CHAPTER 26

ネットワーク分析ポリシーの準備

*ネットワーク分析ポリシー*は、多数のトラフィックの前処理オプションを制御し、アクセス コントロール ポリシーの詳細設定で呼び出されます。ネットワーク分析に関連する前処理は、セキュリティ インテリジェンスによるブラックリスト化や SSL 復号化の後、侵入またはファイル検査の開始前に実行されます。

デフォルトでは、システムは *Balanced Security and Connectivity* ネットワーク分析ポリシーを使用して、アクセス コントロール ポリシーによって処理されるすべてのトラフィックを前処理します。ただし、この前処理を実行するために別のデフォルトのネットワーク分析ポリシーを選択できます。ユーザの利便性を考え、いくつかの変更できないネットワーク分析ポリシーが用意されています。これらのポリシーは、シスコ 脆弱性調査チーム（VRT）によってセキュリティおよび接続性の一定のバランスがとれるように調整されています。カスタム前処理設定を使用して、このデフォルト ポリシーをカスタム ネットワーク分析ポリシーと置き換えることもできます。

ヒント

システム提供の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付けられていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。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）には、ネットワーク分析ポリシーと侵入ポリシーが連携してトラフィックを検査するしくみの概要、およびナビゲーション パネルの使用、競合の解決、変更のコミットに関する基本事項が記載されています。

複数のカスタム ネットワーク分析ポリシーを作成し、それらに異なるトラフィックの前処理を割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN 用に前処理オプションを調整できます。（ASA FirePOWER デバイスでは、VLAN に応じて前処理を制限することはできません）。

（注）

前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。システムはユーザに合わせてポリシーを**調整しません**。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。

この章では、単純なカスタム ネットワーク分析ポリシーを作成する方法について説明します。この章には、ネットワーク分析ポリシーの管理（編集、比較など）に関する基本情報も含まれています。詳細については、以下を参照してください。

カスタム ネットワーク分析ポリシーの作成

ライセンス：Protection

新しいネットワーク分析ポリシーを作成するときは、一意の名前を付け、基本ポリシーを指定し、*インライン モード*を選択する必要があります。

基本ポリシーはネットワーク分析ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。詳細については、基本レイヤについて（24-3 ページ）を参照してください。

ネットワーク分析ポリシーのインライン モードでは、プリプロセッサでトラフィックを変更（正規化）したりドロップしたりして、攻撃者が検出を回避する可能性を最小限にすることができます。パッシブな展開では、インライン モードに関係なく、システムはトラフィック フローに影響を与えることができないことに注意してください。詳細については、インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する（26-6 ページ）を参照してください。

ネットワーク分析ポリシーを作成するには、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。

FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。[ネットワーク分析ポリシー（Network Analysis Policy）] ページにアクセスするには、[ポリシー（Policies）] > [侵入（Intrusion）] を選択し、[ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。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。

手順 2　[ポリシーの作成（Create Policy）] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[ネットワーク分析ポリシー（Network Analysis Policy）] ページに戻るかどうか尋ねられたときに [キャンセル（Cancel）] 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。

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

手順 3　[名前(Name)] に一意のポリシー名を入力し、オプションで [説明(Description)] にポリシーの説明を入力します。

手順 4　[基本ポリシー(Base Policy)] で最初の基本ポリシーを指定します。

システム提供のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

手順 5　プリプロセッサがインライン展開でトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[インライン モード(Inline Mode)] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[インライン モード(Inline Mode)] を無効にします。

手順 6　ポリシーを作成します。

- 新しいポリシーを作成して [ネットワーク分析ポリシー(Network Analysis Policy)] ページに戻るには、[ポリシーの作成(Create Policy)] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度なネットワーク分析ポリシー エディタでそれを開いて編集するには、[ポリシーの作成と編集(Create and Edit Policy)] をクリックします(ネットワーク分析ポリシーの編集(26-4 ページ)を参照)。

