アプリケーション層プリプロセッサの使用

ネットワーク分析ポリシーにアプリケーション層プリプロセッサを設定します。これにより、侵入ポリシーで有効になっているルールを使った検査に向けてトラフィックが準備されます。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。

アプリケーション層プロトコルにより、同一データをさまざまな方法で表すことができます。シスコは、特定タイプのパケット データを侵入ルール エンジンが分析可能なフォーマットに正規化する、アプリケーション層プロトコル デコーダを提供しています。アプリケーション層プロトコル エンコードを正規化することにより、ルール エンジンでさまざまなデータ形式のパケットに同じコンテンツ関連ルールを効果的に適用し、有意な結果を得ることができます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、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が無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーに関する制約事項（23-13 ページ）を参照してください。

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。

ほとんどの場合、侵入ルールで関連するプリプロセッサ ルールが有効になっていないと、プリプロセッサはイベントを生成しません。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- DCE/RPC トラフィックのデコード（27-2 ページ）では、DCE/RPC プリプロセッサについて説明し、回避の試行を防いで DCE/RPC トラフィックでの異常を検出するようにプリプロセッサを設定する方法を説明します。
- DNS ネーム サーバ応答におけるエクスプロイトの検出（27-16 ページ）では、DNS プリプロセッサについて説明し、DNS ネームサーバ応答における 3 種類のエクスプロイトを検出するようにプリプロセッサを設定する方法について説明します。
- FTP および Telnet トラフィックのデコード（27-20 ページ）では、FTP/Telnet デコーダについて説明し、FTP および Telnet トラフィックを正規化およびデコードするようにデコーダを設定する方法について説明します。

- HTTP トラフィックのデコード(27-34 ページ)では、HTTP デコーダについて説明し、HTTP トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Sun RPC プリプロセッサの使用(27-50 ページ)では、RPC デコーダについて説明し、RPC トラフィックを正規化するようにデコーダを設定する方法について説明します。
- Session Initiation Protocol のデコード(27-52 ページ)では、SIP プリプロセッサを使用して SIP トラフィックをデコードし、SIP トラフィックの異常を検出する方法を説明します。
- GTP コマンド チャネルの設定(27-57 ページ)では、GTP プリプロセッサを使用して、パケット デコーダによって抽出された GTP コマンド チャネル メッセージをルール エンジンに提供する方法について説明します。
- IMAP トラフィックのデコード(27-58 ページ)では、IMAP プリプロセッサを使用して IMAP トラフィックをデコードし、IMAP トラフィックの異常を検出する方法を説明します。
- POP トラフィックのデコード(27-62 ページ)では、POP プリプロセッサを使用して POP トラフィックをデコードし、POP トラフィックの異常を検出する方法を説明します。
- SMTP トラフィックのデコード(27-65 ページ)では、SMTP デコーダについて説明し、SMTP トラフィックをデコードおよび正規化するようにデコーダを設定する方法について説明します。
- SSH プロプロセッサによるエクスプロイトの検出(27-73 ページ)では、SSH 暗号化トラフィック内のエクスプロイトを識別して処理する方法について説明します。
- SSL プリプロセッサの使用(27-77 ページ)では、SSL プリプロセッサを使用して暗号化トラフィックを特定し、そのトラフィックのインスペクションを停止して誤検出を排除する方法について説明します。
- SCADA の前処理の設定(28-1 ページ)では、Modbus および DNP3 プリプロセッサを使用して、対応するトラフィックの異常を検出し、特定のプロトコル フィールドを検査するためにデータを侵入ルール エンジンに提供する方法を説明します。

DCE/RPC トラフィックのデコード

ライセンス: Protection

DCE/RPC プロトコルにより、別々のネットワーク ホスト上のプロセスが、同一ホストに配置されている場合と同様に通信できます。通常、このようなプロセス間通信はホスト間で TCP および UDP 経由で転送されます。TCP 転送では、DCE/RPC が Windows Server Message Block(SMB)プロトコルまたは Samba でさらにカプセル化されることがあります。Samba は、Windows や UNIX/Linux 系のオペレーティング システムから構成される混合環境でプロセス間通信に使用されるオープンソースの SMB 実装です。また、ネットワーク上の Windows IIS Web サーバでは IIS RPC over HTTP が使用されることがあります。IIS RPC over HTTP は、プロキシ TCP により伝送される DCE/RPC トラフィックに、ファイアウォールを介して分散通信を提供します。

DCE/RPC プリプロセッサ オプションとその機能の説明には、Microsoft による DCE/RPC の実装である MSRPC が含まれることに注意してください。SMB のオプションと機能についての説明は、SMB と Samba の両方に当てはまります。

ほとんどの DCE/RPC エクスプロイトは、DCE/RPC サーバ(ネットワーク上の Windows または Samba が稼働している任意のホスト)を対象とした DCE/RPC クライアント要求で発生します。またエクスプロイトはサーバ応答でも発生することがあります。DCE/RPC プリプロセッサは、TCP、UDP、および SMB トランスポートでカプセル化された DCE/RPC 要求と応答を検出します。これには、RPC over HTTP バージョン 1 を使用して TCP により伝送される DCE/RPC も含まれます。プリプロセッサは DCE/RPC データ ストリームを分析し、DCE/RPC トラフィックにおける異常な動作と回避技術を検出します。また、SMB データ ストリームを分析し、異常な SMB 動作と回避技術を検出します。

IP 最適化プリプロセッサによる IP 最適化および TCP ストリーム プリプロセッサによる TCP ストリームの再構成に加えて、DCE/RPC プリプロセッサは、SMB のセグメント化解除と DCE/RPC の最適化も行います。TCP ストリームの前処理の使用（29-22 ページ）および IP パケットの最適化（29-13 ページ）を参照してください。

最後に、DCE/RPC プリプロセッサはルール エンジンで処理できるように DCE/RPC トラフィックを正規化します。特定の DCE/RPC サービス、オペレーション、スタブ データを検出するために DCE/RPC ルールのキーワードを使用する方法については、DCE/RPC キーワード（36-65 ページ）を参照してください。

DCE/RPC プリプロセッサを設定するには、プリプロセッサの機能を制御するグローバル オプションを変更するか、IP アドレスと稼働している Windows または Samba のバージョンによってネットワーク上の DCE/RPC サーバを識別する 1 つ以上のターゲットベース サーバ ポリシーを指定します。

ジェネレータ ID（GID）が 132 または 133 の DCE/RPC プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- グローバル DCE/RPC オプションの選択（27-3 ページ）
- ターゲットベース DCE/RPC サーバ ポリシーについて（27-5 ページ）
- DCE/RPC トランスポートについて（27-6 ページ）
- DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）
- DCE/RPC プリプロセッサの設定（27-13 ページ）

グローバル DCE/RPC オプションの選択

ライセンス：Protection

グローバル DCE/RPC プリプロセッサ オプションは、プリプロセッサの機能を制御します。[到達したメモリ容量（Memory Cap Reached）] オプション以外のこれらのオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。特に [最大フラグメント サイズ（Maximum Fragment Size）] オプションと [再構成しきい値（Reassembly Threshold）] オプションは、ルールが検出する必要がある深さと同じかそれ以上にしてください。詳細については、コンテンツ一致の制約（36-20 ページ）および Byte_Jump と Byte_Test の使用（36-34 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

最大フラグメント サイズ

[最適化の有効化（Enable Defragmentation）] が選択されている場合、DCE/RPC フラグメントの許容最大長を 1514 バイトから 65535 バイトまでの範囲で指定します。これよりも大きなフラグメントの場合、プリプロセッサは処理のためにフラグメントの一部を切り捨て、指定のサイズにしてから最適化を行いますが、実際のパケットは変更されません。空白フィールドの場合、このオプションは無効になります。

再構成しきい値

[最適化の有効化（Enable Defragmentation）] が選択されている場合、0 を指定するとこのオプションは無効になり、1 バイトから 65535 バイトの範囲内の値を指定すると、それが、フラグメント化された DCE/RPC の最小バイト数となります。また該当する場合は、再構成されたパケットをルール エンジンに送信する前にキューに入れるセグメント化 SMB のバイト数が指定されます。低い値を指定すると、早期検出の可能性が高くなりますが、パフォーマンスに悪影響を及ぼす可能性があります。このオプションを有効にする場合は、パフォーマンスの影響をテストしておく必要があります。

最適化の有効化

フラグメント化された DCE/RPC トラフィックを最適化するかどうかを指定します。無効にすると、プリプロセッサは引き続き異常を検出して DCE/RPC データをルール エンジンに送信しますが、フラグメント化された DCE/RPC データでのエクスプロイトを見落とすリスクがあります。

このオプションには、DCE/RPC トラフィックを最適化しないという柔軟性がありますが、ほとんどの DCE/RPC エクスプロイトでは、フラグメント化を利用してエクスプロイトを隠ぺいする試みが行われます。このオプションを無効にすると、ほとんどの既知のエクスプロイトがバイパスされ、検出漏れが大量に発生します。

到達したメモリ容量

プリプロセッサに割り当てられた最大メモリ制限に達したか、またはこの制限を超過したことを検出します。最大メモリ制限に達したか、またはこの制限を超過した場合、プリプロセッサはメモリ キャップ イベントを引き起こしたセッションに関連付けられているすべての保留データを解放し、セッションのそれ以降の部分を無視します。

このオプションのイベントを生成するには、ルール 133:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

SMB セッションの自動検出ポリシー

SMB `Session Setup AndX` 要求および応答に指定されている Windows または Samba のバージョンを検出します。検出されたバージョンが、[ポリシー（Policy）] 設定オプションで設定されている Windows または Samba のバージョンと異なる場合、そのセッションに限り、検出されたバージョンが設定バージョンをオーバーライドします。詳細については、ターゲット ベース DCE/RPC サーバ ポリシーについて（27-5 ページ）を参照してください。

たとえば、[ポリシー（Policy）] に Windows XP を設定した場合に、プリプロセッサが Windows Vista を検出すると、プリプロセッサはそのセッションでは Windows Vista ポリシーを使用します。その他の設定は引き続き有効です。

DCE/RPC トランスポートが SMB ではない場合は（トランスポートが TCP または UDP の場合）、バージョンを検出できず、ポリシーを自動的に設定できません。

このオプションを有効にするには、ドロップダウン リストで次のいずれかを選択します。

- サーバ/クライアント トラフィックでポリシー タイプを検査するには、[クライアント（Client）] を選択します。
- クライアント/サーバ トラフィックでポリシー タイプを検査するには、[サーバ（Server）] を選択します。
- サーバ/クライアント トラフィックとクライアント/サーバ トラフィックの両方でポリシー タイプを検査するには、[両方（Both）] を選択します。

ターゲットベース DCE/RPC サーバ ポリシーについて

ライセンス：Protection

ターゲットベースのサーバ ポリシーを 1 つ以上作成することにより、指定したタイプのサーバが処理するのと同様の方法で DCE/RPC トラフィックを検査するように、DCE/RPC プリプロセッサを設定することができます。ターゲットベースのポリシーの設定では、ネットワーク上の指定ホストで実行されている Windows または Samba のバージョンの識別、トランスポート プロトコルの有効化、DCE/RPC トラフィックをこれらのホストに伝送するポートの指定、その他のサーバ固有のオプションの設定などを行います。

Windows および Samba の DCE/RPC の実装は大きく異なります。たとえば、Windows のすべてのバージョンは、DCE/RPC トラフィックの最適化時に最初のフラグメントの DCE/RPC コンテキスト ID を使用しますが、Samba のすべてのバージョンは、最後のフラグメントのコンテキスト ID を使用します。また、特定の関数呼び出しを識別するために、Windows Vista では最初のフラグメントの opnum（操作番号）ヘッダー フィールドを使用しますが、Samba とその他のすべてのバージョンの Windows では最後のフラグメントの opnum フィールドを使用します。

Windows と Samba の SMB の実装にも、大きな違いがあります。たとえば、Windows は名前付きパイプの操作時に SMB OPEN および READ コマンドを認識しますが、Samba はこれらのコマンドを認識しません。

DCE/RPC プリプロセッサを有効にすると、デフォルトのターゲットベース ポリシーが自動的に有効になります。（任意）異なるバージョンの Windows または Samba を実行している他のホストを対象とするターゲットベース ポリシーを追加できます。追加するには、[ポリシー（Policy）] ドロップダウン リストから適切なバージョンを選択します。デフォルトのターゲットベース ポリシーは、別のターゲットベース ポリシーに含まれていないホストに適用されます。

それぞれのターゲットベース ポリシーで、1 つ以上のトランスポートを有効にして、それぞれの*検出ポート*を指定できます。また、*自動検出ポート*を有効にして指定することもできます。詳細については、DCE/RPC トランスポートについて（27-6 ページ）を参照してください。

その他のターゲットベースのポリシー オプションも設定できます。指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそれを検出するように、プリプロセッサを設定できます。SMB トラフィックでファイルを検出し、検出されたファイルで指定のバイト数のデータを検査するように、プリプロセッサを設定できます。また、SMB プロトコルに関する知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定できます。

各ターゲットベースのポリシーでは次の設定が可能です。

- 1 つ以上のトランスポートを有効にし、それぞれについて*検出ポート*を指定します。
- *自動検出ポート*を有効にして指定します。詳細については、DCE/RPC トランスポートについて（27-6 ページ）を参照してください。
- 指定した 1 つ以上の共有 SMB リソースへの接続が試行された場合にそのことを検出するように、プリプロセッサを設定します。
- SMB トラフィックでファイルを検出し、検出されたファイルで指定された数のバイトを検査するように、プリプロセッサを設定します。
- SMB プロトコルの知識を持つユーザだけが変更すべき拡張オプションを変更できます。このオプションでは、連結された SMB AndX コマンドの数が指定された最大数を超えた場合にそのことを検出するようにプリプロセッサを設定します。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、ターゲット ポリシーに対して設定されているポリシー タイプをセッションごとに自動的にオーバーライドできます。SMB セッ

ションの自動検出ポリシー（27-4 ページ）を参照してください。

DCE/RPC プリプロセッサで SMB トラフィック ファイル検出を有効にする他に、オプションでこれらのファイルを検出してブロックするか、または動的分析のために Collective Security Intelligence クラウド に送信するように、ファイル ポリシーを設定できます。そのポリシー内で、[アクション（Action）] として [ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] を選択し、[アプリケーション プロトコル（Application Protocol）] として [任意（Any）] または [NetBIOS-ssn（SMB）] を選択して、ファイル ルールを作成する必要があります。詳細については、「ファイル ポリシーの作成（37-19 ページ）」と「ファイル ルールの操作（37-20 ページ）」を参照してください。

DCE/RPC トランスポートについて

ライセンス：Protection

各ターゲットベース ポリシーでは、TCP、UDP、SMB、および RPC over HTTP トランスポートのうち 1 つ以上を有効にできます。トランスポートを有効にする場合は、1 つ以上の *検出ポート*（DCE/RPC トラフィックを伝送することがわかっているポート）を指定する必要があります。（任意）*自動検出ポート*を有効にして指定できます。プリプロセッサは、自動検出ポートとして指定されたポートを最初にテストして、そのポートが DCE/RPC トラフィックを伝送しているかどうかを判別し、DCE/RPC トラフィックを検出した場合にのみ処理を続行します。

シスコでは、デフォルトの検出ポート（ウェルノウン ポートまたは各プロトコルで一般に使用されているポート）を使用することを推奨しています。検出ポートを追加するのは、デフォルト以外のポートで DCE/RPC トラフィックを検出した場合だけです。

自動検出ポートを有効にする場合は、エフェメラル ポート範囲全体に対応するよう、自動検出ポートが 1024 から 65535 の範囲に設定されていることを確認してください。注意点として、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] オプションまたは [SMB 自動検出ポート（SMB Auto-Detect Ports）] オプションで自動検出ポートを有効にしたり指定したりすることはほとんどありません。これは、指定されているデフォルト検出ポートを除き、どちらの場合もトラフィックが発生することはほとんどなく、その見込みも少ないためです。また、自動検出は、トランスポート検出ポートによって識別されていないポートでのみ発生する点にも注意してください。トランスポートごとに自動検出ポートを有効または無効にする際の推奨事項については、DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

Windows のターゲットベース ポリシーでは、ネットワークのトラフィックに一致するように、1 つ以上の任意のトランスポートのポートを任意の組み合わせで指定できます。しかし、Samba のターゲットベース ポリシーでは SMB トランスポートのポートだけを指定できます。

少なくとも 1 つのトランスポートが有効になっている DCE/RPC ターゲットベース ポリシーを追加した場合を除き、デフォルトの ターゲットベース ポリシーでは少なくとも 1 つの DCE/RPC トランスポートを有効にする必要があります。たとえば、すべての DCE/RPC 実装に対してホストを指定し、未指定のホストにはデフォルトのターゲットベース ポリシーを適用したくない場合があります。そのような場合は、デフォルトのターゲットベース ポリシーのトランスポートを有効化しないようにします。

詳細については、次の各項を参照してください。

- コネクションレス型およびコネクション型 DCE/RPC トラフィックについて（27-7 ページ）
- RPC over HTTP トランスポートについて（27-8 ページ）

コネクションレス型およびコネクション型 DCE/RPC トラフィックについて

ライセンス：Protection

DCE/RPC メッセージは、2 種類の DCE/RPC Protocol Data Unit（PDU）の 1 つに準拠します。

- コネクション型 DCE/RPC PDU プロトコル

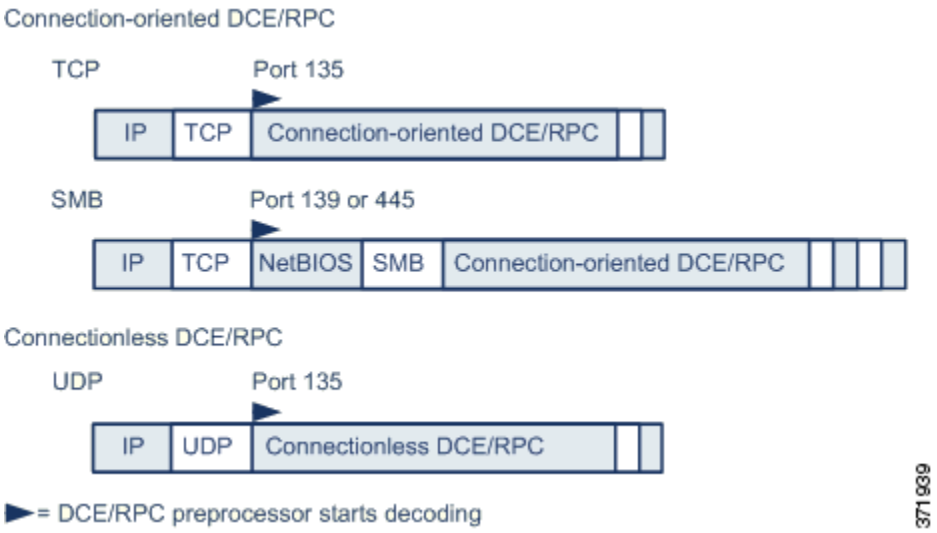
  DCE/RPC プリプロセッサは、TCP、SMB、および RPC over HTTP トランスポートでコネクション型 DCE/RPC を検出します。

- コネクションレス型 DCE/RPC PDU プロトコル

  DCE/RPC プリプロセッサは、UDP トランスポートでコネクションレス型 DCE/RPC を検出します。

この 2 つの DCE/RPC PDU プロトコルには、それぞれ固有のヘッダーとデータ特性があります。たとえば、コネクション型 DCE/RPC のヘッダーの長さは通常は 24 バイトですが、コネクションレス型 DCE/RPC のヘッダーの長さは 80 バイト（固定）です。また、フラグメント化コネクションレス型 DCE/RPC のフラグメントの正しい順序は、コネクションレス型トランスポートでは処理できないため、代わりに、コネクションレス型 DCE/RPC ヘッダーの値によって維持する必要があります。これとは対照的に、コネクション型 DCE/RPC の正しいフラグメント順序はトランスポート プロトコルによって維持されます。DCE/RPC プリプロセッサは、これらや他のプロトコル固有の特性を使用して、異常やその他の検知回避技術について両方のプロトコルをモニタし、トラフィックをデコードおよび最適化してからルール エンジンに渡します。

次の図は、DCE/RPC プリプロセッサが各種トランスポートの DCE/RPC トラフィックの処理を開始するポイントを示します。



この図の次の点に注意してください。

- ウェルノウン TCP または UDP ポート 135 は、TCP および UDP トランスポートの DCE/RPC トラフィックを特定します。
- この図には RPC over HTTP は含まれていません。

