



SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

- [SCADA プリプロセッサの概要](#)（1 ページ）
- [SCADA プリプロセッサのライセンス要件](#)（2 ページ）
- [SCADA プリプロセッサの要件と前提条件](#)（2 ページ）
- [Modbus プリプロセッサ](#)（2 ページ）
- [DNP3 プリプロセッサ](#)（5 ページ）
- [CIP プリプロセッサ](#)（7 ページ）
- [S7Commplus プリプロセッサ](#)（12 ページ）

SCADA プリプロセッサの概要



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、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ー、制御、取得します。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、Distributed Network Protocol（DNP3）、Common Industrial Protocol（CIP）、および S7Commplus SCADA プロトコル用のプリプロセッサを提供します。

Modbus、DNP3、CIP、または S7Commplus プリプロセッサが無効になっている、これらのプリプロセッサのいずれかを必要とする侵入ルールを有効にして展開した場合、システムはプリプロセッサを現在の設定で使用しますが、対応する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になったままとなります。

SCADA プリプロセッサのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

SCADA プリプロセッサの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

Modbus プリプロセッサ



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

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。

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。

関連トピック

[SCADA キーワード](#)

Modbus プリプロセッサポートオプション

ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

Modbus プリプロセッサの設定



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

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。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [Policies] > [Access Control] > [Intrusion]、次に [Network Analysis Policies] を選択します。

(注) カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン (Snort 2 Version)] をクリックします。

ステップ 3 編集するポリシーの横にある [編集 (Edit)] (✎) をクリックします。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーションパネルで [設定 (Settings)] をクリックします。

ステップ 5 [SCADA プリプロセッサ (SCADA Preprocessors)] の下の [Modbus の構成 (Modbus Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

ステップ 6 [Modbus の設定 (Modbus Configuration)] の横にある [編集 (Edit)] (✎) をクリックします。

ステップ 7 [ポート (Ports)] フィールドに値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ 8 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、Modbus プリプロセッサルール (GID 144) を有効にします。詳細については、「[侵入ルール状態の設定](#)」および「[Modbus プリプロセッサルール \(4 ページ\)](#)」を参照してください。
- 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

[レイヤの管理](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー](#)

Modbus プリプロセッサルール

次の表に示す Modbus プリプロセッサルールによって イベントを生成し、インライン展開では、違反パケットをドロップします。するには、これらのルールを有効にする必要があります。

表 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。

DNP3 プリプロセッサ



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

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きます。

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。

関連トピック

[DNP3 キーワード](#)

DNP3 プリプロセッサ オプション

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。

無効な CRC を記録 (Log bad CRCs)

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。

ルール 145:1 を有効にすると、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し、オンライン展開では、違反パケットをドロップします。できます。

DNP3 プリプロセッサの設定



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

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。

手順

ステップ1 [ポリシー (Policies)] > [アクセス制御 (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [Policies] > [Access Control] > [Intrusion]、次に [Network Analysis Policies] を選択します。

(注) カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2番目のパスを使用してポリシーにアクセスします。

ステップ2 編集するポリシーの横にある [Snort 2バージョン (Snort 2 Version)] をクリックします。

ステップ3 編集するポリシーの横にある [編集 (Edit)] (✎) をクリックします。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ4 ナビゲーションパネルで [設定 (Settings)] をクリックします。

ステップ5 [SCADA プリプロセッサ (SCADA Preprocessors)] の下の [DNP3 の構成 (DNP3 Configuration)] が無効になっている場合は、[有効化 (Enabled)] をクリックします。

ステップ6 [DNP3 の設定 (DNP3 Configuration)] の横にある [編集 (Edit)] (✎) をクリックします。

ステップ7 ポートの値を入力します。

複数の値を指定する場合は、カンマで区切ります。

ステップ8 [不良 CRC の記録 (Log bad CRCs)] チェックボックスをオンまたはオフにします。

ステップ9 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。を行うには、DNP3 プリプロセッサルール (GID 145) を有効にします。詳細については、[侵入ルール状態の設定](#)、[DNP3 プリプロセッサ オプション \(5 ページ\)](#)、および [DNP3 プリプロセッサルール \(7 ページ\)](#) を参照してください。
- 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

[レイヤの管理](#)

[競合と変更：ネットワーク分析ポリシーと侵入ポリシー](#)

DNP3 プリプロセッサルール

次の表に示すDNP3プリプロセッサルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。するには、これらのルールを有効にする必要があります。

表 2: DNP3 プリプロセッサルール

プリプロセッサルール ID: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。

CIP プリプロセッサ



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

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 (ENIP) 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](#)」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。[アプリケーション条件とフィルタの設定](#)を参照してください。

CIP プリプロセッサのオプション

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。[TCP ストリームのプリプロセス オプション](#) および [カスタム ネットワーク分析ポリシーの作成](#) 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 イベント

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、対応する侵入ルールに従ってすべての CIP と ENIP のトラフィックを処理します。