ネットワーク分析ポリシーの管理

ライセンス: Protection

[ネットワーク分析ポリシー(Network Analysis Policy)] ページ([ポリシー(Policies)] > [アクセス コントロール(Access Control)] を選択し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリック)で、現在のカスタム ネットワーク分析ポリシーと共に次の情報を表示できます。

- ポリシーが最後に変更された日時(ローカル時間)とそれを変更したユーザ
- プリプロセッサがトラフィックに影響を与えることを許可する [インライン モード(Inline Mode)] 設定が有効になっているかどうか
- トラフィックを前処理するためにアクセス コントロール ポリシーおよびデバイスがどのネットワーク分析ポリシーを使用しているか
- ポリシーに保存されていない変更があるかどうか、およびポリシーを現在編集している人(いれば)に関する情報

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これら 2 つのネットワーク分析ポリシーは、ベースとして「Balanced Security and Connectivity」ネットワーク分析ポリシーを使用します。両者の唯一の相違点はインライン モードです。インライン ポリシーではプリプロセッサによるトラフィックの影響が有効化され、パッシブ ポリシーでは無効化されています。これらのシステム付属のカスタム ポリシーは編集して使用できます。

[ネットワーク分析ポリシー(Network Analysis Policy)] ページのオプションを使用することで、次の表にあるアクションを実行できます。

表 26-1　ネットワーク分析ポリシーの管理操作

目的	操作	参照先
新しいネットワーク分析ポリシーを作成する	[ポリシーの作成(Create Policy)] をクリックします。	カスタム ネットワーク分析ポリシーの作成(26-2 ページ)
既存のネットワーク分析ポリシーを編集する	編集アイコン( )をクリックします。	ネットワーク分析ポリシーの編集(26-4 ページ)
ネットワーク分析ポリシー内の現在の構成設定がリストされた PDF レポートを表示する	レポート アイコン( )をクリックします。	現在のネットワーク分析設定のレポートの生成(26-10 ページ)
2 つのネットワーク分析ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[ポリシーの比較(Compare Policies)] をクリックします。	2 つのネットワーク分析ポリシーまたはリビジョンの比較(26-11 ページ)
ネットワーク分析ポリシーを削除する	削除アイコン( )をクリックし、ポリシーを削除することを確認します。アクセス コントロール ポリシーが参照しているネットワーク分析ポリシーは削除できません。	

ただし、FireSIGHT システム のユーザ アカウントのロールが侵入ポリシーまたは修正侵入ポリシーに限定されている場合は、ネットワーク分析ポリシーに加えて、侵入ポリシーを作成して編集できます。[ネットワーク分析ポリシー(Network Analysis Policy)] ページにアクセスするには、[ポリシー(Policies)] > [侵入(Intrusion)] を選択し、[ネットワーク分析ポリシー(Network Analysis Policy)] をクリックします。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。

ネットワーク分析ポリシーの編集

ライセンス: Protection

新しいネットワーク分析ポリシーを作成すると、そのポリシーには基本ポリシーと同じ設定が付与されます。次の表に、ニーズに合わせて新しいポリシーを調整するために実行できる最も一般的な操作を示します。

表 26-2　ネットワーク分析ポリシーの編集操作

目的	操作	参照先
プリプロセッサがトラフィックを編集またはドロップすることを許可する	[ポリシー情報(Policy Information)] ページで [インライン モード(Inline Mode)] チェック ボックスをオンにします。	インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する(26-6 ページ)
基本ポリシーを変更する	[ポリシー情報(Policy Information)] ページの [基本ポリシー(Base Policy)] ドロップダウン リストから、基本ポリシーを選択します。	基本ポリシーの変更(24-4 ページ)
基本ポリシーの設定を表示する	[ポリシー情報(Policy Information)] ページで [基本ポリシーの管理(Manage Base Policy)] をクリックします。	基本レイヤについて(24-3 ページ)
プリプロセッサの設定を有効化、無効化、または編集する	ナビゲーション パネルで [設定(Settings)] をクリックします。	ネットワーク分析ポリシーでのプリプロセッサの設定(26-7 ページ)
ポリシー層を管理する	ナビゲーション パネルで [ポリシー層(Policy Layers)] をクリックします。	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)