  RPC over HTTP の場合、コネクション型 DCE/RPC は、図に示すように、HTTP を介した初期セットアップ シーケンスの後、TCP 経由で直接伝送されます。詳細については、RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

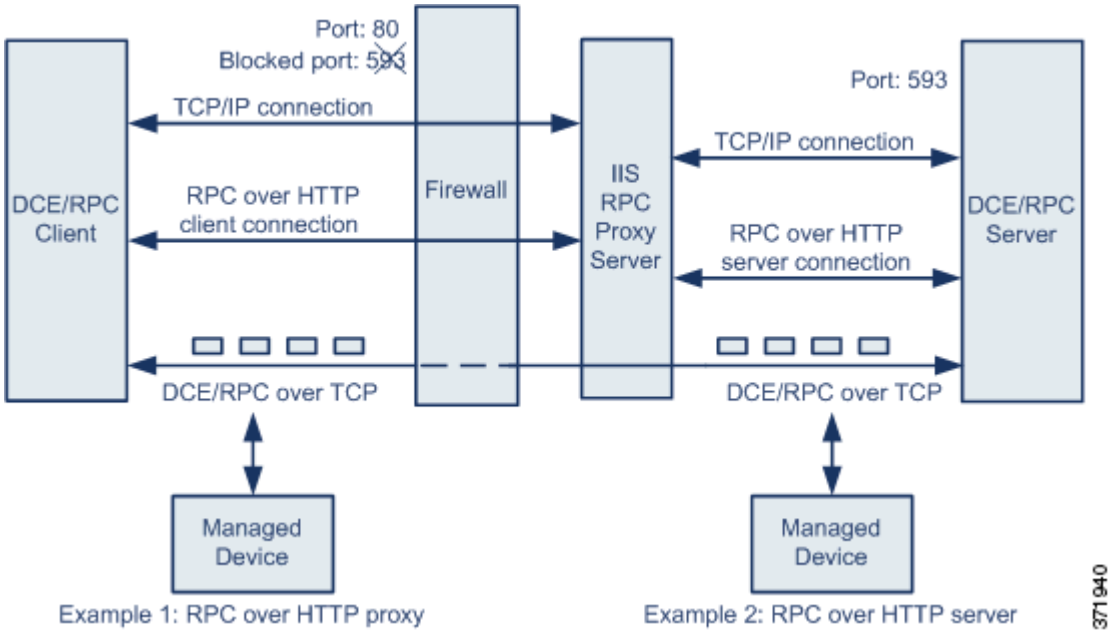
- DCE/RPC プリプロセッサは通常、NetBIOS セッション サービス用のウェルノウン TCP ポート 139 か、同様に実装されたウェルノウン Windows ポート 445 で SMB トラフィックを受信します。

  SMB には DCE/RPC 伝送以外にも多数の機能があるため、プリプロセッサは SMB トラフィックが DCE/RPC トラフィックを伝送しているかどうかをまず検査します。伝送していない場合は処理を停止し、伝送している場合は処理を続行します。
- IP によりすべての DCE/RPC トランスポートがカプセル化されます。
- TCP は、すべてのコネクション型 DCE/RPC を伝送します。
- UDP はコネクションレス型 DCE/RPC を伝送します。

RPC over HTTP トランスポートについて

ライセンス：Protection

Microsoft RPC over HTTP では、次の図に示すように、DCE/RPC トラフィックをトンネリングして、ファイアウォールを通過させることができます。DCE/RPC プリプロセッサは Microsoft RPC over HTTP バージョン 1 を検出します。



Microsoft IIS プロキシ サーバと DCE/RPC サーバは、同じホストまたは別々のホストにインストールできます。いずれの場合でも、個別のプロキシ オプションとサーバ オプションがあります。この図の次の点に注意してください。

- DCE/RPC サーバはポート 593 で DCE/RPC クライアント トラフィックをモニタしますが、ファイアウォールはこのポート 593 をブロックします。

  通常、ファイアウォールではデフォルトでポート 593 がブロックされます。
- RPC over HTTP は、ファイアウォールによって許可される可能性が高いウェルノウン HTTP ポート 80 を使用して、HTTP 経由で DCE/RPC を伝送します。
- 例 1 のように、DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間のトラフィックをモニタする場合は、[RPC over HTTP プロキシ（RPC over HTTP proxy）] オプションを選択します。

- 例 2 のように、Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上にあり、デバイスが 2 つのサーバ間のトラフィックをモニタしている場合は、[RPC over HTTP サーバ（RPC over HTTP server）] オプションを選択します。
- RPC over HTTP により DCE/RPC クライアントとサーバ間でのプロキシ セットアップが完了した後、トラフィックは TCP を経由したコネクション型 DCE/RPC だけで構成されます。

DCE/RPC ターゲットベース ポリシー オプションの選択

ライセンス：Protection

各ターゲットベース ポリシーでは、次に示すさまざまなオプションを指定できます。[到達したメモリ容量（Memory Cap Reached）] および [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] オプション以外のオプションを変更すると、パフォーマンスまたは検出機能に悪影響を及ぼす可能性があります。プリプロセッサについて、またプリプロセッサと有効にされている DCE/RPC ルールとの間の相互作用について十分に理解していない場合は、これらのオプションを変更しないでください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク（Networks）

DCE/RPC ターゲットベース サーバ ポリシーを適用するホストの IP アドレス。

単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの指定については、次を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ポリシー（Policy）

モニタ対象ネットワーク セグメントのターゲット ホストが使用する Windows または Samba DCE/RPC の実装。これらのポリシーの詳細については、ターゲットベース DCE/RPC サーバ ポリシーについて（27-5 ページ）を参照してください。

[SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。SMB セッションの自動検出ポリシー（27-4 ページ）を参照してください。

SMB の無効な共有（SMB Invalid Shares）

1 つ以上の SMB 共有リソースを識別する、大文字と小文字を区別しない英数字テキスト文字列です。指定した共有リソースへの接続が試行されると、プリプロセッサがそのことを検出します。複数の共有をカンマで区切って指定できます。また必要に応じて、共有を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。次に例を示します。

```
"C$", D$, "admin", private
```

SMB ポートと SMB トラフィックの両方の検出が有効に設定されている場合、プリプロセッサは SMB トラフィックで無効な共有を検出します。

ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることに注意してください。たとえば、ドライブ C は C$ または "C$" として指定します。

このオプションのイベントを生成するには、ルール 133:26 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

SMB 最大 AndX チェーン（SMB Maximum AndX Chain）

連結された SMB AndX コマンドの最大数（0 から 255）です。通常、多数の連結 AndX コマンドは異常な動作を表し、場合によっては回避試行を示している可能性があります。連結コマンドを許可しない場合は 1 を指定し、連結コマンドの数の検出を無効にするには 0 を指定します。

プリプロセッサは最初に連結コマンドの数をカウントし、関連する SMB プリプロセッサ ルールが有効であり、連結コマンドの数が設定されている値と等しいかそれ以上の場合にはイベントを生成することに注意してください。その後、処理が続行されます。

（注）　SMB プロトコルに詳しいユーザだけがこのオプションのデフォルト設定を変更するようにしてください。

このオプションのイベントを生成するには、ルール 133:20 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

RPC プロキシ トラフィックのみ（RPC proxy traffic only）

[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] が有効である場合、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであるか、または他の Web サーバ トラフィックを含んでいる可能性があるかどうかを示します。たとえば、ポート 80 はプロキシ トラフィックとその他の Web サーバ トラフィックの両方を伝送する可能性があります。

このオプションが無効になっている場合は、プロキシ トラフィックとその他の Web サーバ トラフィックの両方が想定されます。たとえばサーバが専用プロキシ サーバである場合などに、このオプションを有効にします。有効にすると、プリプロセッサはトラフィックを調べて DCE/RPC を伝送しているかどうかを判別し、伝送していない場合はそのトラフィックを無視し、伝送している場合は処理を続行します。このオプションを有効にすることで機能が追加されるのは、[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）] チェックボックスも有効にされている場合だけであることに注意してください。

RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

有効である場合、DCE/RPC トラフィックが確認されるポートを追加できますが、Web サーバは一般に DCE/RPC トラフィックとその他のトラフィックの両方にデフォルト ポートを使用するため、この操作が必要になることはあまりありません。有効である場合、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] は有効にしませんが、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみであり、その他の Web サーバ トラフィックを含んでいない場合は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を有効にします。

RPC over HTTP サーバ ポート（RPC over HTTP Server Ports）

Microsoft IIS RPC プロキシ サーバと DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定の各ポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

一般に、このオプションを有効にするときは、ネットワーク上のプロキシ Web サーバに注意を払わない場合でも、1025 ～ 65535 のポート範囲で [RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）] も有効にする必要があります。場合によっては RPC over HTTP サーバ ポートを再設定することがあり、その際には再設定したサーバ ポートをこのオプションのポート リストに追加する必要があることに注意してください。

TCP ポート（TCP Ports）

指定の各ポートでの TCP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [TCP 自動検出ポート（TCP Auto-Detect Ports）] も有効にする必要があります。

UDP ポート

指定の各ポートでの UDP の DCE/RPC トラフィックの検出を有効にします。

正当な DCE/RPC トラフィックとエクスプロイトは、さまざまなポートを使用する可能性があります。ポート 1024 より大きい番号のポートが一般的です。通常、このオプションを有効にする場合は、1025 ～ 65535 のポート範囲で [UDP 自動検出ポート（UDP Auto-Detect Ports）] も有効にする必要があります。

SMB ポート（SMB Ports）

指定の各ポートでの SMB の DCE/RPC トラフィックの検出を有効にします。

デフォルトの検出ポートを使用した SMB トラフィックが発生することがあります。他のポートはほとんどありません。通常はデフォルト設定を使用してください。

RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）

管理対象デバイスが DCE/RPC クライアントと Microsoft IIS RPC プロキシ サーバの間に配置されている場合に、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

有効である場合は、一時ポート範囲全体をカバーするため、一般にポート範囲として 1025 から 65535 を指定します。

RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）

Microsoft IIS RPC プロキシ サーバおよび DCE/RPC サーバが異なるホスト上に配置されており、デバイスがこの 2 つのサーバ間のトラフィックをモニタしている場合、指定のポートで RPC over HTTP によりトンネリングされる DCE/RPC トラフィックの自動検出を有効にします。RPC over HTTP トランスポートについて（27-8 ページ）を参照してください。

TCP 自動検出ポート（TCP Auto-Detect Ports）

指定のポートで TCP の DCE/RPC トラフィックの自動検出を有効にします。

UDP 自動検出ポート（UDP Auto-Detect Ports）

指定の各ポートで UDP の DCE/RPC トラフィックの自動検出を有効にします。

SMB 自動検出ポート（SMB Auto-Detect Ports）

SMB の DCE/RPC トラフィックの検出を有効にします。

SMB ファイル インスペクション（SMB File Inspection）

ファイル検出のための SMB トラフィックのインスペクションを有効にします。次の選択肢があります。

- ファイル インスペクションを無効にするには、[オフ（Off）] を選択します。
- SMB でファイル データを検査するが、DCE/RPC トラフィックは検査しない場合は、[ファイルのみ（Only）] を選択します。このオプションを選択すると、ファイルと DCE/RPC トラフィックの両方を検査する場合よりもパフォーマンスが向上する可能性があります。
- SMB でファイルと DCE/RPC トラフィックの両方を検査するには、[オン（On）] を選択します。このオプションを選択すると、パフォーマンスに影響する可能性があります。

SMB トラフィックでの次のファイルについてのインスペクションはサポートされていません。

- SMB 2.x および SMB 3.x で転送されたファイル
- このオプションを有効にしてポリシーを適用する前に確立された TCP または SMB セッションで転送されたファイル
- 1 つの TCP または SMB セッションで同時に転送されたファイル
- 複数の TCP または SMB セッションにわたって転送されたファイル
- メッセージ署名のネゴシエート時など、非連続データを使用して転送されたファイル
- 同一オフセットに異なるデータが含まれており、データがオーバーラップしている転送ファイル
- リモート クライアントがファイル サーバに保存し、そのクライアントで編集用に開かれたファイル

SMB ファイル インスペクションの深さ（SMB File Inspection Depth）

[SMB ファイル インスペクション（SMB File Inspection）] が [ファイルのみ（Only）] または [オン（On）] に設定されている場合に、SMB トラフィックでファイルが検出された時に検査されるデータのバイト数です。次のいずれかを指定します。

- `1` から `2147483647`（約 2GB）までの範囲内の整数
- `0`：ファイル全体を検査する場合
- `-1`：ファイル インスペクションを無効にする場合

このフィールドには、アクセス コントロール ポリシーで定義されている値と等しいか、それよりも小さい値を入力します。[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] で定義されている値よりも大きい値をこのオプションに設定すると、アクセス コントロール ポリシーの設定が、有効な最大値として使用されます。詳細については、ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-21 ページ）参照してください。

[SMB ファイル インスペクション（SMB File Inspection）] が [オフ（Off）] に設定されている場合、このフィールドは無効になります。

DCE/RPC プリプロセッサの設定

ライセンス：Protection

DCE/RPC プリプロセッサのグローバル オプションと、1 つ以上のターゲットベース サーバ ポリシーを設定できます。

ジェネレータ ID（GID）133 のルールを有効にしていない場合、プリプロセッサはイベントを生成しません。特定の検出オプションに関連付けられているルールについては、グローバル DCE/RPC オプションの選択（27-3 ページ）、DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）、およびルール状態の設定（32-23 ページ）を参照してください。

さらに、ほとんどの DCE/RPC プリプロセッサ ルールでは、SMB、コネクション型 DCE/RPC、またはコネクションレス型 DCE/RPC のトラフィックで異常や検知回避技術が検出されると、イベントが生成されます。トラフィック タイプ別に有効にできるルールを次の表に示します。

表 27-1　トラフィックに関連する DCE/RPC ルール

トラフィック	プリプロセッサ ルール GID:SID
SMB	133:2 ～ 133:26、133:48 ～ 133:57
コネクション型 DCE/RPC	133:27 ～ 133:39
コネクションレス型 DCE/RPC	133:40 ～ 133:43

DCE/RPC プリプロセッサを設定する方法：

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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [DCE/RPC 設定（DCE/RPC Configuration）] を有効にしているかどうかに応じて、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。

[DCE/RPC 設定（DCE/RPC 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　グローバル DCE/RPC オプションの選択（27-3 ページ）で説明するオプションを変更できます。

手順 6　次の 2 つの対処法があります。

- 新しいターゲットベースのポリシーを追加します。ページの左側で [サーバ（Servers）] の横にある追加アイコン（  ）をクリックします。[ターゲットの追加（Add Target）] ポップアップ ウィンドウが表示されます。1 つ以上の IP アドレスを [サーバ アドレス（Server Address）] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

  デフォルト ポリシーを含め、最大 255 個のポリシーを設定できます。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のターゲットベースのポリシーの設定を変更します。ページ左側の [サーバ（Servers）] の下で追加したポリシーの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択したエントリが強調表示され、[設定（Configuration）] セクションが更新されて、選択したポリシーの現在の設定が表示されます。既存のポリシーを削除するには、削除するポリシーの横にある削除アイコン（  ）をクリックします。

手順 7　変更できるターゲットベース ポリシー オプションは次のとおりです。

- DCE/RPC のターゲットベース サーバ ポリシーを適用する 1 つ以上のホストを指定するには、[ネットワーク（Networks）] フィールドに、1 つの IP アドレスまたはアドレス ブロック、あるいはこのいずれかまたは両方をカンマで区切ったリストを入力します。

  デフォルト ポリシーを含め、合計で最大 255 個のプロファイルを指定できます。デフォルト ポリシーでは [ネットワーク（Networks）] の設定を変更できないことに注意してください。デフォルト ポリシーは、別のポリシーで指定されていないネットワーク内のすべてのサーバに適用されます。

- ネットワーク セグメントの指定ホストに適用するポリシーのタイプを指定するには、[ポリシー（Policy）] ドロップダウン リストから、いずれかの Windows または Samba ポリシー タイプを選択します。

  [SMB セッションの自動検出ポリシー（Auto-Detect Policy on SMB Session）] グローバル オプションを有効にすると、SMB が DCE/RPC トランスポートの場合に、このオプションの設定をセッションごとに自動的にオーバーライドできます。SMB セッションの自動検出ポリシー（27-4 ページ）を参照してください。

- 指定の共有 SMB リソースへの接続が試行された場合にそのことを検出するようにプリプロセッサを設定するには、[SMB の無効な共有（SMB Invalid Shares）] フィールドに、共有リソースを示す文字列を 1 つまたは複数指定します。文字列の大文字と小文字は区別されず、複数の文字列はカンマで区切って指定します。オプションで、個々の文字列を引用符で囲むこともできます。これは、以前のソフトウェア バージョンでは必須でしたが、現在は必須ではありません。

  たとえば、C$、D$、admin、および private という名前の共有リソースを検出するには、次のように入力します。

  ```
  "C$", D$, "admin", private
  ```

  SMB の無効な共有を検出するには、[SMB ポート（SMB Ports）] または [SMB 自動検出ポート（SMB Auto-Detect Ports）] も有効にして、[SMB トラフィック（SMB Traffics）] グローバル オプションを有効にする必要があります。

  ほとんどの場合、Windows により名前が指定されたドライブを無効な共有として指定するには、このドライブにドル記号を付加する必要があることにも注意してください。たとえば、ドライブ C を指定するには `c$` または `"c$"` と入力します。

- SMB の DCE/RPC トラフィックで検出されたファイルを検査し、DCE/RPC トラフィックの分析はしない場合は、[SMB ファイル インスペクション（SMB File Inspection）] ドロップダウン リストから [ファイルのみ（Only）] を選択します。SMB の DCE/RPC トラフィックで検出されたファイルと DCE/RPC トラフィックを検査するには、[SMB ファイル インスペクション（SMB File Inspection）] ドロップダウン リストから [ファイルのみ（On）] を選択します。[SMB ファイル インスペクションの深さ（SMB File Inspection Depth）] フィールドに、検出されたファイル内の検査対象バイト数を入力します。検出されたファイル全体を検査するには、`0` を入力します。

- 連結された SMB AndX コマンドの最大許容数を指定するには、[SMB AndX の最大チェーン（SMB Maximum AndX Chains）] のフィールドに 0 ～ 255 を入力します。連結されたコマンドを許可しない場合は `1` を指定します。この機能を無効にするには、`0` を入力するか、またはこのオプションを空白のままにします。

（注） SMB プロトコルに詳しいユーザだけが [SMB AndX の最大チェーン（SMB Maximum AndX Chains）] オプションのデフォルト設定を変更するようにしてください。

- Windows ポリシー トランスポートの DCE/RPC トラフィックを伝送することが判明しているポートで、DCE/RPC トラフィックを処理できるようにするには、検出トランスポートの横のチェック ボックスをオンまたはオフにします。またオプションで、伝送用のポートを追加または削除できます。

  Windows ポリシー用に、[RPC over HTTP プロキシ ポート（RPC over HTTP Proxy Ports）]、[RPC over HTTP サーバ ポート（RPC over HTTP Server Ports）]、[TCP ポート（TCP Ports）]、および [UDP ポート（UDP Ports）] のいずれか 1 つまたは任意の組み合わせを選択します。[RPC over HTTP プロキシ（RPC over HTTP proxy）] が有効であり、検出されるクライアント側の RPC over HTTP トラフィックがプロキシ トラフィックのみである場合（つまり、他の Web サーバ トラフィックが含まれていない場合）は、[RPC プロキシ トラフィックのみ（RPC Proxy Traffic Only）] を選択します。

  Samba ポリシー用に [SMB ポート（SMB Ports）] を選択します。

  ほとんどの場合はデフォルト設定を使用します。詳細については、DCE/RPC トランスポートについて（27-6 ページ）、RPC over HTTP トランスポートについて（27-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

  1 つのポートを入力するか、ダッシュ（-）で区切ったポート番号範囲、またはポート番号と範囲をカンマで区切ったリストを入力できます。

- 指定されたポートが DCE/RPC トラフィックを伝送するかどうかを調べて、伝送する場合に処理を続行するには、自動検出トランスポートの横のチェック ボックスをオンまたはオフにします。さらに、必要に応じて、伝送用のポートを追加または削除します。