次の表にイベントビューアに表示される CIP の値を示します。

表 3: CIP イベントフィールドの値

イベント フィールド	表示される値
アプリケーションプロトコル (Application Protocol)	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 (Web Application)]	<p>次に示す特定のアプリケーションを検出しました。</p> <ul style="list-style-type: none"> • トラフィックを許可またはモニターするアクセス制御ルールの場合、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制御ルールが、指定された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、接続をログに記録していないアクセス制御ルールが、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アクセス制御ルールの場合、ブロックされたアプリケーションプロトコル。 アクセス制御ルールが CIP アプリケーションのリストをブロックするときに、検出された最初のアプリケーションが表示されます。

CIP プリプロセッサルール

次の表に示す CIP プリプロセッサルールでイベントを生成するには、それらの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、[侵入ルール状態の設定](#)を参照してください。

表 4: CIP 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	CPNONCONFORMING
148:3	CPCONNECTIONLIMIT
148:4	CIP_REQUEST_LIMIT

CIP プリプロセッサの設定のガイドライン

CIP プリプロセッサを設定するには次の点に注意してください。

- 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 CIP 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。CIP プリプロセッサのオプション (8 ページ)、カスタム ネットワーク分析ポリシーの作成、および TCP ストリームのプリプロセス オプション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 (8 ページ) を参照してください。
- 侵入防御アクションをアクセス コントロール ポリシーのデフォルトのアクションとして使用することをお勧めします。
- 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ります。
- 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ります。
- 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。
- 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、対応するカスタム 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。カスタム ネットワーク分析ポリシーの作成、「デフォルトのネットワーク分析ポリシーの設定」、およびネットワーク分析ルールの設定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」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 (デフォルト設定) ことを確認してください。カスタム ネットワーク分析ポリシーの作成、「デフォルトのネットワーク分析ポリシーの設定」、およびインライン導入でのプリプロセッサによるトラフィックの変更を参照してください。

CIP プリプロセッサの設定



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

始める前に

- CIP ポートとして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。CIP プリプロセッサのオプション (8 ページ)、カスタム ネットワーク分析ポリシーの作成、および TCP ストリームのプリプロセス オプションを参照してください。
- CIP プリプロセッサの設定のガイドライン (9 ページ) の内容についてよく理解しておきます。
- CIP プリプロセッサは、Threat Defense デバイスではサポートされていません。

手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [Policies] > [Access Control] > [Intrusion]、次に [Network Analysis Policies] を選択します。

(注) カスタムユーザロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン (Snort 2 Version)] をクリックします。

ステップ 3 編集するポリシーの横にある [編集 (Edit)] (✎) をクリックします。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ナビゲーションパネルで [設定 (Settings)] をクリックします。

ステップ 5 [SCADA プリプロセッサ (SCADA Preprocessors)] の下の [CIP 設定 (CIP Configuration)] が無効になっている場合は、[有効 (Enabled)] をクリックします。

ステップ 6 CIP プリプロセッサのオプション (8 ページ) で説明するオプションを変更できます。

ステップ 7 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- イベントを生成し、インライン展開では、違反パケットをドロップします。 の場合、CIP 侵入ルールを有効にし、オプションで CIP プリプロセッサルール (GID 148) を有効にします。詳細については、[侵入ルール状態の設定](#)、[CIP プリプロセッサルール \(9 ページ\)](#)、および[CIP イベント \(8 ページ\)](#) を参照してください。
- 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。

S7Commplus プリプロセッサ



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。

S7Commplus プリプロセッサは、S7Commplus トラフィックを検出します。カスタム侵入ルールで S7Commplus キーワードを使用して、S7Commplus トラフィックの攻撃を検出できます。[S7Commplus キーワード](#) を参照してください。

S7Commplus プリプロセッサの設定



(注) このセクションは、Snort 2 プリプロセッサに当てはまります。Snort 3 インспекタの詳細については、<https://www.cisco.com/go/snort3-inspectors> を参照してください。


S7Commplus プリプロセッサは、すべての Threat Defense デバイスでサポートされています。


手順

ステップ 1 [ポリシー (Policies)] > [アクセス制御 (Access Control)]、次に [ネットワーク分析ポリシー (Network Analysis Policy)] をクリックします。または [Policies] > [Access Control] > [Intrusion]、次に [Network Analysis Policies] を選択します。

(注) カスタムユーザーロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン (Snort 2 Version)] をクリックします。

ステップ 3 編集するポリシーの横にある [編集 (Edit)] () をクリックします。

代わりに [表示 (View)] () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- ステップ4** ナビゲーションパネルで [設定 (Settings)] をクリックします。
- ステップ5** [SCADAプリプロセッサ (SCADA Preprocessors)] の下の [S7Commplus設定 (S7Commplus Configuration)] が無効になっている場合は、[有効 (Enabled)] をクリックします。
- ステップ6** 必要に応じて、[S7Commplusの設定 (S7Commplus Configuration)] の横にある [編集 (Edit)] (✎) をクリックし、[s7commplus_ports] を変更して、プリプロセッサが S7Commplus トラフィックを検査するポートを識別します。複数のポートを指定する場合は、カンマで区切ります。
- ステップ7** 最後にポリシーを確定してからこのポリシーで加えた変更を保存するには、[ポリシー情報 (Policy Information)] をクリックし、[変更の確定 (Commit Changes)] をクリックします。
- 変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後にキャッシュされた変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、S7Commplus プリプロセッサルール (GID 149) を有効にします。詳細については、「[侵入ルール状態の設定](#)」を参照してください。
- 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。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。