ネットワーク分析ポリシーの調整時、特にプリプロセッサを無効化するときは、プリプロセッサおよび侵入ルールによっては、トラフィックを特定の方法で最初にデコードまたは前処理する必要があることに留意してください。必要なプリプロセッサを無効にすると、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。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

(注)　前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。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。

システムは、ユーザごとに 1 つのネットワーク分析ポリシーをキャッシュします。ネットワーク分析ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。上の表に示す実行可能な操作の他に、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)では、ナビゲーション パネルの使用、競合の解決、および変更のコミットに関する情報を記載しています。

ネットワーク分析ポリシーを編集するには、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　設定するネットワーク分析ポリシーの横にある編集アイコン（  ）をクリックします。

ネットワーク分析ポリシー エディタが表示され、[ポリシー情報（Policy Information）] ページがフォーカスされ、左側にナビゲーション パネルが配置されます。

手順 3　ポリシーを編集します。上に概要を示したいずれかのアクションを実行します。

手順 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。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。

インライン展開でプリプロセッサがトラフィックに影響を与えることを許可する

ライセンス：Protection

インライン展開では、プリプロセッサによってはトラフィックを変更およびブロックできます。次に例を示します。

- インライン正規化プリプロセッサは、パケットを正規化し、他のプリプロセッサおよび侵入ルール エンジンで分析されるようにパケットを準備します。ユーザは、プリプロセッサの [これらの TCP オプションを許可（Allow These TCP Options）] と [回復不能な TCP ヘッダーの異常をブロック（Block Unrecoverable TCP Header Anomalies）] オプションを使用して、特定のパケットをブロックすることもできます。詳細については、インライン トラフィックの正規化（29-7 ページ）を参照してください。
- システムは無効なチェックサムを持つパケットをドロップできます。チェックサムの検証（29-6 ページ）を参照してください。
- システムはレート ベースの攻撃防御設定に一致するパケットをドロップできます。レート ベース攻撃の防止（34-10 ページ）を参照してください。

ネットワーク分析ポリシーで設定したプリプロセッサがトラフィックに影響を与えるようにするには、プリプロセッサを有効化して適切に設定し、さらに管理対象デバイスを適切にインライン展開する（つまり、インライン インターフェイス セットを設定する）必要があります。最後に、ネットワーク分析ポリシーの [インライン モード（Inline Mode）] 設定を有効にする必要があります。

実際にトラフィックを変更せずに、設定がインライン展開でどのように機能するかを評価する場合は、インライン モードを無効にできます。パッシブ展開またはタップ モードでのインライン展開では、インライン モードであっても、システムはトラフィックに影響を与えることはできません。

インライン モードを無効化すると、侵入イベントのパフォーマンス統計グラフが影響を受けることがあるので注意してください。インライン展開でインライン モードが有効になっている場合、[イベント パフォーマンス（Event Performance）] ページ（[概要（Overview）] > [サマリ（Summary）] > [侵入イベントのパフォーマンス（Intrusion Event Performance）]）には、正規化されたパケットとブロックされたパケットを示すグラフが表示されます。インライン モードを無効化した場合またはパッシブ展開の場合は、正規化またはドロップされた可能性があるトラフィックに関するデータが多数のグラフに表示されます。詳細については、侵入イベントのパフォーマンス統計グラフの生成（41-5 ページ）を参照してください。

ヒント　インライン展開では、シスコはインライン モードを有効にし、[TCP ペイロードの正規化（Normalize TCP Payload）] オプションを有効にしたままインライン正規化プリプロセッサを設定することを推奨しています。パッシブ展開の場合、シスコは、適応型プロファイルを設定することを推奨しています。