  Windows ポリシー用に、[RPC over HTTP サーバ自動検出ポート（RPC over HTTP Server Auto-Detect Ports）]、[TCP 自動検出ポート（TCP Auto-Detect Ports）]、[UDP 自動検出ポート（UDP Auto-Detect Ports）] のいずれかまたは任意の組み合わせを選択します。

  ただし、[RPC over HTTP プロキシ自動検出ポート（RPC over HTTP Proxy Auto-Detect Ports）] または [SMB 自動検出ポート（SMB Auto-Detect Ports）] を選択することはほとんどありません。

  通常、エフェメラル ポート範囲全体をカバーするために、有効にする自動検出ポートに対して 1025 ～ 65535 のポート範囲を指定します。詳細については、DCE/RPC トランスポートについて（27-6 ページ）、RPC over HTTP トランスポートについて（27-8 ページ）、および DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

詳細については、DCE/RPC ターゲットベース ポリシー オプションの選択（27-9 ページ）を参照してください。

手順 8　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。

DNS ネーム サーバ応答におけるエクスプロイトの検出

ライセンス：Protection

DNS プリプロセッサは、DNS ネーム サーバ応答を検査し、次に示す特定のエクスプロイトがあるかどうかを確認します。

- RData テキスト フィールドに対するオーバーフローの試行
- 古い DNS リソース レコード タイプ
- 試験的な DNS リソース レコード タイプ

詳細については、次の各項を参照してください。

- DNS プリプロセッサ リソース レコード インスペクションについて（27-16 ページ）
- RData テキスト フィールドに対するオーバーフローの試行の検出（27-18 ページ）
- 古い DNS リソース レコード タイプの検出（27-18 ページ）
- 試験的な DNS リソース レコード タイプの検出（27-19 ページ）
- DNS プリプロセッサの設定（27-19 ページ）

DNS プリプロセッサ リソース レコード インスペクションについて

ライセンス：Protection

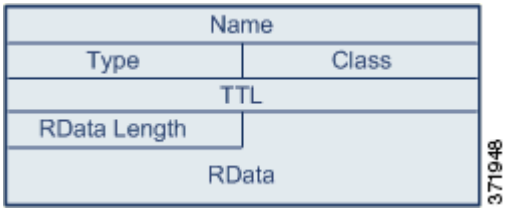
最も一般的なタイプの DNS ネーム サーバ応答には、応答を求めたクエリ内のドメイン名に対応する 1 つ以上の IP アドレスが示されています。その他のタイプのサーバ応答には、たとえば、電子メール メッセージの宛先や、元のクエリの対象のサーバからは取得できない情報を提供できるネームサーバの位置などが記述されています。

DNS 応答は、メッセージ ヘッダー、1 つ以上の要求を含む [質問（Question）] セクション、および [質問（Question）] セクションの要求に対応する 3 つのセクション（[応答（Answer）]、[権威（Authority）]、および [追加情報（Additional Information）]）で構成されます。この 3 セクションの応答には、ネーム サーバに保持されている *リソース レコード*（RR）の情報が反映されます。次の表で、これらの 3 つのセクションについて説明します。

表 27-2　DNS ネーム サーバ RR 応答

セクション	内容	例
応答	クエリに対する特定の回答を提供する 1 つ以上のリソース レコード（オプション）	ドメイン名に対応する IP アドレス
権限	権威ネーム サーバを指し示す 1 つ以上のリソース レコード（オプション）	応答の権威ネーム サーバの名前
その他の情報	[応答（Answer）] セクションに関連する追加情報を提供する 1 つ以上のリソース レコード（オプション）	クエリ対象の別のサーバの IP アドレス

さまざまなタイプのリソース レコードがありますが、これらはすべて一貫して次の構造を保っています。



理論上、すべてのタイプのリソース レコードを、ネーム サーバ応答メッセージの [応答（Answer）]、[権威（Authority）]、または [追加情報（Additional Information）] セクションで使用できます。DNS プリプロセッサは、検出されたエクスプロイトについて、3 つの各応答セクションのすべてのリソース レコードを検査します。

[タイプ（Type）] および [RData] リソース レコード フィールドは、DNS プリプロセッサでは特に重要です。[タイプ（Type）] フィールドは、リソース レコードのタイプを示します。[RData]（リソース データ）フィールドは、応答の内容を示します。[RData] フィールドのサイズと内容は、リソース レコードのタイプによって異なります。

DNS メッセージは通常、UDP トランスポート プロトコルを使用しますが、信頼性のある配信を必要とするメッセージ タイプである場合や、メッセージ サイズが UDP で処理可能なサイズを超えている場合は、TCP を使用します。DNS プリプロセッサは、UDP および TCP の両方のトラフィックで DNS サーバ応答を検査します。

DNS プリプロセッサは、ミッドストリームで検出された TCP セッションを検査せず、ドロップされたパケットが原因でセッションの状態が失われるとインスペクションを終了します。

DNS プリプロセッサ用に設定する一般的なポートは、ウェルノウン ポート 53 です。これは、DNS ネーム サーバが UDP および TCP の両方で DNS メッセージに使用するポートです。

RData テキスト フィールドに対するオーバーフローの試行の検出

ライセンス：Protection

リソース レコード タイプが TXT（テキスト）の場合、RData フィールドは可変長の ASCII テキスト フィールドになります。

DNS プリプロセッサの [RData テキスト フィールドに対するオーバーフローの試行の検出（Detect Overflow attempts on RData Text fields）] オプションを選択した場合は、MITRE の Current Vulnerabilities and Exposures データベースの CVE-2006-3441 エントリで指定されている特定の脆弱性が検出されます。これは、Microsoft Windows 2000 Service Pack 4、Windows XP Service Pack 1 および Service Pack 2、Windows Server 2003 Service Pack 1 の既知の脆弱性です。攻撃者はこの脆弱性を悪用して、[RData] テキスト フィールドの長さの誤算を引き起こし、結果としてバッファ オーバーフローを発生させるよう悪意をもって作られたネーム サーバ応答をホストに送信するか受信させることで、ホストを完全に制御できます。

アップグレードによってこの脆弱性が修正されていないオペレーティング システムが稼働しているホストがネットワーク内に含まれている可能性がある場合は、この機能を有効にする必要があります。

このオプションのイベントを生成するには、ルール 131:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

古い DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが古いタイプとして指定されています。これらは古いレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の古いリソース レコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 27-3　古い DNS リソース レコード タイプ

RR タイプ	コード（Code）	説明
3	MD	メールの宛先
4	MF	メールのフォワーダ

このオプションのイベントを生成するには、ルール 131:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

試験的な DNS リソース レコード タイプの検出

ライセンス：Protection

RFC 1035 ではさまざまなリソース レコード タイプが試験的なタイプとして指定されています。これらは試験的なレコード タイプであるため、一部のシステムはこれらのレコード タイプに対応しておらず、エクスプロイトの対象となることがあります。このようなレコード タイプを含めるようにネットワークを意図的に設定している場合を除き、通常の DNS 応答でこのようなレコード タイプが検出されることは想定されません。

既知の試験的なレコード タイプを検出するようにシステムを設定できます。次の表に、これらのレコード タイプとその説明を示します。

表 27-4　試験的な DNS リソース レコード タイプ

RR タイプ	コード（Code）	説明
7	MB	メールボックスのドメイン名
8	MG	メール グループ メンバー
9	MR	メール リネーム ドメイン名
10	NUL	空白のリソース レコード

このオプションのイベントを生成するには、ルール 131:2 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

DNS プリプロセッサの設定

ライセンス：Protection

DNS プリプロセッサを設定するには、次の手順に従います。このページのオプションの設定の詳細については、RData テキスト フィールドに対するオーバーフローの試行の検出（27-18 ページ）、古い DNS リソース レコード タイプの検出（27-18 ページ）、および試験的な DNS リソース レコード タイプの検出（27-19 ページ）を参照してください。

DNS 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　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [DNS 設定(DNS Configuration)] を有効にしているかどうかに応じて、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。

[DNS 設定(DNS 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　(任意)[設定(Settings)] 領域の次の項目を変更できます。

- [ポート(Ports)] フィールドに、DNS プリプロセッサが DNS サーバ応答をモニタする 1 つ以上の送信元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。
- RData テキスト フィールドでのバッファ オーバーフロー試行の検出を有効にするには、[RData テキスト フィールドでのオーバーフロー試行の検出(Detect Overflow Attempts on RData Text fields)] チェック ボックスをオンにします。
- 古いリソース レコード タイプを検出できるようにするには、[古い DNS RR タイプの検出(Detect Obsolete DNS RR Types)] チェック ボックスをオンにします。
- 試験的なリソース レコード タイプを検出できるようにするには、[試験的な RR タイプの検出(Detect Experimental DNS RR Types)] チェック ボックスをオンにします。

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。

FTP および Telnet トラフィックのデコード

ライセンス: Protection

FTP/Telnet デコーダは FTP および Telnet データ ストリームを分析して、ルール エンジンによる処理の前に FTP および Telnet コマンドを正規化します。

ジェネレータ ID(GID)125 および 126 の FTP および Telnet プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定(32-23 ページ)を参照してください。

詳細は、次のトピックを参照してください。

- グローバル FTP および Telnet オプションについて(27-21 ページ)
- グローバル FTP/Telnet オプションの設定(27-21 ページ)
- Telnet オプションについて(27-22 ページ)
- Telnet オプションの設定(27-23 ページ)
- サーバレベルの FTP オプションについて(27-24 ページ)
- サーバレベルの FTP オプションの設定(27-27 ページ)
- クライアントレベルの FTP オプションについて(27-30 ページ)
- クライアントレベル FTP オプションの設定(27-31 ページ)

グローバル FTP および Telnet オプションについて

ライセンス：Protection

FTP/Telnet デコーダがパケットのステートフル インスペクションまたはステートレス インスペクションを実行するかどうか、デコーダが暗号化 FTP または Telnet セッションを検出するかどうか、およびデコーダが暗号化データの検出後にデータ ストリームの検査を続行するかどうかを決定するグローバル オプションを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、FTP/Telnet デコーダは状態を保存し、各パケットにセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

FTP データ転送を検査するには、このオプションを選択する必要があります。

暗号化トラフィックの検出（Detect Encrypted Traffic）

暗号化 Tenet および FTP セッションを検出します。

このオプションのイベントを生成するには、ルール 125:7 および 126:2 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

暗号化データの検査を続行（Continue to Inspect Encrypted Data）

プリプロセッサに対し、データ ストリームの暗号化後もデータ ストリームの検査を続行し、最終的にデコードされたデータを検索するように指示します。

グローバル FTP/Telnet オプションの設定

ライセンス：Protection

ステートレスまたはステートフル インスペクションを実行するかどうか、暗号化トラフィックを検出するかどうか、および暗号化されていると判定されたデータ ストリームの暗号化データの検査をデコーダが続行するかどうかを制御するために、FTP/Telnet デコーダのグローバル オプションを設定する必要があります。グローバル設定の詳細については、グローバル FTP および Telnet オプションについて（27-21 ページ）を参照してください。

グローバル オプションを設定するには、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。

[詳細設定(Advanced Settings)] ページが表示されます。

手順 4　[アプリケーション層プロプロセッサ(Application Layer Preprocessors)] の下の [FTP と Telnet の構成(FTP and Telnet Configuration)] を有効にしているかどうかに応じて、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。

[FTP と Telnet の構成(FTP and Telnet 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。

ヒント　このページのその他オプションの設定の詳細については、Telnet オプションの設定(27-23 ページ)、サーバレベルの FTP オプションの設定(27-27 ページ)、およびクライアントレベル FTP オプションの設定(27-31 ページ)を参照してください。

手順 5　(任意)[グローバル設定(Global Settings)] ページ領域の次の項目を変更できます。

- FTP パケットを含む再構成された TCP ストリームを検査するには、[ステートフル インスペクション(Stateful Inspection)] を選択します。再構成されていないパケットだけを検査するには、[ステートフル インスペクション(Stateful Inspection)] をクリアします。
- 暗号化トラフィックを検出するには、[暗号化トラフィックの検出(Detect Encrypted Traffic)] を選択します。暗号化トラフィックを無視するには、[暗号化トラフィックの検出(Detect Encrypted Traffic)] をクリアします。
- 必要に応じて、ストリームが再度復号され処理可能になる場合に備えて、暗号化後もストリームの検査を続行する場合は、[続行(Continue)] を選択します。

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。

Telnet オプションについて

ライセンス: Protection

FTP/Telnet デコーダによる Telnet コマンドの正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There(AYT)攻撃数のしきい値を設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート(Ports)

Telnet トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。

正規化（Normalize）

指定のポートへの Telnet トラフィックを正規化します。

異常検知（Detect Anomalies）

対応する SE（サブネゴシエーション終了）がない Telnet SB（サブネゴシエーション開始）の検出を有効にします。

Telnet がサポートするサブネゴシエーションは、SB（サブネゴシエーション開始）で開始し、SE（サブネゴシエーション終了）で終了していなければなりません。しかし、一部の Telnet サーバ実装では、対応する SE のない SB が無視されます。これは、回避事例につながるおそれのある異常な動作です。FTP はコントロール接続で Telnet プロトコルを使用するため、FTP もこの動作の影響を受けます。

この異常が Telnet トラフィックで検出される場合にイベントを生成するにはルール 126:3 を有効にし、FTP コマンド チャネルで検出される場合にイベントを生成するにはルール 125:9 を有効にできます。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Are You There 攻撃のしきい値（Are You There Attack Threshold Number）

連続する AYT コマンドの数が指定のしきい値を超えた場合にそのことを検出します。シスコは、AYT しきい値に 20 以下の値を設定することを推奨します。

このオプションのイベントを生成するには、ルール 126:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Telnet オプションの設定

ライセンス：Protection

正規化を有効または無効にし、特定の異常ケースを有効または無効にし、許容可能な Are You There（AYT）攻撃数のしきい値を制御することができます。Telnet オプションの詳細については、Telnet オプションについて（27-22 ページ）を参照してください。

Telnet オプションを設定するには、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　[アプリケーション層プロプロセッサ（Application Layer Preprocessors）] の下の [FTP と Telnet の構成（FTP and Telnet Configuration）] を有効にしているかどうかに応じて、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。

[FTP と Telnet の構成（FTP and Telnet 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。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定（27-21 ページ）、サーバレベルの FTP オプションの設定（27-27 ページ）、およびクライアントレベル FTP オプションの設定（27-31 ページ）を参照してください。

手順 5　（任意）[Telnet 設定（Telnet Settings）] ページ領域の次の項目を変更できます。

- [ポート（Ports）] フィールドに、Telnet トラフィックをデコードする 1 つ以上のポートを指定します。通常、Telnet は TCP ポート 23 に接続します。複数のポートを指定する場合は、カンマで区切ります。

注意　暗号化トラフィック（SSL）はデコードできないので、ポート 22（SSH）を追加すると、予想外の結果が生じる可能性があります。

- Telnet 正規化を有効または無効にするには、Telnet プロトコル オプションの [正規化（Normalize）] チェック ボックスをオンまたはオフにします。
- 異常検出を有効または無効にするには、Telnet プロトコル オプションの [異常検知（Detect Anomalies）] チェック ボックスをオンまたはオフにします。
- 許容する連続 AYT コマンドの数を [Are You There 攻撃のしきい値（Are You There Attack Threshold Number）] に指定します。

ヒント　シスコは、AYT しきい値としてデフォルト値以下の値を設定することを推奨します。

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。

サーバレベルの FTP オプションについて

ライセンス：Protection

複数の FTP サーバでデコード オプションを設定できます。作成する各サーバ プロファイルには、トラフィックをモニタするサーバのサーバ IP アドレスとポートが含まれます。検証する FTP コマンドと、特定のサーバで無視する FTP コマンドを指定し、コマンドの最大パラメータ長を設定できます。また、デコーダが特定のコマンドで検証する特定のコマンド構文を設定し、代替最大コマンド パラメータ長を設定することもできます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

FTP サーバの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。設定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ポート

管理対象デバイスがトラフィックをモニタする FTP サーバのポートを指定するには、このオプションを使用します。インターフェイスで、複数のポートをカンマで区切って指定します。

File Get コマンド（File Get Commands）

サーバからクライアントにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

File Put コマンド（File Put Commands）

クライアントからサーバにファイルを転送するために使用する FTP コマンドを定義するには、このオプションを使用します。サポートからの指示がない限り、これらの値を変更しないでください。

追加 FTP コマンド（Additional FTP Commands）

デコーダが検出するコマンドを追加で指定するには、この行を使用します。複数のコマンドを追加する場合は、コマンドをスペースで区切ってください。

デフォルト最大パラメータ長（Default Max Parameter Length）

代替最大パラメータ長が設定されていないコマンドの最大パラメータ長を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

代替最大パラメータ長（Alternate Max Parameter Length）

異なる最大パラメータ長を検出するコマンドを指定し、それらのコマンドの最大パラメータ長を指定するには、このオプションを使用します。[追加（Add）] をクリックして行を追加し、特定のコマンドで検出する異なる最大パラメータ長を指定します。

フォーマット文字列攻撃の検査コマンド（Check Commands for String Format Attacks）

指定されたコマンドでフォーマット文字列攻撃を検査するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:5 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

コマンドの妥当性（Command Validity）

特定のコマンドの有効な形式を入力するには、このオプションを使用します。FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントの作成については、FTP コマンド パラメータ検証ステートメントの作成（27-26 ページ）を参照してください。[追加（Add）] をクリックして、コマンド検証行を追加します。

このオプションのイベントを生成するには、ルール 125:2 および 125:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

FTP 転送を無視（Ignore FTP Transfers）

データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして FTP データ転送のパフォーマンスを改善するには、このオプションを使用します。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP サーバによる Telnet 消去コマンドの処理方法と一致する必要があります。一般に、新しい FTP サーバは Telnet 消去コマンドを無視しますが、ほとんどの古いサーバは Telnet 消去コマンドを処理する点に注意してください。

トラブルシューティング：FTP コマンドの検証設定のログを記録（Troubleshooting Options：Log FTP Command Validation Configuration）

トラブルシューティングについてサポートに問い合わせた際に、サーバ用にリストされている FTP コマンドごとに設定情報を出力するように、システムを設定することを指示される場合があります。

注意　このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響を与えるので、サポートからガイダンスを受けた場合にのみ変更してください。

FTP コマンド パラメータ検証ステートメントの作成

ライセンス：Protection

FTP コマンドに対する検証ステートメントを設定するときには、複数の代替パラメータをスペースで区切って指定できます。2 つのパラメータ間にバイナリ OR 関係を作成するには、検証ステートメントでこの 2 つのパラメータをパイプ文字（|）で区切って指定します。パラメータを大カッコ（[]）で囲むと、これらのパラメータがオプションであることを示します。パラメータを中カッコ（{}）で囲むと、これらのパラメータが必須であることを示します。

FTP 通信の一部として受信したパラメータの構文を検証する FTP コマンド パラメータ検証ステートメントを作成できます。詳細については、サーバレベルの FTP オプションについて (27-24 ページ)を参照してください。

FTP コマンド パラメータ検証ステートメントに使用できるパラメータを次の表に示します。

表 27-5　FTP コマンド パラメータ

使用するパラメータ	実行される検証
`int`	示されるパラメータが整数である必要があります。
`number`	示されるパラメータが 1 ～ 255 の範囲内の整数である必要があります。
`char` *`_chars`*	示されるパラメータが単一文字であり、かつ *`_chars`* 引数に指定した文字の 1 つである必要があります。 たとえば、検証引数 `char` *`SBC`* を使用して `MODE` のコマンド検証を定義すると、`MODE` コマンドのパラメータが、文字 `S`(Stream モードを示す)、文字 `B`(Block モードを示す)、または文字 `C`(Compressed モードを示す)を含んでいるかどうかが検証されます。
`date` *`_datefmt`*	*`_datefmt`* に `#` が含まれている場合、示されるパラメータは数値である必要があります。 *`_datefmt`* に `C` が含まれている場合、示されるパラメータは文字である必要があります。 *`_datefmt`* にリテラル文字列が含まれている場合、示されるパラメータはリテラル文字列に一致している必要があります。
`string`	示されるパラメータが文字列である必要があります。
`host_port`	示されるパラメータは、RFC 959(Network Working Group による File Transfer Protocol 仕様)で定義されている有効なホスト ポート指定子である必要があります。

