベントを生成するには、次の表に示す DNP3 プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-23 ページ）を参照してください。

表 28-2　DNP3 プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
145:1	[無効な CRC を記録（Log bad CRC）] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。

DNP3 プリプロセッサの使用について、ネットワークに DNP3 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。詳細については、TCP ストリームの前処理の設定（29-32 ページ）を参照してください。

設定できる DNP3 プリプロセッサ オプションを以下に説明します。

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。各ポートに 0 ～ 65535 の値を指定できます。

無効な CRC を記録（Log bad CRCs）

有効である場合、DNP3 リンク層フレームに含まれているチェックサムが検証されます。無効なチェックサムを含むフレームは無視されます。

無効なチェックサムが検出されたときにイベントを生成するには、ルール 145:1 を有効にします。

DNP3 プリプロセッサを設定するには、以下の手順を実行します。

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

手順 4　[SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の設定（DNP3 Configuration）] を有効にしているかどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[DNP3 の設定（DNP3 Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　オプションで、プリプロセッサが DNP3 トラフィックを検査するポートを変更します。0 ～ 65535 の整数を指定できます。複数のポートを指定する場合はカンマで区切ります。

手順 6　オプションで、[無効な CRC を記録（Log bad CRCs）] チェック ボックスをオンまたはオフにして、DNP3 リンク層フレームに含まれているチェックサムを検証し、無効なチェックサムのフレームを無視するかどうかを指定します。

手順 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、ネットワーク分析ポリシーの編集操作の表を参照してください。

CIP プリプロセッサの設定

ライセンス：Protection

Common Industrial Protocol（CIP）は、産業自動化アプリケーションをサポートするために広く使用されているアプリケーション プロトコルです。EtherNet/IP は、イーサネット ベースのネットワークで使用される CIP の実装です。

CIP プリプロセッサは、TCP または UDP で実行される CIP および ENIP トラフィックを検出し、それを侵入ルール エンジンに送信します。カスタム侵入ルールで CIP および ENIP のキーワードを使用すると、CIP および ENIP トラフィックで攻撃を検出できます。CIP および ENIP のキーワード（36-87 ページ）を参照してください。さらに、アクセス コントロール ルールで CIP および ENIP アプリケーションの条件を指定することによって、トラフィックを制御できます。アプリケーション トラフィックの制御（16-2 ページ）を参照してください。

次の点に注意してください。

- CIP および ENIP アプリケーションを検出し、それらをアクセス コントロール ルールや侵入ルールなどで使用するには、対応するネットワーク分析ポリシーで CIP プリプロセッサを手動で有効にする必要があります。アクセス コントロールのデフォルト ネットワーク分析ポリシーの設定（25-4 ページ）およびネットワーク分析ルールを使用して前処理するトラフィックの指定（25-5 ページ）を参照してください。
- CIP のプリプロセッサ ルールおよび CIP 侵入ルールをトリガーするトラフィックをドロップするには、対応する侵入ポリシーの [インラインの場合ドロップする（Drop when Inline）] オプションが有効になっていることを確認します。インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。
- アクセス コントロール ルールを使用して CIP または ENIP アプリケーション トラフィックをブロックするには、対応するネットワーク分析ポリシーでインライン正規化プリプロセッサおよびその [インライン モード（Inline Mode）] オプションが有効になっていることを確認してください。インライン トラフィックの正規化（29-7 ページ）およびインライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。
- リストするデフォルトの CIP 検出ポート 44818 およびその他のポートを、TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加します。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。
- イベント ビューアには、CIP アプリケーションに対する特別な処理が用意されています。CIP イベントについて（28-7 ページ）を参照してください。

イベントを生成するには、次の表に示す CIP プリプロセッサ ルールを有効にする必要があります。ルールの有効化については、ルール状態の設定（32-23 ページ）を参照してください。

表 28-3　CIP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	ルール メッセージ
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

次のリストで、変更できる CIP プリプロセッサ オプションについて説明します。

ポート

CIP および ENIP トラフィックを検査するポートを指定します。0 ～ 65535 の整数を指定できます。ポート番号が複数ある場合は、カンマで区切ります。

(注)　リストするデフォルトの CIP 検出ポート 44818 およびその他のポートを、TCP ストリームのリスト [ストリームの再構成をどちらのポートでも実行する（Perform Stream Reassembly on Both Ports）] に追加する**必要があります**。ストリーム再構成のオプションの選択（29-30 ページ）を参照してください。