プリプロセッサがインライン展開でトラフィックに影響を与えることを許可するには、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。

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

手順 3　プリプロセッサがトラフィックに影響を与えるようにするかどうかを指定します。

- プリプロセッサがトラフィックに影響を与えるようにするには、[インライン モード（Inline Mode）] を有効にします。
- プリプロセッサがトラフィックに影響を与えないようにするには、[インライン モード（Inline Mode）] を無効にします。

手順 4　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。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。

ネットワーク分析ポリシーでのプリプロセッサの設定

ライセンス：Protection

*プリプロセッサ*は、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックの詳細な検査に備えます。プリプロセッサは、設定されたプリプロセッサ オプションがパケットによりトリガーされたときに、プリプロセッサ イベントを生成できます（プリプロセッサ イベントの読み取り（41-43 ページ）を参照）。デフォルトで有効になるプリプロセッサや、それぞれのデフォルト設定は、ネットワーク分析ポリシーの基本ポリシーに応じて決まります。

ネットワーク分析ポリシーのナビゲーション パネルで [設定(Settings)] を選択すると、ポリシーによりタイプ別のプリプロセッサがリストされます。[設定(Settings)] ページで、ネットワーク分析ポリシーのプリプロセッサを有効または無効にしたり、プリプロセッサの設定ページにアクセスしたりできます。

プリプロセッサを設定するには、それを有効にする必要があります。プリプロセッサを有効にすると、そのプリプロセッサに関する設定ページへのサブリンクがナビゲーション パネル内の [設定(Settings)] リンクの下に表示され、この設定ページへの [編集(Edit)] リンクが [設定(Settings)] ページのプリプロセッサの横に表示されます。

ヒント　プリプロセッサの設定を基本ポリシーの設定に戻すには、プリプロセッサ設定ページで [デフォルトに戻す(Revert to Defaults)] をクリックします。プロンプトが表示されたら、復元することを確認します。

プリプロセッサを無効にすると、サブリンクと [編集(Edit)] リンクは表示されなくなりますが、設定は保持されます。特定の分析を実行するには、多くのプリプロセッサおよび侵入ルールで、トラフィックをまず特定の方法でデコードまたは前処理する必要があることに注意してください。必要なプリプロセッサを無効にすると、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。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

(注)　多くの場合、プリプロセッサの設定には特定の専門知識が必要で、通常は、ほとんどあるいはまったく変更を必要としません。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。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。

プリプロセッサの設定を変更するには、その設定とネットワークへの潜在的影響を理解する必要があります。次の各項には、プリプロセッサごとの固有の設定詳細情報へのリンクがあります。

アプリケーション層プリプロセッサ

アプリケーション層プロトコル デコーダは、特定のタイプのパケット データを、侵入ルール エンジンで分析できる形式に正規化します。

表 26-3　アプリケーション層プリプロセッサの設定

設定	参照先
DCE/RPC の設定	DCE/RPC トラフィックのデコード(27-2 ページ)
DNS の設定	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)
FTP および Telnet の設定	FTP および Telnet トラフィックのデコード(27-20 ページ)
HTTP の設定	HTTP トラフィックのデコード(27-34 ページ)
Sun RPC の設定	Sun RPC プリプロセッサの使用(27-50 ページ)
SIP の設定	Session Initiation Protocol のデコード(27-52 ページ)
GTP コマンド チャネルの設定	GTP コマンド チャネルの設定(27-57 ページ)
IMAP の設定	IMAP トラフィックのデコード(27-58 ページ)

表 26-3　アプリケーション層プリプロセッサの設定（続き）

設定	参照先
POP の設定	POP トラフィックのデコード（27-62 ページ）
SMTP の設定	SMTP トラフィックのデコード（27-65 ページ）
SSH の設定	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）
SSL の設定	SSL プリプロセッサの使用（27-77 ページ）