上記の表の構文を必要に応じて組み合わせることにより、トラフィックを検証する必要がある各 FTP コマンドを正しく検証するパラメータ検証ステートメントを作成できます。

(注)　TYPE コマンドに複合式を含める場合は、式をスペースで囲んでください。また、式内の各オペランドをスペースで囲んでください。たとえば、`char A|B` ではなく `char A | B` と入力します。

サーバレベルの FTP オプションの設定

ライセンス：Protection

サーバ レベルでさまざまなオプションを設定できます。追加する FTP サーバごとに、モニタ対象のポート、検証対象のコマンド、コマンドのデフォルト最大パラメータ長、特定のコマンドの代替パラメータ長、および特定のコマンドの検証構文を指定できます。また、FTP チャネルでフォーマット文字列攻撃や Telnet コマンドを調べるかどうか、および各コマンドの設定情報を出力するかどうかを選択できます。サーバレベルの FTP オプションの詳細については、サーバレベルの FTP オプションについて (27-24 ページ)を参照してください。

サーバレベルの FTP オプションの設定方法:

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　[アプリケーション層プロプロセッサ(Application Layer Preprocessors)] の下の [FTP と Telnet の構成(FTP and Telnet Configuration)] を有効にしているかどうかに応じて、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。

[FTP と Telnet の構成(FTP and Telnet 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。

ヒント　このページのその他オプションの設定の詳細については、グローバル FTP/Telnet オプションの設定(27-21 ページ)、Telnet オプションの設定(27-23 ページ)、およびクライアントレベル FTP オプションの設定(27-31 ページ)を参照してください。

手順 5　次の 2 つの対処法があります。

- 新しいサーバ プロファイルを追加します。ページの左側で [FTP サーバ(FTP Server)] の横にある追加アイコン( )をクリックします。[ターゲットの追加(Add Target)] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス(Server Address)] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則(1-24 ページ)を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ(25-3 ページ)を参照してください。

ページの左側の FTP サーバのリストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定（Configuration）] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のサーバ プロファイルの設定を変更します。ページ左側の [FTP サーバ（FTP Server）] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト（default）] をクリックします。

  選択した項目が強調表示され、[設定（Configuration）] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（ ）をクリックします。

手順 6　（任意）[設定（Configuration）] ページ領域の次の項目を変更できます。

- [ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。

- FTP トラフィックをモニタするポートを指定します。ポート 21 は FTP トラフィック用のウェルノウン ポートです。

- [File Get コマンド（File Get Commands）] フィールドで、サーバからクライアントにファイルを転送するために使用される FTP コマンドを更新します。

- [File Put コマンド（File Put Commands）] フィールドで、クライアントからサーバにファイルを転送するために使用される FTP コマンドを更新します。

（注） サポートからの指示がない限り、[File Get コマンド（File Get Commands）] フィールドと [File Put コマンド（File Put Commands）] フィールドの値は変更しないでください。

- FTP/Telnet プリプロセッサによりデフォルトで検査される FTP コマンド以外に、追加の FTP コマンドを検出するには、[追加 FTP コマンド（Additional FTP Commands）] フィールドに、コマンドをスペースで区切って入力します。

  追加 FTP コマンドは、必要な数だけ追加できます。

（注） 追加できるコマンドには、`XPWD`、`XCWD`、`XCUP`、`XMKD`、`XRMD` があります。これらのコマンドの詳細については、RFC 775（Network Working Group によるディレクトリに基づく FTP コマンドの仕様）を参照してください。

- [デフォルト最大パラメータ長（Default Max Parameter Length）] フィールドに、コマンド パラメータの最大長をバイト数で指定します。

- 特定のコマンドで異なる最大パラメータ長を検出するには、[代替最大パラメータ長（Alternate Max Parameter Length）] の横の [追加（Add）] をクリックします。表示される行の最初のテキスト ボックスに、最大パラメータ長を指定します。2 番目のテキスト ボックスに、この代替最大パラメータ長を適用するコマンドをスペースで区切って指定します。

  代替最大パラメータ長は、必要な数だけ追加できます。

- 特定のコマンドでフォーマット文字列攻撃を検査するには、[フォーマット文字列攻撃の検査コマンド（Check Commands for String Format Attacks）] テキスト ボックスにコマンドをスペースで区切って指定します。

- コマンドの有効な形式を指定するには、[コマンドの妥当性（Command Validity）] の横の [追加（Add）] をクリックします。検証対象のコマンドを指定してから、コマンド パラメータの検証ステートメントを入力します。検証ステートメントの構文の詳細については、サーバレベルの FTP オプションについて（27-24 ページ）を参照してください。
- データ転送チャネルで状態インスペクション以外のすべてのインスペクションを無効にして、FTP データ転送のパフォーマンスを改善するには、[FTP 転送を無視（Ignore FTP Transfers）] を有効にします。

（注）　データ転送を検査するには、グローバル FTP/Telnet オプション [ステートフル インスペクション（Stateful Inspection）] を選択する必要があります。グローバル オプションの設定の詳細については、グローバル FTP および Telnet オプションについて（27-21 ページ）を参照してください。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）] を有効にします。

手順 7　サポートから指示された場合にのみ、オプションで、関連するトラブルシューティング オプションを変更します。そのためには、[トラブルシューティング オプション（Troubleshooting Options）] の横にある [+] 記号をクリックします。

手順 8　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。

クライアントレベルの FTP オプションについて

ライセンス：Protection

FTP クライアントのプロファイルを作成できます。各プロファイル内で、クライアントからの FTP 応答の最大応答長を指定できます。また、デコーダが特定のクライアントの FTP コマンド チャネルでのバウンス攻撃と telnet コマンドの使用を検出するかどうかを設定できます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

FTP クライアントの 1 つ以上の IP アドレスを指定するには、このオプションを使用します。

1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト プロファイルを含め最大 255 個のプロファイルを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則（1-24 ページ）を参照してください。

デフォルト ポリシーの default 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたはアドレス ブロックは指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、any を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

最大応答長（Max Response Length）

FTP クライアントからの応答文字列の最大長を指定するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

FTP バウンス試行の検出（Detect FTP Bounce Attempts）

FTP バウンス攻撃を検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:8 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

FTP バウンスの許可（Allow FTP Bounce to）

FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとそれらのホスト上のポートのリストを設定するには、このオプションを使用します。

FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）

FTP コマンド チャネルで Telnet コマンドが使用された場合にそのことを検出するには、このオプションを使用します。

このオプションのイベントを生成するには、ルール 125:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

正規化時に消去コマンドを無視（Ignore Erase Commands during Normalization）

[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] が選択されている場合に、FTP トラフィックの正規化時に Telnet の文字および行の消去コマンドを無視するには、このオプションを使用します。この設定は、FTP クライアントによる Telnet 消去コマンドの処理方法に一致している必要があります。一般に、新しい FTP クライアントは Telnet 消去コマンドを無視しますが、ほとんどの古いクライアントは Telnet 消去コマンドを処理する点に注意してください。

クライアントレベル FTP オプションの設定

ライセンス：Protection

クライアントからの FTP トラフィックをモニタするように、FTP クライアントのクライアント プロファイルを設定できます。クライアントをモニタするために設定できるオプションの詳細については、クライアントレベルの FTP オプションについて（27-30 ページ）を参照してください。Telnet オプションの詳細については、Telnet オプションについて（27-22 ページ）を参照してください。その他の FTP オプションの詳細については、サーバレベルの FTP オプションについて（27-24 ページ）およびグローバル FTP および Telnet オプションについて（27-21 ページ）を参照してください。

クライアントレベルの FTP オプションの設定方法:

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　[アプリケーション層プロプロセッサ(Application Layer Preprocessors)] の下の [FTP と Telnet の構成(FTP and Telnet Configuration)] を有効にしているかどうかに応じて、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。

[FTP と Telnet の構成(FTP and Telnet Configuration)] ページが表示されます。

手順 5　次の 2 つの対処法があります。

- 新しいクライアント プロファイルを追加します。ページの左側で [FTP クライアント(FTP Client)] の横にある追加アイコン( )をクリックします。[ターゲットの追加(Add Target)] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [クライアント アドレス(Client Address)] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。指定できる最大文字数は 1024 文字です。デフォルト ポリシーを含め最大 255 個のポリシーを設定できます。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則(1-24 ページ)を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ(25-3 ページ)を参照してください。

  ページの左側の FTP クライアントのリストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定(Configuration)] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のクライアント プロファイルの設定を変更します。ページ左側の [FTP クライアント(FTP Client)] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト(default)] をクリックします。

  選択した項目が強調表示され、[設定(Configuration)] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン( )をクリックします。

手順 6　（任意）[設定（Configuration）] ページ領域の次の項目を変更できます。

- オプションで、[ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

  ページの左側で、強調表示されているアドレスが更新されます。

  デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのクライアント ホストに適用されます。
- [最大応答長（Max Response Length）] フィールドに、FTP クライアントからの応答の最大長をバイト単位で指定します。
- FTP バウンス攻撃を検出するには、[FTP] を選択します。

  FTP/Telnet デコーダは、FTP PORT コマンドが発行されたとき、指定のホストがクライアントの指定のホストと一致しない場合にそのことを検出します。
- FTP PORT コマンドを FTP バウンス攻撃として扱わない追加のホストとポートのリストを設定するには、[FTP バウンスの許可（Allow FTP Bounce to）] フィールドに、各ホスト（または CIDR 形式のネットワーク）、コロン（:）、およびポートまたはポート範囲をこの順序で指定します。ホストのポート範囲を入力するには、範囲の開始ポートと範囲の最終ポートをダッシュ（-）でつなげて表します。複数のホストを入力するには、ホスト項目をカンマで区切って入力します。

  たとえば、ホスト 192.168.1.1 に対する FTP PORT コマンドをポート 21 で許可し、ホスト 192.168.1.2 に対するコマンドをポート 22 ～ 1024 のいずれかで許可するには、次のように入力します。

  ```
  192.168.1.1:21, 192.168.1.2:22-1024
  ```

  FireSIGHT システムで CIDR 表記およびプレフィクス長を使用する方法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

（注） 1 つのホストの個々の複数のポートを指定するには、ポート定義ごとにホストの IP アドレスを繰り返す必要があります。たとえば、192.168.1.1 のポート 22 と 25 を指定するには、`192.168.1.1:22, 192.168.1.1:25` と入力します。

- Telnet コマンドが FTP コマンド チャネルで使用された場合にそのことを検出するには、[FTP コマンドでの Telnet エスケープ コードの検出（Detect Telnet Escape Codes within FTP Commands）] を選択します。
- FTP トラフィックの正規化時に Telnet の文字消去コマンドおよび行消去コマンドを無視するには、[正規化時に消去コマンドを無視（Ignore Erase Commands During Normalization）] を選択します。

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、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。

HTTP トラフィックのデコード

ライセンス：Protection

HTTP Inspect プリプロセッサは、次の処理を行います。

- ネットワーク上の Web サーバに送信される HTTP 要求と Web サーバから受信する HTTP 応答をデコードおよび正規化する。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバに送信されたメッセージを URI、非 cookie ヘッダー、cookie ヘッダー、メソッド、メッセージ ボディの各コンポーネントに分ける。
- HTTP 関連の侵入ルールのパフォーマンス向上のために、Web サーバから受信したメッセージをステータス コード、ステータス メッセージ、非 set-cookie ヘッダー、cookie ヘッダー、および応答ボディの各コンポーネントに分ける。
- URI エンコード攻撃の可能性を検出する。
- 正規化データを追加ルール処理に使用できるようにする。

HTTP トラフィックはさまざまな形式でエンコードされている可能性があり、このことが、ルールによる適切な検査の実施を困難にしています。HTTP Inspect は 14 種類のエンコードをデコードし、HTTP トラフィックが最良のインスペクションを受けられるようにします。

HTTP Inspect のオプションは、グローバルに設定するか、1 つのサーバで設定するか、またはサーバ リストに対して設定することができます。

HTTP Inspect プリプロセッサを使用するときは、次の点に注意してください。

- プリプロセッサ エンジンは HTTP の正規化を*ステートレス*に実行します。つまり、パケット単位で HTTP 文字列を正規化し、TCP ストリーム プリプロセッサにより再構成された HTTP 文字列のみを処理できます。
- ジェネレータ ID（GID）119 の HTTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- グローバル HTTP 正規化オプションの選択（27-34 ページ）
- グローバル HTTP 設定オプションの設定（27-36 ページ）
- サーバレベル HTTP 正規化オプションの選択（27-36 ページ）
- サーバレベル HTTP 正規化エンコード オプションの選択（27-45 ページ）
- HTTP サーバ オプションの設定（27-47 ページ）
- 追加の HTTP Inspect プリプロセッサ ルールの有効化（27-49 ページ）

グローバル HTTP 正規化オプションの選択

ライセンス：Protection

HTTP Inspect プリプロセッサのグローバル HTTP オプションは、プリプロセッサの機能を制御します。Web サーバ ポートとして指定されていないポートが HTTP トラフィックを受信する場合の HTTP 正規化を有効または無効にするには、このオプションを使用します。

次の点に注意してください。

- [無制限の圧縮解除（Unlimited Decompression）] を有効にすると、変更のコミット時に [圧縮データの最大深さ（Maximum Compressed Data Depth）] および [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションが自動的に 65535 に設定されます。詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）を参照してください。
- アクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーと、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で、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] オプションの値が異なる場合は、最も大きな値が使用されます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

異常な HTTP サーバの検出（Detect Anomalous HTTP Servers）

Web サーバ ポートとして指定されていないポートに送信された HTTP トラフィックまたはこのポートで受信した HTTP トラフィックを検出します。

（注） このオプションをオンにする場合は、[HTTP 設定（HTTP Configuration）] ページで、HTTP トラフィックを受信するすべてのポートがサーバ プロファイルにリストされていることを確認してください。確認せずにこのオプションと関連するプリプロセッサ ルールを有効にすると、サーバとの間の通常のトラフィックによってイベントが生成されます。デフォルトのサーバ プロファイルには、HTTP トラフィックに一般に使用されるすべてのポートが含まれていますが、このプロファイルを変更した場合は、イベントの生成を防ぐために別のプロファイルにそれらのポートを追加する必要があります。

このオプションのイベントを生成するには、ルール 120:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

HTTP プロキシ サーバの検出（Detect HTTP Proxy Servers）

[HTTP プロキシの使用を許可（Allow HTTP Proxy Use）] オプションで定義されていないプロキシ サーバを使用する HTTP トラフィックを検出します。

このオプションのイベントを生成するには、ルール 119:17 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

圧縮データの最大深さ（Maximum Compressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、圧縮解除する圧縮データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

圧縮解除データの最大深さ（Maximum Decompressed Data Depth）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合に、正規化された圧縮データの最大サイズを設定します。指定できるバイト数は 1 ～ 65535 です。

グローバル HTTP 設定オプションの設定

ライセンス：Protection

非標準ポートへの HTTP トラフィックとプロキシ サーバを使用する HTTP トラフィックの検出を設定できます。グローバル HTTP 設定オプションの詳細については、グローバル HTTP 正規化オプションの選択（27-34 ページ）を参照してください。

グローバル HTTP 設定オプションを設定するには、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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [HTTP 設定（HTTP Configuration）] を有効にしているかどうかに応じて、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。

[HTTP 設定（HTTP Configuration）] ページが表示されます。

手順 5　グローバル HTTP 正規化オプションの選択（27-34 ページ）で説明するグローバル 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。

サーバレベル HTTP 正規化オプションの選択

ライセンス：Protection

サーバレベルのオプションは、モニタ対象サーバごとに設定するか、すべてのサーバに対してグローバルに設定するか、またはサーバ リストに対して設定することができます。また、事前定義のサーバ プロファイルを使用してこれらのオプションを設定するか、またはご使用の環境のニーズに合わせて個別に設定することができます。これらのオプション、またはこれらのオプションを設定するデフォルト プロファイルの 1 つを使用して、トラフィックを正規化する HTTP サーバ ポート、正規化するサーバ応答ペイロードの量、および正規化するエンコードのタイプを指定します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ネットワーク

1 つ以上のサーバの IP アドレスを指定するには、このオプションを使用します。1 つの IP アドレスまたはアドレス ブロックを指定するか、そのいずれかまたは両方から成るカンマで区切ったリストを指定できます。

デフォルト プロファイルを含めてプロファイルの合計数は最大 255 ですが、さらに、HTTP サーバ リストに最大 496 文字（約 26 エントリ）を含めることができ、すべてのサーバ プロファイルに対して合計 256 のアドレス エントリを指定できます。FireSIGHT システムでの IPv4 CIDR 表記と IPv6 プレフィクス長の使用法については、IP アドレスの表記規則（1-24 ページ）を参照してください。

デフォルト ポリシーの `default` 設定では、別のターゲットベース ポリシーでカバーされていないモニタ対象ネットワーク セグメントのすべての IP アドレスが指定されることに注意してください。したがって、デフォルト ポリシーの IP アドレスまたは CIDR ブロック/プレフィックス長は指定できず、また指定する必要もありません。また、別のポリシーでこの設定を空白にしたり、`any` を表すアドレス表記（0.0.0.0/0 または ::/0）を使用したりすることはできません。

また、ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ（25-3 ページ）を参照してください。

ポート

プリプロセッサ エンジンが HTTP トラフィックを正規化するポート。ポート番号が複数ある場合は、カンマで区切ります。

サイズ超過のディレクトリ長（Oversize Dir Length）

指定された値よりも長い URL ディレクトリを検出します。

このオプションのイベントを生成するには、ルール 119:15 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

クライアント フローの深さ（Client Flow Depth）

[ポート（Ports）] で定義されているクライアント側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数（ヘッダーとペイロード データを含む）を指定します。ルール内の HTTP コンテンツ ルール オプションによって要求メッセージの特定の部分が検査される場合は、[クライアント フローの深さ（Client Flow Depth）] は適用されません。詳細については、HTTP コンテンツ オプション（36-26 ページ）を参照してください。

-1 ～ 1460 の値を指定できます。シスコは、[クライアント フローの深さ（Client Flow Depth）] をその最大値に設定することを推奨しています。次のいずれかを指定します。

- 1 ～ 1460 を指定すると、最初のパケットで指定のバイト数が検査されます。最初のパケットのバイト数が指定のバイト数よりも少ない場合は、パケット全体が検査されます。指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることに注意してください。

  また、値 300 を指定すると、通常は、多くのクライアント要求ヘッダーの終わりにある大きな HTTP Cookie のインスペクションが排除されることにも注意してください。

– 0 を指定すると、すべてのクライアント側トラフィックが検査されます。これにはセッション内の複数のパケットが含まれ、必要な場合には 1460 バイトの制限を超えることもあります。この値はパフォーマンスに影響する可能性があることに注意してください。

– -1 を指定すると、クライアント側のすべてのトラフィックが無視されます。

サーバ フローの深さ（Server Flow Depth）

[ポート（Ports）] で指定されたサーバ側 HTTP トラフィックについて、ルールで検査される raw HTTP パケットのバイト数を指定します。[HTTP 応答の検査（Inspect HTTP Responses）] が無効である場合は raw ヘッダーとペイロードが検査され、[HTTP 応答の検査（Inspect HTTP Response）] が有効である場合は、raw 応答ボディのみが検査されます。

[サーバ フローの深さ（Server Flow Depth）] では、[ポート（Ports）] で定義されているサーバ側 HTTP トラフィックについて、ルールで検査されるセッション内の raw サーバ応答データのバイト数を指定します。このオプションを使用して、HTTP サーバ応答データのインスペクションのレベルとパフォーマンスのバランスを調整できます。ルール内の HTTP コンテンツ オプションによって要求メッセージの特定の部分が検査される場合は、Server Flow Depth は適用されません。詳細については、HTTP コンテンツ オプション（36-26 ページ）を参照してください。

クライアント フローの深さ（Client Flow Depth）とは異なり、サーバ フローの深さ（Server Flow Depth）では、ルールが検査するバイト数を、HTTP 要求パケットごとではなく、HTTP 応答ごとのバイト数として指定します。

-1 ～ 65535 の値を指定できます。シスコは、[サーバ フローの深さ（Server Flow Depth）] をその最大値に設定することを推奨しています。次のいずれかの値を指定できます。

– 1 ～ 65535 の範囲の値:

[HTTP 応答の検査（Inspect HTTP Responses）] が**有効**である場合、raw HTTP 応答ボディのみが検査され、raw HTTP ヘッダーは検査されません。また、[圧縮データの検査（Inspect Compressed Data）] が有効である場合は、圧縮解除データも検査されます。