デフォルトの未接続タイムアウト（秒）

CIP 要求メッセージにプロトコル固有のタイムアウト値が含まれておらず、[TCP 接続あたりの未接続な同時要求の最大数（Maximum number of concurrent unconnected requests per TCP connection）] に達した場合は、このオプションで指定した秒数の間、システムがメッセージの時間を測定します。タイマーが満了すると、他の要求用のスペースを確保するために、メッセージが削除されます。0 ～ 360 の整数を指定できます。0 を指定すると、プロトコル固有のタイムアウト値を持たないすべてのトラフィックは、最初にタイムアウトになります。

TCP 接続あたりの未接続な同時要求の最大数（Maximum number of concurrent unconnected requests per TCP connection）

システムが接続を閉じるまで無応答のままにすることができる同時要求の数。1 ～ 10000 の整数を指定できます。

TCP 接続あたりの CIP 接続の最大数（Maximum number of CIP connections per TCP connection）

システムが TCP 接続ごとに許可する同時 CIP 接続の最大数。1 ～ 10000 の整数を指定できます。

CIP プリプロセッサの設定方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して [アクセス コントロール ポリシー（Access Control Policy）] ページを表示し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。

[ネットワーク分析ポリシー（Network Analysis Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合に変更を破棄し、操作を続行するには、[OK] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルで [設定（Settings）] をクリックします。

[設定（Settings）] ページが表示されます。

手順 4　[SCADA プリプロセッサ（SCADA Preprocessors）] の [CIP の設定（CIP Configuration）] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[CIP の設定（CIP Configuration）] ページが表示されます。ページ下部のメッセージには、設定を含むネットワーク分析ポリシー層が示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　この項で説明するオプションを変更できます。

手順 6　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

CIP イベントについて

設計上、セッションごとに 1 回ずつ、同じアプリケーションがアプリケーション ディテクタで検出されてイベント ビューアに表示されます。1 つの CIP セッションでは複数のアプリケーションを別々のパケットに含めることができ、単一の CIP パケットに複数のアプリケーションを格納できます。CIP プリプロセッサは、対応するルールに従ってすべての CIP および ENIP トラフィックを処理し、CIP イベントの表示を次のように制御します。

- アプリケーション プロトコル：**CIP** または **ENIP**
- クライアント：**CIP クライアント**または **ENIP クライアント**
- Web アプリケーション：検出された次のような特定のアプリケーション：
  - トラフィックを許可またはモニタするルールの場合：セッションで検出された最後のアプリケーション プロトコル。

    接続をログに記録するよう設定されたアクセス コントロール ルールが、指定された CIP アプリケーションのイベントを生成しないことがあります。一方、接続をログに記録するよう設定されていないアクセス コントロール ルールが、CIP アプリケーションのイベントを生成することがあります。
  - トラフィックをブロックするルールの場合：ブロックをトリガーしたアプリケーション プロトコル。

    アクセス コントロール ルールが CIP アプリケーションのリストをブロックすると、イベント ビューアに、検出された最初のアプリケーションが表示されます。

次の点に注意してください。

- アクセス コントロール ポリシーのデフォルト アクションである [侵入防御（Intrusion Prevention）] を使用することを推奨します。
- CIP プリプロセッサは、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 [アクセス制御：すべてのトラフィックを信頼（Access Control: Trust All Traffic）] をサポートしていません。このアクションを実行すると、侵入ルールとアクセス コントロール ルールで指定された CIP アプリケーションによりトリガーされたトラフィックがドロップされないなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、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 [アクセス制御：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をサポートしていません。このアクションを実行すると、ブロックされると想定されない CIP アプリケーションがブロックされるなど、望ましくない動作が生じる可能性があるためです。
- CIP プリプロセッサは、CIP アプリケーションのアプリケーション可視性（ネットワーク検出を含む）をサポートしていません。

詳細については、接続およびセキュリティ インテリジェンスのデータ フィールドについて（39-4 ページ）を参照してください。