SCADA プリプロセッサ

Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、インスペクションのためにデータを侵入ルール エンジンに提供します。

表 26-4　SCADA プリプロセッサの設定

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

トランスポート層/ネットワーク層プリプロセッサ

ネットワーク層とトランスポート層のプリプロセッサは、ネットワーク層とトランスポート層でエクスプロイトを検出します。パケットがプリプロセッサに送信される前に、パケット デコーダにより、パケット ヘッダーとペイロードが、プリプロセッサや侵入ルール エンジンで簡単に使用できる形式に変換されます。また、パケット ヘッダー内でさまざまな異常動作が検出されます。

表 26-5　トランスポート層とネットワーク層のプリプロセッサの設定

設定	参照先
チェックサム検証	チェックサムの検証（29-6 ページ）
インライン正規化	インライン トラフィックの正規化（29-7 ページ）
IP 最適化	IP パケットの最適化（29-13 ページ）
パケットのデコード	パケットのデコードについて（29-18 ページ）
TCP ストリームの設定	TCP ストリームの前処理の使用（29-22 ページ）
UDP ストリームの設定	UDP ストリームの前処理の使用（29-35 ページ）

一部のトランスポートおよびネットワーク プリプロセッサの詳細設定は、アクセス コントロール ポリシーを適用するすべてのネットワークおよびゾーン、および VLAN にグローバルに適用されることに注意してください。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。トランスポート/ネットワークの詳細設定の構成（29-2 ページ）を参照してください。

特定の脅威の検出

Back Orifice プリプロセッサは、Back Orifice マジック クッキーについて UDP トラフィックを分析します。スキャン アクティビティを報告するようにポートスキャン ディテクタを設定できます。レート ベースの攻撃防御は、ネットワークを圧迫することを意図した SYN フラッドや膨大な同時接続からネットワークを保護するのに役立ちます。

表 26-6　特定の脅威の検出の設定

設定	参照先
Back Orifice の検出	Back Orifice の検出（34-2 ページ）
ポートスキャン検出	ポートスキャンの検出（34-3 ページ）
レート ベースの攻撃防御	レート ベース攻撃の防止（34-10 ページ）

侵入ポリシーで、ASCII テキストのクレジット カード番号や社会保障番号などのセンシティブ データを検出するセンシティブ データ プリプロセッサを設定することに注意してください。詳細については、センシティブ データの検出（34-20 ページ）を参照してください。

現在のネットワーク分析設定のレポートの生成

ライセンス：Protection

ネットワーク分析ポリシー レポートは、特定の時点でのポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

このレポートには、次の情報が含まれており、監査目的や現在の設定の調査目的に使用できます。

表 26-7　ネットワーク分析ポリシー レポートのセクション

セクション	説明
ポリシー情報	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。また、インライン正規化を有効にできるかどうか、現在のルール更新のバージョン、および基本ポリシーが現在のルール更新にロックされているかどうかも示されます。
設定	有効なすべてのプリプロセッサの設定とその構成を表示します。

また、2 つのネットワーク分析ポリシーや同じポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つのネットワーク分析ポリシーまたはリビジョンの比較（26-11 ページ）を参照してください。

ネットワーク分析ポリシー レポートを表示するには、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　レポートの生成対象とするポリシーの横にあるレポート アイコン( )をクリックします。ネットワーク分析ポリシー レポートを生成する前に、必ず変更をコミットしてください。コミットされた変更だけがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

2 つのネットワーク分析ポリシーまたはリビジョンの比較

ライセンス：Protection

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのネットワーク分析ポリシーの相違点を調べることができます。2 つのネットワーク分析ポリシーまたは同じネットワーク分析ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