[HTTP 応答の検査（Inspect HTTP Responses）] が**無効**である場合、raw パケット ヘッダーとペイロードが検査されます。

セッションの応答バイト数が指定の値よりも少ない場合は、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）すべての応答パケットが完全に検査されます。セッションの応答バイト数が指定の値よりも多い場合、そのセッションで、ルールにより（必要に応じて複数パケットにわたって）指定のバイト数だけが検査されます。

フローの深さ（Flow Depth）の値が小さいと、[ポート（Ports）] で定義されているサーバ側トラフィックを対象とするルールで、検出漏れが発生する可能性があります。これらのルールのほとんどは HTTP ヘッダーまたはコンテンツ（通常、非ヘッダー データの先頭の約 100 バイト以内）を対象とします。通常はヘッダーの長さは 300 バイト未満ですが、ヘッダー サイズは異なることがあります。

指定された値は、セグメント化されたパケットと再構成されたパケットの両方に適用されることにも注意してください。

– 0 を指定すると、[ポート（Port）] で定義されているすべての HTTP サーバ側トラフィックでパケット全体が検査されます。これにはセッションでの 65535 バイトよりも大きな応答データも含まれます。

この値はパフォーマンスに影響する可能性があることに注意してください。

– -1

[HTTP 応答の検査（Inspect HTTP Responses）] が**有効**な場合、raw HTTP ヘッダーだけが検査され、raw HTTP 応答ボディは検査されません。

[HTTP 応答の検査（Inspect HTTP Responses）] が**無効**である場合、[ポート（Ports）] で定義されているすべてのサーバ側トラフィックは無視されます。

最大ヘッダー長（Maximum Header Length）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効である場合は、HTTP 要求、および HTTP 応答で、指定されている最大バイト数よりも長いヘッダー フィールドを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:19 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

最大ヘッダー数（Maximum Number of Headers）

HTTP 要求でヘッダー数がこの設定を超えている場合にそのことを検出します。有効にするには、1 ～ 1024 の値を指定します。

このオプションのイベントを生成するには、ルール 119:20 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

最大スペース数（Maximum Number of Spaces）

折りたたみ行のスペースの数が HTTP 要求のこの設定と等しいか、超えている場合にそのことを検出します。値 0 を指定すると、このオプションが無効になります。有効にするには、1 ～ 65535 の値を指定します。

このオプションのイベントを生成するには、ルール 119:26 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

HTTP クライアント ボディの抽出の深さ（HTTP Client Body Extraction Depth）

HTTP クライアント要求のメッセージ ボディから抽出するバイト数を指定します。侵入ルールを使用して抽出データを検査するには、`content` または `protected_content` キーワードを [HTTP クライアント ボディ（HTTP Client Body）] オプションと共に選択します。詳細については、HTTP コンテンツ オプション（36-26 ページ）を参照してください。

-1 ～ 65495 の値を指定します。クライアント ボディを無視するには、-1 を指定します。クライアント ボディ全体を抽出するには、0 を指定します。抽出対象のバイト数を指定すると、システム パフォーマンスが向上することがある点に注意してください。また、侵入ルールで [HTTP クライアント ボディ（HTTP Client Body）] オプションが機能するためには、0 ～ 65495 の値を指定する必要があります。

小さいチャンク サイズ（Small Chunk Size）

チャンクが小さいとみなされるサイズの最大バイト数を指定します。1 ～ 255 の値を指定します。値 0 を指定すると、異常な小さなセグメントの連続の検出が無効になります。詳細については、[連続する小さいチャンク（Consecutive Small Chunks）] オプションを参照してください。

連続する小さいチャンク（Consecutive Small Chunks）

チャンク転送エンコードを使用するクライアント トラフィックまたはサーバ トラフィックで異常に大量であるとみなされる、連続する小さなチャンクの数を指定します。[小さいチャンク サイズ（Small Chunk Size）] オプションは、小さなチャンクの最大サイズを指定します。

たとえば、10 バイト以下のチャンクが 5 つ連続していることを検出するには、[小さいチャンク サイズ（Small Chunk Size）] に 10 を設定し、[連続する小さいチャンク（Consecutive Small Chunks）] に 5 を設定します。

大量の小さなチャンクが検出される場合にイベントをトリガーするには、クライアント トラフィックの場合はプリプロセッサ ルール 119:27 を有効にし、サーバ トラフィックの場合はルール 120:7 を有効にします。[小さいチャンク サイズ（Small Chunk Size）] が有効であり、このオプションが 0 または 1 に設定されている場合にこれらのルールを有効にすると、指定されたサイズ以下のすべてのチャンクでイベントがトリガーとして使用されます。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

HTTP メソッド（HTTP Methods）

システムがトラフィックで検出すると予期される、GET および POST 以外の HTTP 要求メソッドを指定します。複数の値はカンマで区切ります。

侵入ルールでは、HTTP メソッドのコンテンツを検索するために、`content` または `protected_content` キーワードが **HTTP Method** 引数と共に使用されます。HTTP コンテンツ オプション（36-26 ページ）を参照してください。GET、POST、およびこのオプションで設定されているメソッド以外のメソッドがトラフィックで検出される場合にイベントを生成するには、ルール 119:31 を有効にします。

アラートなし（No Alerts）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

（注）　このオプションでは、HTTP 標準テキスト ルールと共有オブジェクトのルールは無効に**なりません**。

HTTP ヘッダーの正規化（Normalize HTTP Headers）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、要求ヘッダーと応答ヘッダーの非 cookie データの正規化が有効になります。[HTTP 応答の検査（Inspect HTTP Responses）] が有効**ではない**場合は、要求ヘッダーと応答ヘッダーで cookie を含む HTTP ヘッダー全体の正規化が有効になります。

HTTP Cookie の検査（Inspect HTTP Cookies）

HTTP 要求ヘッダーからの cookie の抽出を有効にします。また、[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、応答ヘッダーからの set-cookie データの抽出も有効になります。cookie の抽出が不要な場合は、このオプションを無効にするとパフォーマンスが向上します。

`Cookie:` および `Set-Cookie:` のヘッダー名、ヘッダー行の先頭のスペース、およびヘッダー行の末尾の `CRLF` は、cookie の一部ではなくヘッダーの一部として検査されます。

HTTP ヘッダーの Cookie の正規化（Normalize Cookies in HTTP headers）

HTTP 要求ヘッダーの cookie の正規化を有効にします。[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、応答ヘッダーの set-cookie データの正規化も有効になります。このオプションを選択する前に、[HTTP Cookie の検査（Inspect HTTP Cookies）] を選択する必要があります。

HTTP プロキシの使用を許可（Allow HTTP Proxy Use）

モニタ対象 Web サーバを HTTP プロキシとして使用できるようにします。このオプションは、HTTP 要求のインスペクションでのみ使用されます。

URI のみの検査（Inspect URI Only）

正規化された HTTP 要求パケットの URI 部分のみを検査します。

HTTP 応答の検査（Inspect HTTP Responses）

HTTP 応答の拡張インスペクションが有効になり、プリプロセッサは、HTTP 要求メッセージのデコードと正規化の他に、ルール エンジンによるインスペクションのために応答フィールドを抽出します。このオプションを有効にすると、応答ヘッダー、ボディ、ステータス コードなどがシステムにより抽出されます。また [HTTP Cookie の検査（Inspect HTTP Cookies）] が有効な場合は、set-cookie データも抽出されます。詳細については、HTTP コンテンツ オプション（36-26 ページ）、HTTP エンコードのタイプと位置によるイベントの生成（36-104 ページ）、および特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 120:2 および 120:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

UTF エンコードを UTF-8 に正規化（Normalize UTF Encodings to UTF-8）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、HTTP 応答内の UTF-16LE、UTF-16BE、UTF-32LE、および UTF32-BE エンコードが検出され、UTF-8 に正規化されます。

このオプションのイベントを生成するには、ルール 120:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

圧縮データの検査（Inspect Compressed Data）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合は、HTTP 応答ボディ内の gzip および deflate 互換圧縮データの圧縮解除と、正規化された圧縮解除データのインスペクションが有効になります。システムは、チャンク HTTP 応答データと非チャンク HTTP 応答データを検査します。システムは、必要に応じて複数のパケットにわたり圧縮解除データをパケット単位で検査します。つまり、システムが異なるパケットの圧縮解除データをインスペクションのために結合させることはありません。[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

無制限の圧縮解除（Unlimited Decompression）

[圧縮データの検査（Inspect Compressed Data）]（および任意で、[SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））]、[SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））]、または [PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））]）が有効な場合、複数のパケットにわたって [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] がオーバーライドされます。つまり、このオプションにより、複数のパケットにわたる無制限の圧縮解除が有効になります。このオプションを有効にしても、単一パケット内での [圧縮データの最大深さ（Maximum Compressed Data Depth）] または [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] には影響しないことに注意してください。また、このオプションを有効にすると、変更のコミット時に、[圧縮データの最大深さ（Maximum Compressed Data Depth）] と [圧縮解除データの最大深さ（Maximum Decompressed Data Depth）] が 65535 に設定されることにも注意してください。グローバル HTTP 正規化オプションの選択（27-34 ページ）を参照してください。

Javascript の正規化（Normalize Javascript）

[HTTP 応答の検査（Inspect HTTP Responses）] が有効な場合、HTTP 応答ボディ内での Javascript の検出と正規化を有効にします。プリプロセッサは unescape 関数や decodeURI 関数、String.fromCharCode メソッドなどの難読化 Javascript データを正規化します。プリプロセッサは、unescape、decodeURI、および decodeURIComponent 関数内の次のエンコードを正規化します。

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

プリプロセッサは連続するスペースを検出し、1 つのスペースに正規化します。このオプションが有効である場合、設定フィールドでは、難読化 Javascript データで許容する連続スペースの最大数を指定できます。入力できる値は、1 ～ 65535 です。値 0 を指定すると、このフィールドに関連付けられているプリプロセッサ ルール（120:10）が有効かどうかに関係なく、イベントの生成が無効になります。

プリプロセッサは、Javascript の正符号（+）演算子も正規化し、この演算子を使用して文字列を連結します。

`file_data` キーワードを使用して、侵入ルールに対し正規化された Javascript データを指し示すことができます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:9、120:10、および 120:11 を有効にします。

表 27-6　[Javascript の正規化（Normalize Javascript）] オプションのルール

ルール	イベントがトリガーとして使用される条件
120:9	プリプロセッサ内の難読化レベルが 2 以上である。
120:10	Javascript 難読化データで連続するスペースの数が、許容される連続スペースの最大数として設定された値以上である。
120:11	エスケープされたデータまたはエンコードされたデータに、複数のエンコード タイプが含まれている。

詳細については、ルール状態の設定（32-23 ページ）を参照してください。

SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））および SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、これらのオプションは、HTTP 要求の HTTP 応答ボディ内にあるファイルの圧縮部分を圧縮解除します。

（注）　HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

- [SWF ファイルの圧縮解除（LZMA）（Decompress SWF File（LZMA））] は、Adobe ShockWave Flash（`.swf`）ファイルの LZMA 互換の圧縮部分を圧縮解除します。
- [SWF ファイルの圧縮解除（Deflate）（Decompress SWF File（Deflate））] は、Adobe ShockWave Flash（`.swf`）ファイルの deflate 互換の圧縮部分を圧縮解除します。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:12 および 120:13 を有効にします。

表 27-7　[SWF ファイルの圧縮解除（Decompress SWF File）] オプションのルール

ルール	イベントがトリガーとして使用される条件
120:12	deflate ファイルの圧縮解除に失敗
120:13	LZMA ファイルの圧縮解除に失敗

PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））

[HTTP Inspect の応答（HTTP Inspect Responses）] が有効な場合、[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate）] は、HTTP 要求の HTTP 応答ボディ内にある Portable Document Format（`.pdf`）ファイルの deflate 互換の圧縮部分を圧縮解除します。システムは、`/FlateDecode` ストリーム フィルタが付いた PDF ファイルだけを圧縮解除できます。他のフィルタ（`/FlateDecode /FlateDecode` など）はサポートしていません。

（注）　HTTP GET 応答で見つかったファイルの圧縮部分**のみ**を圧縮解除できます。

[圧縮データの最大深さ（Maximum Compressed Data Depth）]、[圧縮解除データの最大深さ（Maximum Decompressed Data Depth）]、または圧縮データの終わりに到達すると、圧縮解除が終了します。[無制限の圧縮解除（Unlimited Decompression）] を選択していない場合は、[サーバ フローの深さ（Server Flow Depth）] に到達すると、圧縮解除データのインスペクションが終了します。圧縮解除データを検査するには、`file_data` ルール キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

このオプションのイベントを生成するには、次に示すように、ルール 120:14、120:15、120:16、および 120:17 を有効にします。

表 27-8　[PDF ファイルの圧縮解除（Deflate）（Decompress PDF File（Deflate））] オプションのルール

ルール	イベントがトリガーとして使用される条件
120:14	ファイルの圧縮解除に失敗
120:15	圧縮タイプがサポート対象外のタイプであるため、ファイルの圧縮解除に失敗
120:16	PDF ストリーム フィルタがサポート対象外のフィルタであるため、ファイルの圧縮解除に失敗
120:17	ファイルの解析に失敗

元のクライアント IP アドレスの抽出（Extract Original Client IP Address）

X-Forwarded-For（XFF）ヘッダー、True-Client-IP、またはカスタム定義の HTTP ヘッダーから、元のクライアント IP アドレスを抽出できるようにします。侵入イベント テーブル ビューで、抽出された元のクライアント IP アドレスを表示できます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 119:23、119:29、および 119:30 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

XFF ヘッダーの優先順位（XFF Header Priority）

[元のクライアント IP アドレスの抽出（Extract Original Client IP Address）] が有効な場合、システムが元のクライアント IP の HTTP ヘッダーを処理する順序を指定します。モニタ対象ネットワークで、X-Forwarded-For（XFF）または True-Client-IP 以外の元のクライアント IP ヘッダーが発生すると予測される場合は、[追加（Add）] をクリックしてプライオリティ リストに追加のヘッダー名を追加できます。追加したら、各ヘッダー タイプの横にある上下矢印アイコンを使用して、優先順位を調整します。HTTP 要求に複数の XFF ヘッダーがある場合は、優先順位が最も高いヘッダーだけが処理されます。

URI のログ（Log URI）

raw URI が存在する場合に、HTTP 要求パケットから raw URI を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこの URI を関連付けます。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP URI] 列に、抽出された URI の先頭 50 文字を表示できます。パケット ビューでは、URI 全体（最大 2048 バイト）を表示できます。詳細については、侵入イベントについて（41-12 ページ）とイベント情報の表示（41-27 ページ）を参照してください。

ホスト名のログ（Log Hostname）

ホスト名が存在する場合に、HTTP 要求の Host ヘッダーからホスト名を抽出できるようにし、このセッションで生成されるすべての侵入イベントにこのホスト名を関連付けます。複数の Host ヘッダーがある場合は、1 番目のヘッダーからホスト名を抽出します。

このオプションが有効である場合、侵入イベント テーブル ビューの [HTTP ホスト名（HTTP Hostname）] 列に、抽出されたホスト名の先頭 50 文字を表示できます。パケット ビューでは、ホスト名全体（最大 256 バイト）を表示できます。詳細については、侵入イベントについて（41-12 ページ）とイベント情報の表示（41-27 ページ）を参照してください。

このオプションのイベントを生成するには、ルール 119:25 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

プリプロセッサとルール 119:24 が有効である場合は、HTTP 要求で複数の Host ヘッダーが検出される場合でも、プリプロセッサはこのオプションの設定に関係なく、侵入イベントを生成することに注意してください。詳細については、追加の HTTP Inspect プリプロセッサ ルールの有効化（27-49 ページ）を参照してください。

プロファイル（Profile）

HTTP トラフィック向けに正規化されたエンコードのタイプを指定します。システムには、ほとんどのサーバに適用できるデフォルト プロファイル、Apache サーバと IIS サーバ用のデフォルト プロファイル、およびモニタ対象トラフィックのニーズに合わせて調整できるカスタムのデフォルト設定があります。詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（27-45 ページ）を参照してください。

サーバレベル HTTP 正規化エンコード オプションの選択

ライセンス：Protection

サーバレベルの HTTP 正規化オプションを選択することで、HTTP トラフィック向けに正規化するエンコード タイプを指定し、このタイプのエンコードを含むトラフィックに対してイベントを生成させることができます。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ASCII エンコーディング

エンコードされた ASCII 文字をデコードし、ルール エンジンが ASCII エンコード URI でイベントを生成するかどうかを指定します。

このオプションのイベントを生成するには、ルール 119:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

UTF-8 エンコーディング

URI の標準 UTF-8 Unicode シーケンスをデコードします。

このオプションのイベントを生成するには、ルール 119:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Microsoft %U エンコーディング

%u とその後に続く 4 文字を使用する IIS %u エンコード スキームをデコードします。この 4 文字は、IIS Unicode コードポイントに関連する 16 進数のエンコード値です。

ヒント　正規のクライアントが %u エンコードを使用することはほとんどないため、シスコは、%u エンコードによってエンコードされている HTTP トラフィックをデコードすることを推奨します。

このオプションのイベントを生成するには、ルール 119:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

ベア バイト UTF-8 エンコーディング

ベア バイト エンコードをデコードします。ベア バイト エンコードでは、UTF-8 値のデコード時に非 ASCII 文字が有効な値として使用されます。

ヒント　ベア バイト エンコードにより、ユーザは IIS サーバをエミュレートし、非標準エンコードを正しく解釈することができます。正規のクライアントはこの方法で UTF-8 をエンコードしないため、シスコでは、このオプションを有効にすることを推奨しています。

このオプションのイベントを生成するには、ルール 119:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Microsoft IIS エンコーディング

Unicode コードポイント マッピングを使用してデコードします。

ヒント　これは主に攻撃と回避の試行で見られるため、シスコはこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:7 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

二重エンコーディング

要求 URI を 2 回通過し、それぞれでデコードを実行するようにすることで、IIS 二重エンコード トラフィックをデコードします。これは通常は攻撃シナリオでのみ検出されるため、シスコはこのオプションを有効にすることを推奨します。

このオプションのイベントを生成するには、ルール 119:2 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

マルチスラッシュ難読化

1 つの行内の複数のスラッシュを 1 つのスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:8 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

IIS バックスラッシュ難読化

バックスラッシュをスラッシュに正規化します。

このオプションのイベントを生成するには、ルール 119:9 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

ディレクトリ トラバーサル

ディレクトリ トラバーサルおよび自己参照用ディレクトリを正規化します。一部の Web サイトはディレクトリ トラバーサルを使用してファイルを参照するため、このタイプのトラフィックに対してイベントを生成するために、関連するプリプロセッサ ルールを有効にすると、誤検出が発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:10 および 119:11 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

タブ難読化

スペース区切り記号としてタブを使用する非 RFC 標準を正規化します。Apache やその他の非 IIS Web サーバは、URL の区切り文字としてタブ文字（0x09）を使用します。

（注） このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

このオプションのイベントを生成するには、ルール 119:12 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

無効な RFC デリミタ

URI データの改行（\ n）を正規化します。

このオプションのイベントを生成するには、ルール 119:13 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

webroot ディレクトリ トラバーサル

URL の初期ディレクトリを越えて横断するディレクトリ トラバーサルを検出します。

このオプションのイベントを生成するには、ルール 119:18 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

タブ URI デリミタ

URI の区切り文字としてタブ文字（0x09）を有効にします。Apache、新しいバージョンの IIS、およびその他の一部の Web サーバは、URL の区切り文字としてタブ文字を使用します。

(注)　このオプションの設定に関係なく、空白文字（0x20）がタブの前にある場合、HTTP Inspect プリプロセッサはそのタブをスペースとして扱います。

非 RFC 文字

対応するフィールドに追加された非 RFC 文字リストが、着信または発信 URI データ内に含まれている場合にそれを検出します。このフィールドを変更する場合は、バイト文字を表す 16 進表記を使用します。このオプションを設定する場合は、値を慎重に設定してください。非常に一般的な文字を使用すると、イベントが大量に発生する可能性があります。

このオプションのイベントを生成するには、ルール 119:14 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

最大チャンク エンコーディング サイズ

URI データで異常に大きなチャンク サイズを検出します。

このオプションのイベントを生成するには、ルール 119:16 および 119:22 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

