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（18-1 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。ASA FirePOWER モジュールは、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。

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モジュール 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（30-79 ページ）およびDNP3 キーワード（30-80 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（23-1 ページ）
- DNP3 プリプロセッサの設定（23-3 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（30-79 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（27-22 ページ）を参照してください。

表 23-1　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。

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクセス コントロール ポリシー（Access Control Policy）] の順に選択します。

[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　編集するアクセス 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ページが表示されます。

手順 4　[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] の横にある編集アイコン（）をクリックします。

[ネットワーク分析と侵入ポリシー（Network Analysis and Intrusion Policies）] ポップアップ ウィンドウが表示されます。

手順 5　[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] をクリックします。

[ネットワーク分析ポリシー リスト（Network Analysis Policy List）] ポップアップ ウィンドウが表示されます。

手順 6　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（18-16 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 7　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 8　[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（19-1 ページ）を参照してください。

手順 9　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 10　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（18-16 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（30-80 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（27-22 ページ）を参照してください。

表 23-2　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。

表 23-2　DNP3 プリプロセッサ ルール(続き)

プリプロセッサ ルール GID:SID	説明
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(24-32 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。

手順 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アクセス コントロール ポリシー(Access Control Policy)] の順に選択します。

[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　編集するアクセス 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ページが表示されます。

手順 4　[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] の横にある編集アイコン( )をクリックします。

[ネットワーク分析と侵入ポリシー(Network Analysis and Intrusion Policies)] ポップアップ ウィンドウが表示されます。

手順 5　[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] をクリックします。

[ネットワーク分析ポリシー リスト(Network Analysis Policy List)] ポップアップ ウィンドウが表示されます。

手順 6　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（18-16 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 7　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 8　[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（19-1 ページ）を参照してください。

手順 9　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 10　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 11　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。