パイプラインのデコードを無効にする

パイプライン処理された要求の HTTP デコードを無効にします。このオプションが無効である場合、パイプラインで待機する HTTP 要求には、デコードおよび分析は行われず、汎用パターン マッチングを使用した検査のみが行われるため、パフォーマンスが向上します。

Non-Strict URI 解析

Non-Strict URI 解析を有効にします。このオプションは、「GET /index.html abc xo qr \n」という形式の非標準 URI を受け入れるサーバでのみ使用します。このオプションを使用すると、デコーダは URI が 1 番目のスペースと 2 番目のスペースで囲まれているものと想定します。これは、2 番目のスペースの後に有効な HTTP 識別子がない場合でも同様です。

拡張 ASCII エンコーディング

HTTP 要求 URI の拡張 ASCII 文字の解析を有効にします。このオプションは、カスタム サーバ プロファイルでのみ使用可能であり、Apache、IIS、またはすべてのサーバ向けに提供されるデフォルト プロファイルでは使用できないことに注意してください。

HTTP サーバ オプションの設定

ライセンス：Protection

HTTP サーバ オプションを設定するには、次の手順に従います。HTTP サーバ オプションの詳細については、サーバレベル HTTP 正規化オプションの選択（27-36 ページ）およびサーバレベル HTTP 正規化エンコード オプションの選択（27-45 ページ）を参照してください。

サーバレベルの HTTP 設定オプションの設定方法:

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　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [HTTP 設定(HTTP Configuration)] を有効にしているかどうかに応じて、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。

[HTTP 設定(HTTP 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　次の 2 つの対処法があります。

- 新しいサーバ プロファイルを追加します。ページの左側で [サーバ(Servers)] の横にある追加アイコン( )をクリックします。[ターゲットの追加(Add Target)] ポップアップ ウィンドウが表示されます。クライアントの 1 つ以上の IP アドレスを [サーバ アドレス(Server Address)] フィールドに指定し、[OK] をクリックします。

  単一の IP アドレスまたはアドレス ブロック、あるいはこれらのいずれかまたは両方をカンマで区切ったリストを指定できます。リストに入力できる文字数は最大 496 文字、すべてのサーバ プロファイルで指定できるアドレス項目の総数は 256、作成できるプロファイルの総数はデフォルト プロファイルを含めて 255 です。FireSIGHT システムでの IPv4 および IPv6 アドレス ブロックの使用については、IP アドレスの表記規則(1-24 ページ)を参照してください。

  ターゲットベースのポリシーでトラフィックを処理する場合、特定するネットワークは、ターゲットベースのポリシーの設定対象となるネットワーク分析ポリシーによって処理されるネットワーク、ゾーン、VLAN のサブセットであるか、またはそれらに一致する必要があります。詳細については、ネットワーク分析ポリシーによる前処理のカスタマイズ(25-3 ページ)を参照してください。

  ページの左側のサーバ リストに新しい項目が表示され、選択されていることを示すために強調表示されます。[設定(Configuration)] セクションが更新され、追加したプロフィールの現行設定が反映されます。

- 既存のプロファイルの設定を変更します。ページ左側の [サーバ(Servers)] の下で追加したプロファイルの設定済みアドレスをクリックするか、または [デフォルト(default)] をクリックします。

選択した項目が強調表示され、[設定（Configuration）] セクションが更新され、選択したプロファイルの現行設定が表示されます。既存のプロファイルを削除するには、削除するプロファイルの横にある削除アイコン（ ）をクリックします。

手順 6　オプションで、[ネットワーク（Networks）] フィールドにリストされているアドレスを変更し、ページの他の領域をクリックします。

ページの左側で、強調表示されているアドレスが更新されます。

デフォルト プロファイルでは [ネットワーク（Network）] の設定を変更できないことに注意してください。デフォルト プロファイルは、別のプロファイルで指定されていないネットワーク上のすべてのサーバに適用されます。

手順 7　[ポート（Ports）] フィールドに、HTTP Inspect で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。

手順 8　サーバレベル HTTP 正規化オプションの選択（27-36 ページ）で説明するその他のオプションを変更できます。

手順 9　次の手順に従ってサーバ プロファイルを選択します。

- 独自のサーバ プロファイルを作成するには、[カスタム（Custom）] を選択します（詳細については、サーバレベル HTTP 正規化エンコード オプションの選択（27-45 ページ）を参照）。
- すべてのサーバに対して適切な標準のデフォルト プロファイルを使用するには、[すべて（All）] を選択します。
- デフォルトの IIS プロファイルを使用するには、[IIS] を選択します。
- デフォルトの Apache プロファイルを使用するには、[Apache] を選択します。

手順 10　[カスタム（Custom）] を選択すると、カスタム オプションが表示されます。

手順 11　プロファイルで、使用する HTTP デコード オプションを設定します。

使用可能な正規化オプションの詳細についてはサーバレベル HTTP 正規化オプションの選択（27-36 ページ）、参照してください。

手順 12　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。

追加の HTTP Inspect プリプロセッサ ルールの有効化

ライセンス：Protection

特定の設定オプションに関連付けられていない HTTP Inspect プリプロセッサ ルールのイベントを生成するには、次の表の「プリプロセッサ ルール GID：SID」列のルールを有効にできます。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

表 27-9　追加の HTTP Inspect プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
120:5	HTTP 応答トラフィックで UTF-7 エンコードが検出された場合にイベントが生成されます。UTF-7 は、SMTP トラフィックなどで 7 ビット パリティが必要な場合にのみ使用してください。
119:21	HTTP 要求ヘッダーに複数の `content-length` フィールドがある場合にイベントが生成されます。
119:24	HTTP 要求に複数の Host ヘッダーがある場合に、イベントが生成されます。
119:28 120:8	これらのルールを有効にする場合、イベントは生成されません。
119:32	トラフィックで HTTP バージョン 0.9 が検出されると、イベントが生成されます。TCP ストリームの設定も有効にする必要があることに注意してください。TCP ストリームの前処理の使用（29-22 ページ）を参照してください。
119:33	エスケープされていないスペースが HTTP URI に含まれている場合に、イベントが生成されます。
119:34	TCP 接続に 24 以上のパイプライン処理された HTTP 要求が含まれている場合に、イベントが生成されます。

Sun RPC プリプロセッサの使用

ライセンス：Protection

RPC（Remote Procedure Call）正規化では、フラグメント化された RPC レコードが 1 つのレコードに正規化されるので、ルール エンジンがそのレコード全体を検査できます。たとえば、攻撃者が RPC `admind` が実行されているポートの検出を試行するとします。一部の UNIX ホストは、RPC `admind` を使用してリモート分散システム タスクを実行します。ホストが弱い認証を実行する場合、悪意のあるユーザがリモート管理のコントロールを獲得できることがあります。Snort ID（SID）が 575 の標準テキスト ルール（ジェネレータ ID：1）は、この攻撃を検出するために、特定のロケーションでコンテンツを検索し、不適切な `portmap GETPORT` 要求を特定します。

ポート

トラフィックを正規化するポートを示します。インターフェイスで、複数のポートをカンマで区切って指定します。一般的な RPC ポートは 111 および 32771 です。ネットワークが他のポートに RPC トラフィックを送信する場合は、それらのポートの追加を検討してください。

RPC フラグメント化レコードの検出（Detect fragmented RPC records）

RPC フラグメント化レコードを検出します。

このオプションのイベントを生成するには、ルール 106:1 および 106:5 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

1 パケットの複数レコードの検出（Detect multiple records in one packet）

パケット（または再構成されたパケット）ごとに、複数の RPC 要求を検出します。

このオプションのイベントを生成するには、ルール 106:2 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

1 フラグメントを超えるフラグメント化レコード合計の検出（Detect fragmented record sums which exceed one fragment）

現在のパケット長を超える再構成されたフラグメント化レコード長を検出します。

このオプションのイベントを生成するには、ルール 106:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

1 パケットのサイズを超える単一フラグメント レコードの検出（Detect single fragment records which exceed the size of one packet）

部分的なレコードを検出します。

このオプションのイベントを生成するには、ルール 106:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Sun RPC プリプロセッサの設定

ライセンス：Protection

Sun RPC プリプロセッサを設定するには、次の手順を使用できます。Sun RPC プリプロセッサ設定オプションの詳細については、Sun RPC プリプロセッサの使用（27-50 ページ）を参照してください。

Sun RPC 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [Sun RPC 設定（Sun RPC Configuration）] を有効にしているかどうかに応じて、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。

[Sun RPC 設定（Sun RPC 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　[ポート（Ports）] フィールドに、RPC トラフィックをデコードするポートの番号を入力します。複数のポートを指定する場合は、カンマで区切ります。

手順 6　[Sun RPC 設定（Sun RPC Configuration）] ページの次の検出オプションを選択またはクリアできます。

- **RPC フラグメント化レコードの検出（Detect fragmented RPC records）**
- **1 パケットの複数レコードの検出（Detect multiple records in one packet）**
- **1 パケットを超えるフラグメント化レコード合計の検出（Detect fragmented record sums which exceed one packet）**
- **1 パケットのサイズを超える単一フラグメント レコードの検出（Detect single fragment records which exceed the size of one packet）**

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、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。

Session Initiation Protocol のデコード

ライセンス：Protection

Session Initiation Protocol（SIP）は、インターネット テレフォニー、マルチメディア会議、インスタント メッセージング、オンライン ゲーム、ファイル転送などのクライアント アプリケーションの 1 人以上のユーザに対し、1 つ以上のセッションのコール設定、変更、およびティアダウンを提供します。各 SIP 要求の *method* フィールドは要求の目的を示し、要求 URI により要求の送信先が指定されます。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。

SIP を使用してコールがセットアップされた後、後続の音声およびビデオによる通信は Real-time Transport Protocol（RTP）により処理されます。セッションのこの部分は、コール チャネル、データ チャネル、または音声/ビデオ データ チャネルと呼ばれることがあります。RTP は、データチャネル パラメータ ネゴシエーション、セッション通知、およびセッションへの招待のために、SIP メッセージ ボディ内で Session Description Protocol（SDP）を使用します。

SIP プリプロセッサは次の処理を実行します。

- SIP 2.0 トラフィックのデコードおよび分析
- SDP データが存在する場合はこのデータを含む SIP ヘッダーとメッセージ ボディを抽出し、抽出したデータを今後のインスペクションのためにルール エンジンに受け渡す
- 条件（SIP パケットにおける異常または既知の脆弱性、順序が正しくないコール シーケンス、または無効なコール シーケンス）が検出され、対応するプリプロセッサ ルールが有効である場合にイベントを生成する
- コール チャネルを無視する（オプション）

プリプロセッサは、SIP メッセージ ボディに組み込まれている SDP メッセージに示されているポートに基づいて RTP チャネルを識別しますが、RTP プロトコル インスペクションを実行しません。

SIP プリプロセッサを使用するときは、次の点に注意してください。

- UDP は通常、SIP でサポートされるメディア セッションを伝送します。UDP ストリームの前処理により、SIP プリプロセッサに対し SIP セッション トラッキングが提供されます。
- SIP ルール キーワードにより、SIP パケット ヘッダーまたはメッセージ ボディを指し示し、検出対象を特定の SIP メソッドまたはステータス コードのパケットに限定できます。詳細については、SIP キーワード（36-69 ページ）を参照してください。
- 有効である場合、関連するルール（ジェネレータ ID（GID）140）も有効にしていないと、抽出したデータをルール エンジンに送信するまで、プリプロセッサはイベントを生成しません。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- SIP プリプロセッサ オプションの選択（27-53 ページ）
- SIP プリプロセッサの設定（27-55 ページ）
- 追加の SIP プリプロセッサ ルールの有効化（27-55 ページ）

SIP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる SIP プリプロセッサ オプションについて以下で説明します。

[要求 URI の最大長（Maximum Request URI Length）]、[コール ID の最大長（Maximum Call ID Length）]、[要求名の最大長（Maximum Request Name Length）]、[送信元の最大長（Maximum From Length）]、[送信先の最大長（Maximum To Length）]、[経由の最大長（Maximum Via Length）]、[連絡先の最大長（Maximum Contact Length）]、および [コンテンツの最大長（Maximum Content Length）] オプションでは、1 ～ 65535 バイト、または 0 バイトを指定できます。0 を指定すると、関連するルールが有効であるかかどうかに関係なく、このオプションのイベント生成が無効になります。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SIP 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。

検査するメソッド（Methods to Check）

検出する SIP メソッドを指定します。次に示す現在定義されている SIP メソッドを指定できます。

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

メソッドでは大文字と小文字が区別されません。メソッド名には英字、数字、下線文字を使用できます。その他の特殊文字は使用できません。複数のメソッドはカンマで区切ります。

新しい SIP メソッドが今後定義される可能性があるため、設定には、現在定義されていない英字文字列を含めることができます。システムでは最大 32 個のメソッド（現在定義されている 21 個のメソッドと追加の 11 個のメソッド）がサポートされます。システムは、設定される未定義のメソッドをすべて無視します。

合計 32 個のメソッドには、このオプションに指定するメソッドの他に、侵入ルールで `sip_method` キーワードを使用して指定するメソッドも含まれます。詳細については、sip_method（36-70 ページ）を参照してください。

セッション内のダイアログ最大数（Maximum Dialogs within a Session）

ストリーム セッション内で許容されるダイアログの最大数を指定します。この数より多くのダイアログが作成されると、ダイアログの数が、指定されている最大数以下になるまで、最も古いダイアログから順に削除されます。また、ルール 140:27 が有効である場合にもイベントがトリガーとして使用されます。

1 ～ 4194303 の整数を指定できます。

要求 URI の最大長（Maximum Request URI Length）

[要求 URI（Request-URI）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:3 が有効である場合、URI がこれよりも長いとイベントがトリガーとして使用されます。[要求 URI（Request-URI）] フィールドは、要求の宛先のパスまたはページを示します。

コール ID の最大長（Maximum Call ID Length）

要求または応答の [コール ID（Call-ID）] ヘッダー フィールドの最大許容バイト数を指定します。ルール 140:5 が有効である場合、コール ID がこれよりも長いとイベントがトリガーとして使用されます。[コール ID（Call-ID）] フィールドによって、要求や応答内の SIP セッションが一意に識別されます。

要求名の最大長（Maximum Request Name Length）

要求名で許容される最大バイト数を指定します。要求名は、CSeq トランザクション ID に指定されるメソッドの名前です。ルール 140:7 が有効である場合、要求名がこれよりも長いとイベントがトリガーとして使用されます。

送信元の最大長（Maximum From Length）

要求または応答の [送信元（From）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:9 が有効である場合、[送信元（From）] がこれよりも長いとイベントがトリガーとして使用されます。[送信元（From）] フィールドは、メッセージの発信側を識別します。

送信先の最大長（Maximum To Length）

要求または応答の [送信先（To）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:11 が有効である場合、[送信先（To）] がこれよりも長いとイベントがトリガーとして使用されます。[送信先（To）] フィールドは、メッセージの受信側を識別します。

経由の最大長（Maximum Via Length）

要求または応答の [経由（Via）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:13 が有効である場合、[経由（Via）] がこれよりも長いとイベントがトリガーとして使用されます。[経由（Via）] フィールドには要求がたどるパスが示され、応答の場合は受信者情報が示されます。

連絡先の最大長（Maximum Contact Length）

要求または応答の [連絡先（Contact）] ヘッダー フィールドで許容される最大バイト数を指定します。ルール 140:15 が有効である場合、[連絡先（Contact）] がこれよりも長いとイベントがトリガーとして使用されます。[連絡先（Contact）] フィールドには、後続のメッセージについての連絡先を指定する URI が示されます。

コンテンツの最大長（Maximum Content Length）

要求または応答のメッセージ ボディのコンテンツで許容される最大バイト数を指定します。ルール 140:16 が有効である場合、コンテンツがこれよりも長いとイベントがトリガーとして使用されます。

音声/ビデオ データ チャネルを無視（Ignore Audio/Video Data Channel）

データ チャネル トラフィックのインスペクションを有効または無効にします。このオプションを有効にすると、プリプロセッサはその他の非データ チャネル SIP トラフィックのインスペクションを続行するので注意してください。

SIP プリプロセッサの設定

ライセンス：Protection

SIP プリプロセッサを設定するには、次の手順に従います。

SIP 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SIP 設定（SIP Configuration）] を有効にしているかどうかに応じて、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。

[SIP 設定（SIP 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　SIP プリプロセッサ オプションの選択（27-53 ページ）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。

追加の SIP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す SIP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の SIP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、こ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、ルール状態の設定（32-23 ページ）を参照してください。

表 27-10　追加の SIP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
140:1	プリプロセッサがモニタしている SIP セッションの数が、システムで許容される最大数である場合に、イベントが生成されます。
140:2	SIP 要求で [要求 URI（Request URI）] 必須フィールドが空である場合に、イベントが生成されます。
140:4	SIP 要求または応答の [コール ID（Call ID）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:6	SIP 要求または応答の CSeq フィールドのシーケンス番号値が、231 未満の 32 ビット符号なし整数ではない場合に、イベントが生成されます。
140:8	SIP 要求または応答で [送信元（From）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:10	SIP 要求または応答で [送信先（To）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:12	SIP 要求または応答で [経由（Via）] ヘッダー フィールドが空である場合に、イベントが生成されます。
140:14	SIP 要求または応答で [連絡先（Contact）] 必須ヘッダー フィールドが空である場合に、イベントが生成されます。
140:17	UDP トラフィック内の 1 つの SIP 要求または応答パケットに複数のメッセージが含まれている場合に、イベントが生成されます。SIP の旧バージョンでは複数メッセージがサポートされていますが、SIP 2.0 ではパケットあたり 1 メッセージだけがサポートされていることに注意してください。
140:18	UDP トラフィック内の SIP 要求または応答のメッセージ ボディの実際の長さが、SIP 要求または応答の [コンテンツ長（Content-Length）] ヘッダー フィールドの指定値と一致しない場合に、イベントが生成されます。
140:19	プリプロセッサが SIP 応答の [CSeq] フィールドのメソッド名を認識しない場合に、イベントが生成されます。
140:20	SIP サーバが、認証済み招待メッセージに対してチャレンジを送信しない場合に、イベントが生成されます。これは InviteReplay 請求攻撃の場合に発生することに注意してください。
140:21	コール セットアップの前にセッション情報が変更されると、イベントが生成されます。これは FakeBusy 請求攻撃の場合に発生することに注意してください。
140:22	応答ステータス コードが 3 桁の数値ではない場合に、イベントが生成されます。
140:23	[コンテンツ タイプ（Content-Type）] ヘッダー フィールドにコンテンツ タイプが指定されておらず、メッセージ ボディにデータが含まれている場合に、イベントが生成されます。
140:24	SIP バージョンが 1、1.1、または 2.0 のいずれでもない場合に、イベントが生成されます。
140:25	SIP 要求で、[CSeq] ヘッダーで指定されたメソッドとメソッド フィールドが一致しない場合に、イベントが生成されます。
140:26	プリプロセッサが SIP 要求のメソッド フィールドに指定されたメソッドを認識しない場合に、イベントが生成されます。

GTP コマンド チャネルの設定

ライセンス：Protection

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。GTP プリプロセッサは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージをインスペクションのためにルール エンジンに転送します。GTP コマンド チャネル トラフィックでエクスプロイトがあるかどうかを検査するには、`gtp_version`、`gtp_type`、および `gtp_info` ルール キーワードを使用します。

1 つの構成オプションで、プリプロセッサが GTP コマンド チャネル メッセージ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 GTP 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 27-11　GTP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
143:1	プリプロセッサが無効なメッセージの長さを検出すると、イベントが生成されます。
143:2	プリプロセッサが無効な情報要素の長さを検出すると、イベントが生成されます。
143:3	プリプロセッサが誤った順序の情報要素を検出すると、イベントが生成されます。

GTP プリプロセッサが GTP コマンド メッセージをモニタするポートを変更するには、次の手順を使用します。

GTP コマンド チャネルを設定するには、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　[アプリケーション層プリプロセッサ(Application Layer Preprocessors)] の下の [GTP コマンド チャネル設定(GTP Command Channel Configuration)] を有効にしているかどうかに応じて、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。

[GTP コマンド チャネル設定(GTP Command Channel Configuration)] ページが表示されます。

手順 5　オプションで、プリプロセッサが GTP コマンド メッセージ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。

IMAP トラフィックのデコード

ライセンス: Protection

Internet Message Application Protocol(IMAP)は、リモート IMAP サーバから電子メールを取得するときに使用されます。IMAP プリプロセッサはサーバ/クライアント IMAP4 トラフィックを検査し、関連するプリプロセッサ ルールが有効な場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ IMAP4 トラフィックの電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、特定のペイロード タイプを指し示す(36-108 ページ)を参照してください。

抽出とデコードでは、複数の添付ファイル(存在する場合)や、複数パケットにまたがる大きな添付ファイルなども処理されます。

IMAP プリプロセッサ ルールにより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。IMAP プリプロセッサ ルールのジェネレータ ID(GID)は 141 です。詳細については、ルール状態の設定(32-23 ページ)を参照してください。

詳細については、次の各項を参照してください。

- IMAP プリプロセッサ オプションの選択(27-58 ページ)
- IMAP プリプロセッサの設定(27-60 ページ)
- 追加の IMAP プリプロセッサ ルールの有効化(27-61 ページ)

IMAP プリプロセッサ オプションの選択

ライセンス: Protection

変更できる IMAP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル(存在する場合)および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] オプションの値が以下のポリシーで異なる場合は、最も大きい値が使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

詳細については、「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）」と「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。

注意 [Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7-Bit/8-Bit/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の値を変更すると、アクセス コントロール ポリシーの適用時に Snort プロセスが再開され、一時的にトラフィック検査が中断されます。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 の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

IMAP 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。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 141:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合は、ルール 141:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効な場合は、ルール 141:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。

IMAP プリプロセッサの設定

ライセンス：Protection

IMAP プリプロセッサを設定するには、次の手順に従います。IMAP プリプロセッサ設定オプションの詳細については、IMAP プリプロセッサ オプションの選択（27-58 ページ）を参照してください。

IMAP 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [IMAP 設定（IMAP Configuration）] を有効にしているかどうかに応じて、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。

[IMAP 設定（IMAP 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　IMAP トラフィックをデコードする必要があるポートを指定します。ポート番号が複数ある場合は、カンマで区切ります。

手順 6　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64 デコーディングの深さ（Base64 Decoding Depth）**
- **7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）**
- **Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）**

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

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、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。

追加の IMAP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す IMAP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の IMAP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、こ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、ルール状態の設定（32-23 ページ）を参照してください。

表 27-12　追加の IMAP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
141:1	プリプロセッサが RFC 3501 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
141:2	プリプロセッサが RFC 3501 に定義されていないサーバ応答を検出すると、イベントが生成されます。
141:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

POP トラフィックのデコード

ライセンス：Protection

Post Office Protocol（POP）は、リモート POP メール サーバから電子メールを取得するときに使用されます。POP プリプロセッサはサーバ/クライアント POP3 トラフィックを検査し、関連するプリプロセッサ ルールが有効である場合は、異常なトラフィックがあるとイベントを生成します。プリプロセッサは、クライアント/サーバ POP3 トラフィックで電子メール添付ファイルを抽出してデコードし、添付ファイル データをルール エンジンに送信することもできます。添付ファイル データを指し示すには、侵入ルールで `file_data` キーワードを使用します。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

抽出とデコードでは、複数の添付ファイル（存在する場合）や、複数パケットにまたがる大きな添付ファイルなども処理されます。

POP プリプロセッサ ルールにより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。POP プリプロセッサ ルールのジェネレータ ID（GID）は 142 です。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の各項を参照してください。

- POP プリプロセッサ オプションの選択（27-62 ページ）
- POP プリプロセッサの設定（27-64 ページ）
- 追加の POP プリプロセッサ ルールの有効化（27-65 ページ）

POP プリプロセッサ オプションの選択

ライセンス：Protection

変更できる POP プリプロセッサ オプションを以下で説明します。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、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の間で異なる場合は、最も大きな値が使用されることに注意してください。

注意　[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7-Bit/8-Bit/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の値を変更すると、アクセス コントロール ポリシーの適用時に Snort プロセスが再開され、一時的にトラフィック検査が中断されます。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 の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

POP 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。

Base64 デコーディングの深さ（Base64 Decoding Depth）

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 142:4 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

デコードを必要としない各 MIME 電子メール添付ファイルから抽出するデータの最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。

quoted-printable デコードが有効な場合は、ルール 142:6 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

各 Unix-to-Unix エンコード（UU エンコード）電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。

Unix-to-Unix デコードが有効な場合は、ルール 142:7 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

POP プリプロセッサの設定

ライセンス：Protection

POP プリプロセッサを設定するには、次の手順に従います。POP プリプロセッサ設定オプションの詳細については、POP プリプロセッサ オプションの選択（27-62 ページ）を参照してください。

POP 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [POP 設定（POP Configuration）] を有効にしているかどうかに応じて、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。

[POP 設定（POP 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　IMAP トラフィックをデコードする必要があるポートを指定します。ポート番号が複数ある場合は、カンマで区切ります。

手順 6　次に示す電子メール添付ファイル タイプの任意の組み合わせから抽出してデコードするデータの最大バイト数を指定します。

- **Base64 デコーディングの深さ（Base64 Decoding Depth）**
- **7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）**
- **Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）**

タイプごとに 1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

添付ファイル データを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

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、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。

追加の POP プリプロセッサ ルールの有効化

ライセンス：Protection

次の表に示す POP プリプロセッサ ルールは、特定の設定オプションに関連付けられていません。その他の POP プリプロセッサ ルールと同様に、これらのルールによってイベントを生成する場合は、こ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、ルール状態の設定（32-23 ページ）を参照してください。

表 27-13　追加の POP プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
142:1	プリプロセッサが RFC 1939 に定義されていないクライアント コマンドを検出すると、イベントが生成されます。
142:2	プリプロセッサが RFC 1939 に定義されていないサーバ応答を検出すると、イベントが生成されます。
142:3	プリプロセッサが使用しているメモリの量が、システムでの最大許容量に達している場合に、イベントが生成されます。この時点で、プリプロセッサはメモリが使用可能になるまでデコードを停止します。

SMTP トラフィックのデコード

ライセンス：Protection

SMTP プリプロセッサはルール エンジンに対し、SMTP コマンドを正規化するように指示します。このプリプロセッサは、クライアント/サーバ トラフィックで電子メール添付ファイルを抽出してデコードします。またソフトウェアのバージョンによっては、SMTP トラフィックによりトリガーされた侵入イベントの表示時にコンテキストを提供するため、電子メール ファイル名、アドレス、およびヘッダー データを抽出します。

SMTP プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）124 の SMTP プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

詳細については、次の項を参照してください。

- SMTP デコードについて（27-65 ページ）
- SMTP デコードの設定（27-70 ページ）
- SMTP 最大デコード メモリ アラートの有効化（27-73 ページ）

SMTP デコードについて

ライセンス：Protection

正規化を有効または無効にし、SMTP デコーダが検出する異常トラフィックのタイプを制御するオプションを設定できます。

MIME 電子メール添付ファイルのデコードが不要な場合のデコードまたは抽出では、複数の添付ファイル（存在する場合）および複数パケットにまたがる大きな添付ファイルが処理されることに注意してください。

[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の各オプションの値が、アクセス コントロール ポリシーに関連付けられている侵入ポリシーと、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の間で異なる場合は、最も大きな値が使用されることに注意してください。

注意　[Base64 デコーディングの深さ（Base64 Decoding Depth）]、[7-Bit/8-Bit/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）]、[Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）]、または [Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）] の値を変更すると、アクセス コントロール ポリシーの適用時に Snort プロセスが再開され、一時的にトラフィック検査が中断されます。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 の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

ポート

SMTP トラフィックを正規化するポートを指定します。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。

ステートフル インスペクション（Stateful Inspection）

選択されている場合、SMTP デコーダは状態を保存し、各パケットのセッション コンテキストを提供し、再構成されたセッションだけを検査します。選択されていない場合、セッション コンテキストなしで個々のパケットを分析します。

正規化（Normalize）

[すべて（All）] に設定すると、すべてのコマンドが正規化されます。コマンドの後に複数のスペース文字があるかどうかを確認します。

[なし（None）] に設定すると、コマンドは正規化されません。

[Cmds] に設定すると、[カスタム コマンド（Custom Commands）] にリストされているコマンドが正規化されます。

カスタム コマンド（Custom Commands）

[正規化（Normalize）] が [Cmds] に設定されている場合に、リストされているコマンドが正規化されます。

正規化する必要があるコマンドをテキスト ボックスに指定します。コマンドの後に複数のスペース文字があるかどうかを確認します。

スペース文字（ASCII 0x20）とタブ文字（ASCII 0x09）は、正規化のためにスペース文字としてカウントされます。

データを無視（Ignore Data）

メール データを処理せず、MIME メール ヘッダー データだけを処理します。

TLS データを無視（Ignore TLS Data）

Transport Layer Security プロトコルで暗号化されたデータを処理しません。

アラートなし（No Alerts）

関連するプリプロセッサ ルールが有効である場合に、侵入イベントを無効にします。

不明なコマンドの検出（Detect Unknown Commands）

SMTP トラフィックで不明なコマンドを検出します。

このオプションのイベントを生成するには、ルール 124:5 および 124:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

コマンドラインの最大長（Max Command Line Len）

SMTP コマンドラインがこの値より長い場合にそのことを検出します。コマンドラインの長さを検出しない場合は、0 を指定します。

RFC 2821（Network Working Group による Simple Mail Transfer Protocol 仕様）では、コマンドラインの最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

ヘッダー行の最大長（Max Header Line Len）

SMTP データ ヘッダー行がこの値より長い場合にそのことを検出します。データ ヘッダー行の長さを検出しない場合は、0 を指定します。

このオプションのイベントを生成するには、ルール 124:2 および 124:7 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

応答行の最大長（Max Response Line Len）

SMTP 応答行がこの値より長い場合にそのことを検出します。応答行の長さを検出しない場合は、0 を指定します。

RFC 2821 では、応答行の最大長として 512 が推奨されています。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

代替のコマンドラインの最大長（Alt Max Command Line Len）

指定のコマンドの SMTP コマンドラインがこの値より長い場合にそのことを検出します。指定したコマンドのコマンドライン長を検出しない場合は、0 を指定します。多数のコマンドに対して、さまざまなデフォルト ライン長が設定されています。

この設定は、指定されたコマンドの [コマンドラインの最大長（Max Command Line Len）] の設定をオーバーライドします。

このオプションのイベントを生成するには、ルール 124:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

無効なコマンド（Invalid Commands）

これらのコマンドがクライアント側から送信された場合にそのことを検出します。

このオプションのイベントを生成するには、ルール 124:5 および 124:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

有効なコマンド（Valid Commands）

このリストのコマンドを許可します。

このリストが空の場合でも、プリプロセッサにより許可される有効なコマンドは、ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR です。

（注）　RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

このオプションのイベントを生成するには、ルール 124:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

データ コマンド（Data Commands）

RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

バイナリ データ コマンド（Binary Data Commands）

RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

認証コマンド（Authentication Commands）

クライアントおよびサーバ間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

xlink2state の検出（Detect xlink2state）

X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出します。インライン展開では、システムはこれらのパケットをドロップすることもできます。

このオプションのイベントを生成するには、ルール 124:8 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Base64 デコーディングの深さ（Base64 Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、すべての Base64 データをデコードする場合は 0 を指定します。Base64 データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

4 で割り切れない正の値は、次に大きい 4 の倍数に切り上げられることに注意してください。ただし 65533、65534、および 65535 は 65532 に切り下げられます。

Base64 デコードが有効である場合、ルール 124:10 を有効にして、デコードの失敗時にイベントを生成することができます。デコードは、エンコードが誤っている場合やデータが破損している場合などに失敗する可能性があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

このオプションは、廃止されたオプション [MIME デコーディングの有効化（Enable MIME Decoding）] および [MIME デコーディングの最大の深さ（Maximum MIME Decoding Depth）] の代わりに使用されます。廃止されたこれらのオプションは、既存の侵入ポリシーでは後方互換性を維持する目的で引き続きサポートされています。

7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）

[データを無視（Ignore Data）] が無効である場合、デコードを必要としない各 MIME 電子メール添付ファイルから抽出する最大バイト数を指定します。これらの添付ファイル タイプには、7 ビット、8 ビット、バイナリ、およびさまざまなマルチパート コンテンツ タイプ（プレーンテキスト、jpeg イメージ、mp3 ファイルなど）があります。1 ～ 65535 バイトを指定するか、または、パケットのすべてのデータを抽出する場合は 0 を指定します。非デコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータを抽出しません。

Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）

[データを無視（Ignore Data）] が無効な場合、各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。

1 ～ 65535 バイトを指定するか、または、パケットのすべての QP エンコード データをデコードする場合は 0 を指定します。QP エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

quoted-printable デコードが有効な場合は、ルール 124:11 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）

[データを無視（Ignore Data）] が無効な場合、各 Unix-to-Unix（UU エンコード）電子メール添付ファイルから抽出してデコードする最大バイト数を指定します。1 ～ 65535 バイトを指定するか、または、パケットのすべての UU エンコード データをデコードする場合は 0 を指定します。UU エンコード データを無視するには、-1 を指定します。[データを無視（Ignore Data）] が選択されている場合、プリプロセッサはデータをデコードしません。

Unix-to-Unix デコードが有効な場合は、ルール 124:13 を有効にして、デコードの失敗時にイベントを生成することができます。デコードが失敗するのは、エンコードが誤っている場合やデータが破損している場合などです。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

MIME 添付ファイル名のログ（Log MIME Attachment Names）

MIME Content-Disposition ヘッダーからの MIME 添付ファイル名の抽出を有効にして、セッションで生成されるすべての侵入イベントにこのファイル名を関連付けます。複数ファイル名がサポートされています。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール添付（Email Attachment）] 列に、イベントに関連付けられているファイル名が表示されます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

受信者アドレスのログ（Log To Addresses）

SMTP RCPT TO コマンドからの受信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの受信者アドレスに関連付けます。複数の受信者がサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール受信者（Email Recipient）] 列に、イベントに関連付けられている受信者が表示されます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

送信者アドレスのログ（Log From Addresses）

SMTP MAIL FROM コマンドからの送信者の電子メール アドレスの抽出を有効にし、セッションで生成されるすべての侵入イベントにこの送信者アドレスを関連付けます。複数の送信者アドレスがサポートされます。

このオプションが有効である場合、侵入イベントのテーブル ビューの [電子メール送信者（Email Sender）] 列に、イベントに関連付けられている送信者が表示されます。詳細については、侵入イベントについて（41-12 ページ）を参照してください。

ヘッダーのログ（Log Headers）

電子メール ヘッダーの抽出を有効にします。抽出されるバイト数は、[ヘッダーのログの深さ（Header Log Depth）] に指定されている値によって決まります。

キーワード `content` または `protected_content` を使用して、電子メール ヘッダー データをパターンとして使用する侵入ルールを作成できます。侵入イベント パケット ビューに、抽出された電子メール ヘッダーが表示されます。詳細については、コンテンツ一致の制約（36-20 ページ）とパケット ビューの使用（41-25 ページ）を参照してください。

ヘッダーのログの深さ（Header Log Depth）

[ヘッダーのログ（Log Headers）] が有効である場合、抽出する電子メールヘッダーのバイト数を指定します。0 ～ 20480 バイトを指定できます。値 0 を指定すると、[ヘッダーのログ（Log Headers）] が無効になります。

SMTP デコードの設定

ライセンス：Protection

侵入ポリシーの [SMTP の設定（SMTP Configuration）] ページを使用して、SMTP 正規化を設定できます。SMTP プリプロセッサ設定オプションの詳細については、SMTP デコードについて（27-65 ページ）を参照してください。

SMTP デコード オプションの設定方法：

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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SMTP 設定（SMTP Configuration）] を有効にしているかどうかに応じて、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。

[SMTP 設定（SMTP Configuration）] ページが表示されます。次の図は、防御センター パケット ビューを示します。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　SMTP トラフィックをデコードする必要があるポートを、カンマで区切って指定します。

手順 6　SMTP パケットを含む再構成された TCP ストリームを調べるには、[ステートフル インスペクション（Stateful Inspection）] を選択します。再構成されていない SMTP パケットだけを検査するには、[ステートフル インスペクション（Stateful Inspection）] をクリアします。

手順 7　正規化オプションを設定します。

- すべてのコマンドを正規化するには、[すべて（All）] を選択します。
- [カスタム コマンド（Custom Commands）] に指定されているコマンドだけを正規化するには、[Cmds] を選択して、正規化するコマンドを指定します。複数のコマンドはスペースで区切ります。
- コマンドを正規化しない場合は、[なし（None）] を選択します。
- MIME メール ヘッダー データ以外のメール データを無視するには、[データを無視（Ignore Data）] をオンにします。
- Transport Security Layer プロトコルで暗号化されたデータを無視するには、[TLS データを無視（Ignore TLS Data）] をオンにします。
- 関連するプリプロセッサ ルールが有効である場合にイベント生成を無効にするには、[アラートなし（No Alerts）] をオンにします。
- SMTP データで不明なコマンドを検出するには、[不明なコマンドの検出（Detect Unknown Commands）] を選択します。

手順 8　[コマンドラインの最大長（Max Command Line Len）] フィールドに、コマンドラインの最大長を指定します。

手順 9　[ヘッダー行の最大長（Max Header Line Len）] フィールドに、データ ヘッダー行の最大長を指定します。

手順 10　[応答行の最大長（Max Response Line Len）] フィールドに、応答行の最大長を指定します。

（注）　RCPT TO および MAIL FROM は SMTP コマンドです。プリプロセッサ設定では、コマンド名 RCPT と MAIL がそれぞれ使用されます。プリプロセッサはコード内で RCPT および MAIL を正しいコマンド名にマッピングします。

手順 11　必要に応じて、[代替のコマンドラインの最大長（Alt Max Command Line Len）] の横にある [追加（Add）] をクリックして、代替最大コマンドライン長を指定するコマンドを追加します。続いてライン長を指定し、このライン長を適用するコマンドをスペースで区切って指定します。

手順 12　[無効なコマンド（Invalid Commands）] フィールドに、無効として扱う検出対象コマンドを指定します。複数のコマンドはスペースで区切ります。

手順 13　[有効なコマンド（Valid Commands）] フィールドに、有効として扱うコマンドを指定します。複数のコマンドはスペースで区切ります。

（注）　[有効なコマンド（Valid Commands）] リストが空の場合でも、プリプロセッサにより有効なコマンドとして許可されるコマンドは、ATRN、AUTH、BDAT、DATA、DEBUG、EHLO、EMAL、ESAM、ESND、ESOM、ETRN、EVFY、EXPN、HELO、HELP、IDENT、MAIL、NOOP、QUIT、RCPT、RSET、SAML、SOML、SEND、ONEX、QUEU、STARTTLS、TICK、TIME、TURN、TURNME、VERB、VRFY、X-EXPS、X-LINK2STATE、XADR、XAUTH、XCIR、XEXCH50、XGEN、XLICENSE、XQUE、XSTA、XTRN、XUSR です。

手順 14　[データ コマンド（Data Commands）] フィールドに、RFC 5321 に基づく SMTP DATA コマンドによるデータの送信と同じ方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

手順 15　[バイナリ データ コマンド（Binary Data Commands）] フィールドに、RFC 3030 に基づく BDAT コマンドによるデータの送信と類似の方法でデータ送信を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

手順 16　[認証コマンド（Authentication Commands）] フィールドに、クライアントとサーバの間で認証交換を開始するコマンドを指定します。複数のコマンドはスペースで区切ります。

手順 17　X-Link2State Microsoft Exchange バッファ データ オーバーフロー攻撃の一部であるパケットを検出するには、[xlink2state の検出（Detect xlink2state）] を選択します。

手順 18　各種電子メール添付ファイルで抽出およびデコードするデータの最大バイト数を指定するには、次に示す添付ファイル タイプの値を指定します。

- **Base64 デコーディングの深さ（Base64 Decoding Depth）**
- **7 ビット/8 ビット/バイナリのデコーディングの深さ（7-Bit/8-Bit/Binary Decoding Depth）**（プレーン テキスト、jpeg イメージ、mp3 ファイルなどの各種マルチパート コンテンツ タイプを含む）
- **Quoted-Printable（QP）のデコーディングの深さ（Quoted-Printable Decoding Depth）**
- **Unix-to-Unix（UU）のデコーディングの深さ（Unix-to-Unix Decoding Depth）**

1 ～ 65535 バイトを指定するか、または、当該タイプのパケットのすべてのデータを抽出し、必要に応じてデコードする場合は 0 を指定します。添付ファイル タイプのデータを無視するには、-1 を指定します。

抽出したデータを検査するには、侵入ルールで `file_data` キーワードを使用できます。詳細については、特定のペイロード タイプを指し示す（36-108 ページ）を参照してください。

また、クロスパケット データや複数の TCP セグメントにわたるデータを抽出してデコードするには、SMTP の [ステートフル インスペクション（Stateful Inspection）] オプションも選択する必要があります。

手順 19　SMTP トラフィックによりトリガーとして使用された侵入イベントとコンテキスト情報を関連付けるためのオプションを設定します。

- 侵入イベントに関連付ける MIME 添付ファイル名を抽出できるようにするには、[MIME 添付ファイル名のログ（Log MIME Attachment Names）] を選択します。
- 受信者の電子メール アドレスを抽出できるようにするには、[受信者アドレスのログ（Log To Addresses）] を選択します。
- 侵入イベントに関連付ける送信者の電子メール アドレスを抽出できるようにするには、[送信者アドレスのログ（Log From Addresses）] を選択します。
- 侵入イベントに関連付ける電子メール ヘッダーを抽出し、電子メール ヘッダーを検査するルールを作成できるようにするには、[ヘッダーのログ（Log Headers）] を選択します。

  ヘッダー情報は侵入イベント パケット ビューに表示されることに注意してください。また、キーワード `content` または `protected_content` と共に電子メール ヘッダー データをパターンとして使用する侵入ルールを作成することもできます。詳細については、イベント情報の表示（41-27 ページ）とコンテンツ一致の検索（36-16 ページ）を参照してください。

オプションで [ヘッダーのログの深さ(Header Log Depth)] に、抽出する電子メール ヘッダーのバイト数 0 ～ 20480 を指定できます。値 0 を指定すると、[ヘッダーのログ(Log Headers)] が無効になります。

手順 20 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。

SMTP 最大デコード メモリ アラートの有効化

ライセンス: Protection

有効になっているプリプロセッサが次のタイプのエンコード データのデコードに使用しているメモリの容量がシステムの最大許容メモリ量に達した場合にイベントを生成するには、SMTP プリプロセッサ ルール 124:9 を有効にします。

- Base64
- 7 ビット/8 ビット/バイナリ
- Quoted-printable
- Unix-to-Unix

最大デコード メモリを超えた場合、メモリが使用可能になるまで、プリプロセッサはこれらのタイプのエンコード データのデコードを停止します。このプリプロセッサ ルールは、1 つの特定の設定オプションに関連付けられていません。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。

SSH プロプロセッサによるエクスプロイトの検出

ライセンス: Protection

SSH プリプロセッサは、チャレンジレスポンス バッファ オーバーフロー エクスプロイト、CRC-32 エクスプロイト、SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト、プロトコル不一致、不正な SSH メッセージ方向を検出します。このプリプロセッサは、バージョン 1 または 2 ではないバージョン文字列も検出します。

チャレンジレスポンス バッファ オーバーフロー攻撃と CRC-32 攻撃はいずれもキー交換の後に発生するので、暗号化されています。いずれの攻撃でも、20 KB を超える普通よりも大きなペイロードが認証チャレンジ直後にサーバに送信されます。CRC-32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジレスポンス バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。バージョン文字列は、セッションの開始時に読み取られます。バージョン文字列の違いを除き、この両方の攻撃は同様に扱われます。

SecureCRT SSH エクスプロイトとプロトコル不一致攻撃は、鍵交換前に接続をセキュリティで保護しようとするときに発生します。SecureCRT エクスプロイトでは、非常に長いプロトコル ID 文字列がクライアントに送信され、これが原因でバッファ オーバーフローが発生します。プロトコル不一致は、非 SSH クライアント アプリケーションがセキュア SSH サーバに接続しようとした場合、またはサーバとクライアントのバージョン番号が一致しない場合に発生します。

指定のポートまたは一連のポートでトラフィックを検査するか、または SSH トラフィックを自動的に検出するように、プリプロセッサを設定できます。指定バイト数に達するまでに指定数の暗号化パケットが渡されたか、指定パケット数に達するまでにバイト数が指定最大バイト数を超えるまで、SSH トラフィックの検査が続行されます。最大バイト数を超えた場合は、CRC-32（SSH バージョン 1）または チャレンジレスポンス バッファ オーバーフロー（SSH バージョン 2）攻撃が発生したとみなされます。また、SecureCRT エクスプロイト、プロトコル不一致、および不正なメッセージ方向を検出できます。プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

SSH プリプロセッサを使用するときは、次の点に注意してください。

- ジェネレータ ID（GID）128 の SSH プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があります。詳細については、ルール状態の設定（32-23 ページ）を参照してください。
- SSH プリプロセッサは、ブルート フォース攻撃には対処しません。ブルート フォース攻撃の試行については、動的ルール状態の追加（32-34 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。

- SSH プリプロセッサ オプションの選択（27-74 ページ）
- SSH プリプロセッサの設定（27-77 ページ）

SSH プリプロセッサ オプションの選択

ライセンス：Protection

このセクションでは、SSH プリプロセッサを設定するときに使用できるオプションについて説明します。

次のいずれかが発生すると、プリプロセッサはセッションのトラフィックの検査を停止します。

- この数の暗号化パケットで、サーバとクライアント間で有効な交換が行われた場合。接続は続行します。
- 検査対象の暗号化パケットの数に達する前に、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] に達した場合。この場合、攻撃があったものと想定されます。

[検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）] に達するまでの有効な各サーバ応答により、[サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）] がリセットされ、パケット カウントが続行します。

次に示す SSH のプリプロセッサの設定例で説明します。

- [サーバ ポート（Server Ports）]：22
- [自動検出ポート（Autodetect Ports）]：off
- [プロトコル バージョン ストリングの最大長（Maximum Length of Protocol Version String）]：80
- [検査する暗号化パケットの数（Number of Encrypted Packets to Inspect）]：25
- [サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）]：19,600
- 検出オプションはすべて有効です。

この例では、プリプロセッサはポート 22 のトラフィックだけを検査します。つまり、自動検出が無効であるため、指定されたポートでのみ検査をします。

また、次のいずれかが発生すると、この例のプリプロセッサはトラフィックの検査を停止します。

- クライアントが 25 個の暗号化パケットを送信したが、すべてのパケットのデータ合計が 19,600 バイト以下であった。攻撃はなかったと想定されます。
- クライアントが、25 個の暗号化パケットで 19,600 バイトを超えるデータを送信した。この場合、この例のセッションは SSH バージョン 2 セッションであるため、プリプロセッサはこの攻撃がチャレンジレスポンス バッファ オーバーフロー攻撃であるとみなします。

この例のプリプロセッサは、トラフィックの処理時に以下の状況が発生しているかどうかも検出します。

- 80 バイトより長いバージョン文字列によりトリガーとして使用されるサーバ オーバーフロー（これは SecureCRT エクスプロイトを示します）
- プロトコルの不一致
- 誤った方向に流れるパケット

最後に、プリプロセッサは、バージョン 1 または 2 以外のすべてのバージョン文字列を自動的に検出します。

以下の説明でプリプロセッサ ルールが言及されていない場合、オプションにはプリプロセッサ ルールが関連付けられていません。

サーバ ポート（Server Ports）

SSH プリプロセッサがトラフィックを検査する必要があるポートを指定します。

1 つのポート、または複数のポートをカンマで区切ったリストを設定できます。

自動検出ポート（Autodetect Ports）

SSH トラフィックを自動的に検出するようにプリプロセッサを設定します。

このオプションが選択されている場合、プリプロセッサはすべてのトラフィックで SSH バージョン番号を検査します。クライアント パケットにもサーバ パケットにもバージョン番号が含まれていない場合は、処理が停止します。無効である場合、プリプロセッサは [サーバ ポート（Server Ports）] オプションで指定されているトラフィックだけを検査します。

検査する暗号化パケットの最大数（Number of Encrypted Packets to Inspect）

セッションあたりの検査対象の暗号化パケットの数を指定します。

このオプションをゼロに設定すると、すべてのトラフィックの通過が許可されます。

検査対象の暗号化パケットの数を減らすと、一部の攻撃が検出されなくなることがあります。検査対象の暗号化パケットの数を増やすと、パフォーマンスに悪影響を及ぼす可能性があります。

サーバ応答がないまま送信されたバイト数（Number of Bytes Sent Without Server Response）

SSH クライアントが、応答を得ることなく、サーバに送信できる最大バイト数を指定します。この最大バイト数を超えると、チャレンジレスポンス バッファ オーバーフロー攻撃または CRC-32 攻撃であるとみなされます。

プリプロセッサがチャレンジレスポンス バッファ オーバーフローまたは CRC-32 エクスプロイトを誤検出する場合は、このオプションの値を増やしてください。

プロトコル バージョン ストリングの最大長（Maximum Length of Protocol Version String）

サーバのバージョン文字列の最大許容バイト数を指定します。この値を超えると、SecureCRT エクスプロイトとみなされます。

チャレンジレスポンス バッファ オーバーフロー攻撃の検出（Detect Challenge-Response Buffer Overflow Attack）

チャレンジレスポンス バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:1 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

SSH1 CRC-32 攻撃の検出（Detect SSH1 CRC-32 Attack）

CRC-32 エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:2 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

サーバ オーバーフローの検出（Detect Server Overflow）

SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイトの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:3 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

プロトコル不一致の検出（Detect Protocol Mismatch）

プロトコル不一致の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:4 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

正しくないメッセージ方向の検出（Detect Bad Message Direction）

トラフィックのフロー方向が正しくない場合（つまり、推定されるサーバがクライアント トラフィックを生成したり、クライアントがサーバ トラフィックを生成したりした場合）の検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:5 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

特定のペイロードに正しくないペイロード サイズの検出（Detect Payload Size Incorrect for the Given Payload）

SSH パケットに指定された長さが IP ヘッダーに指定されている合計長と矛盾する場合や、メッセージが切り捨てられる場合、つまり完全な SSH ヘッダーを形成できる十分なデータがない場合などの、誤ったペイロード サイズのパケットの検出を有効または無効にします。

このオプションのイベントを生成するには、ルール 128:6 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

正しくないバージョン ストリングの検出（Detect Bad Version String）

有効である場合、プリプロセッサは、設定していない場合でもバージョン 1 または 2 以外のバージョン文字列を検出することに注意してください。

このオプションのイベントを生成するには、ルール 128:7 を有効にします。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

SSH プリプロセッサの設定

ライセンス：Protection

このセクションでは、SSH プリプロセッサを設定する方法について説明します。

SSH 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSH 設定（SSH Configuration）] を有効にしているかどうかに応じて、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。

[SSH 設定（SSH 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　[SSH の設定（SSH Configuration）] プリプロセッサ ページのすべてのオプションを変更できます。詳細については、SSH プリプロセッサ オプションの選択（27-74 ページ）を参照してください。

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。

SSL プリプロセッサの使用

ライセンス：機能に依存

SSL プリプロセッサでは SSL インスペクションを設定できます。SSL インスペクションは、暗号化トラフィックのブロック、暗号化トラフィックの復号化、アクセス コントロールによるトラフィックの検査を実行します。SSL インスペクションが設定されているかどうかに関わらず、SSL プリプロセッサは、トラフィックで検出された SSL ハンドシェイク メッセージを分析し、セッションを暗号化するタイミングを決定します。暗号化トラフィックを識別することにより、システムは暗号化ペイロードの侵入およびファイル インスペクションを停止できます。これによって、誤検出が減少し、パフォーマンスが向上します。詳細については、トラフィック復号の概要（19-1 ページ）とアクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

SSL プリプロセッサは、暗号化トラフィックを検査して Heartbleed バグを悪用する試みを検出し、そのような悪用を検出するとイベントを生成します。

SSL プリプロセッサを使用して暗号化トラフィックを復号化する場合、ライセンスは必要ありません。マルウェアや侵入に対する暗号化ペイロードのインスペクションの停止、Heartbleed バグの悪用の検出を含め、すべての SSL プリプロセッサ機能には Protection ライセンスが必要です。

(注)　システム付属のネットワーク分析ポリシーは、デフォルトで SSL プリプロセッサを有効にします。暗号化トラフィックがネットワークを通過することを予想している場合は、カスタム展開で SSL プリプロセッサを無効にしないことを推奨します。

詳細については、次の項を参照してください。

- SSL 前処理について（27-78 ページ）
- SSL プリプロセッサ ルールの有効化（27-79 ページ）
- SSL プリプロセッサの設定（27-80 ページ）

SSL 前処理について

ライセンス：Protection

SSL インスペクションを設定すると、SSL プリプロセッサは暗号化データに対する侵入およびファイル インスペクションを停止して、SSL ポリシーにより暗号化トラフィックを検査します。これにより誤検出を排除できます。SSL プリプロセッサは、SSL ハンドシェイクを検査するときに状態情報を保持し、そのセッションの状態と SSL バージョンの両方を追跡します。セッションの状態が暗号化されていることをプリプロセッサが検出すると、そのセッションのトラフィックは暗号化されているものとしてシステムによりマークされます。暗号化が確定した場合に暗号化セッションにおけるすべてのパケット処理を停止し、Heartbleed のバグを悪用する試みが検出された場合にイベントを生成するように、システムを設定できます。

パケットごとに、IP ヘッダー、TCP ヘッダー、および TCP ペイロードがトラフィックに含まれており、このトラフィックが SSL 前処理用に指定されているポートで発生することが SSL プリプロセッサにより確認されます。次に示す状況では、対象トラフィックについて、トラフィックが暗号化されているかどうかが判別されます。

- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、サーバとクライアントの両方からの完了メッセージ、および Application レコードが存在するが Alert レコードがない各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効にされておらず、Alert レコードによる応答がない Application レコードが存在する各側からの 1 つ以上のパケットが、セッションに含まれている。
- システムがセッションのすべてのパケットを監視し、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、クライアントからの完了メッセージ、および Application レコードが存在するが Alert レコードがないクライアントからの 1 つ以上のパケットが、セッションに含まれている。
- システムがトラフィックの一部を検出せず、[サーバ側のデータを信頼する（Server side data is trusted）] が有効であり、Alert レコードによる応答がない Application レコードが存在するクライアントからの 1 つ以上のパケットが、セッションに含まれている。

暗号化トラフィックの処理を停止することを選択する場合、セッションが暗号化されているものとしてマークされると、そのセッションのその後のパケットは無視されます。

また、SSL ハンドシェイク時、プリプロセッサはハートビート要求と応答をモニタします。プリプロセッサは、以下を検出したときにイベントを生成します。

- ペイロード自体よりも大きいペイロード長の値を含むハートビート要求
- [ハートビートの最大長（Max Heartbeat Length）] フィールドに格納されている値よりも大きいハートビート応答

（注）　ルール内で SSL 状態またはバージョン情報を使用するには、キーワード `ssl_state` および `ssl_version` をルールに追加します。詳細については、セッションからの SSL 情報の抽出（36-60 ページ）を参照してください。

SSL プリプロセッサ ルールの有効化

ライセンス：Protection

有効である場合、SSL プリプロセッサは、SSL セッション開始時に交換されるハンドシェイクと鍵交換メッセージの内容を検査します。セッションが暗号化されると、侵入やマルウェア対するトラフィックの検査を一時停止できます。SSL インスペクションを設定した場合、SSL プリプロセッサは、ユーザがアクセス コントロールによって復号化、ブロック、暗号化、検査できる暗号化トラフィックも識別します。

ジェネレータ ID（GID）137 の SSL プリプロセッサ ルールを使用してイベントを生成する場合は、これらのルールを有効にする必要があることに注意してください。詳細については、ルール状態の設定（32-23 ページ）を参照してください。

次の表に、有効にできる SSL プリプロセッサ ルールを示します。

表 27-14　SSL プリプロセッサ ルール

プリプロセッサ ルール GID:SID	説明
137:1	server hello の後の client hello（これは無効で、異常な動作とみなされる）を検出します。
137:2	[サーバ側のデータを信頼する（Server side data is trusted）] が無効な場合に、client hello のない server hello を検出します。これは無効であり、異常な動作としてみなされます。詳細については、SSL プリプロセッサの設定（27-80 ページ）を参照してください。
137:3	[最大ハートビート長（Max Heartbeat Length）] フィールドにゼロ以外の値が含まれている場合に、ペイロード自体よりも大きいペイロード長の値を含むハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。
137:4	[最大ハートビート長（Max Heartbeat Length）] フィールドで指定されているゼロ以外の値よりも大きいハートビート要求を検出します。このようなハートビート要求は、Heartbleed バグを悪用する試みを示しています。

SSL プリプロセッサの設定

ライセンス：Protection

SSL インスペクションを設定しないと、システムは、復号化せずに、マルウェアと侵入について暗号化トラフィックを検査します。SSL プリプロセッサを有効にすると、セッションが暗号化されたときにそのことを検出します。SSL プリプロセッサが有効にされると、ルール エンジンがこのプリプロセッサを呼び出し、SSL の状態およびバージョン情報を取得できるようになります。侵入ポリシーでキーワード `ssl_state` および `ssl_version` を使用してルールを有効にする場合は、そのポリシーで SSL プリプロセッサも有効にする必要があります。

また、暗号化セッションによるインスペクションと再構成を無効にするには、[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションを有効にします。SSL プリプロセッサによりセッションの状態が維持されるため、セッションのすべてのトラフィックのインスペクションを無効にできます。システムが暗号化セッションのトラフィックのインスペクションを停止するのは、SSL 前処理が有効であり、**かつ** [暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションが選択されている場合だけです。[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションをオフにした場合は、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを変更できません。

サーバ トラフィックのみに基づいて暗号化トラフィックを識別するには、[サーバ側のデータを信頼する（Server side data is trusted）] オプションを有効にできます。つまり、トラフィックが暗号化されていることを示すサーバ側のデータが信頼されます。SSL プリプロセッサは通常、クライアント トラフィックと、そのトラフィックに対するサーバの応答の両方を調べ、セッションが暗号化されているかどうかを判別します。ただし、セッションの両側を検出できない場合には、システムはトランザクションを暗号化されているものとしてマークしないため、セッションが暗号化されていることを示す SSL サーバを信頼できます。[サーバ側のデータを信頼する（Server side data is trusted）] オプションを有効にする場合は、[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] オプションも有効にして、システムが暗号化セッションのトラフィックの検査を続行しないようにする必要があることに注意してください。

プリプロセッサの [ハートビートの最大長（Max Heartbeat Length）] オプションを設定することで、SSL ハンドシェイク内のハートビート要求と応答を確認して Heartbleed バグを悪用する試みを検出できます。ペイロードが実際のペイロード長よりも大きいハートビート要求、またはハートビート応答が [ハートビートの最大長（Max Heartbeat Length）] の値よりも大きいハートビート要求を検出した場合、プリプロセッサはイベントを生成します。

プリプロセッサがトラフィックで暗号化セッションをモニタするポートを指定できます。

（注） SSL プリプロセッサは、SSL モニタの対象として指定されたポートで SSL 以外のトラフィックを検出すると、そのトラフィックを SSL トラフィックとしてデコードすることを試みた後、破損しているものとしてマークします。

SSL 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　[アプリケーション層プリプロセッサ（Application Layer Preprocessors）] の下の [SSL 設定（SSL Configuration）] を有効にしているかどうかに応じて、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。

[SSL 設定（SSL 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　SSL プリプロセッサが、暗号化されたセッションのトラフィックをモニタする必要があるポートを、カンマで区切って入力します。[ポート（Ports）] フィールドに指定されるポートでのみ、暗号化トラフィックが検査されます。

手順 6　[暗号化トラフィックのインスペクションを停止（Stop inspecting encrypted traffic）] チェック ボックスをクリックして、セッションが暗号化されているものとしてマークされた後のそのセッションでのトラフィックのインスペクションを有効または無効にします。

手順 7　[サーバ側のデータを信頼する（Server side data is trusted）] チェック ボックスをクリックして、クライアント側トラフィックのみに基づく暗号化トラフィックの識別を有効または無効にします。

手順 8　[最大ハートビート長（Max Heartbeat Length）] フィールドにバイト数を入力し、Heartbleed バグを悪用する試みに対する SSL ハンドシェイク内のハートビート要求と応答の検査を有効にします。1 ～ 65535 の整数を指定できます。このオプションを無効にする場合は 0 を入力します。

手順 9　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。