ネットワーク分析ポリシーまたはポリシーのリビジョンを比較するために使用できる、次の 2 つのツールがあります。

- 比較ビューは、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の差異のみを横並び形式で表示します。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、2 つのネットワーク分析ポリシーまたはネットワーク分析ポリシー リビジョン間の差異のみを記録しています。これは PDF 形式であるという以外は、ネットワーク分析ポリシー レポートと類似した形式です。

  これを使用して、ポリシーの比較を保存、コピー、出力、共有して、さらに検証することができます。

ポリシー比較ツールの概要と使用法の詳細については、次の項を参照してください。

- ネットワーク分析ポリシー比較ビューの使用（26-11 ページ）
- ネットワーク分析ポリシー比較レポートの使用（26-12 ページ）

ネットワーク分析ポリシー比較ビューの使用

ライセンス：Protection

比較ビューは、両方のポリシーまたはポリシー リビジョンを横並び形式で表示します。各ポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示される名前で見分けます。ポリシー名とともに、最後に変更された時刻と、最後に変更したユーザが表示されます。

2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

次の表に、実行できる操作を記載します。

表 26-8　ネットワーク分析ポリシー比較ビューの操作

目的	操作
変更に個別にナビゲートする	タイトル バーの上にある [前へ(Previous)] または [次へ(Next)] をクリックします。 左側と右側の間にある二重矢印アイコン( )が移動し、表示している違いを示す [差異(Difference)] 番号が変わります。
特定のプリプロセッサの設定を含む階層を特定する	表示する設定の横にある詳細設定アイコン( )の上にカーソルを移動します。 ウィンドウに、プリプロセッサの設定が含まれている階層の名前が表示されます。
新しいポリシー比較ビューを生成する	[新しい比較(New Comparison)] をクリックします。 [比較の選択(Select Comparison)] ウィンドウが表示されます。詳細については、ネットワーク分析ポリシー比較レポートの使用 (26-12 ページ)を参照してください。
ポリシー比較レポートを生成する	[比較レポート(Comparison Report)] をクリックします。 ポリシー比較レポートは、2 つのポリシーまたはポリシー リビジョン間の差異のみをリストする PDF ドキュメントを作成します。

ネットワーク分析ポリシー比較レポートの使用

ライセンス: Protection

ネットワーク分析ポリシー比較レポートは、ネットワーク分析ポリシー比較ビューで特定された 2 つネットワーク分析ポリシー間または同じネットワーク分析ポリシーの 2 つのリビジョン間のすべての差異の記録を示す、PDF 形式のレポートです。このレポートを使用して、2 つのネットワーク分析ポリシーの設定の間の差異をさらに調べ、その結果を保存して配信することができます。

ネットワーク分析ポリシー比較レポートは、アクセス可能な任意のポリシーに関して、比較ビューから生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。ネットワーク分析ポリシー比較レポートは、表 26-7 (26-10 ページ)に記載されているセクションで構成されます。

ヒント　同様の手順で、SSL、アクセス コントロール、侵入、ファイル、システム、またはヘルスのポリシーを比較できます。

2 つのネットワーク分析ポリシーまたはポリシー リビジョンを比較するには、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　[ポリシーの比較（Compare Policies）] をクリックします。

[比較の選択（Select Comparison）] ウィンドウが表示されます。

手順 3　[比較対象（Compare Against）] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[他のポリシー（Other Policy）] を選択します。

  ページが更新されて、[ポリシー A（Policy A）] と [ポリシー B（Policy B）] という 2 つのドロップダウンリストが表示されます。
- 同じポリシーの 2 つのリビジョンを比較するには、[その他のリビジョン（Other Revision）] を選択します。

  ページが更新され、[ポリシー（Policy）]、[リビジョン A（Revision A）] および [リビジョン B（Revision B）] ドロップダウン リストが表示されます。

手順 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合は、[ポリシー A（Policy A）] と [ポリシー B（Policy B）] ドロップダウンリストから比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[ポリシー（Policy）] を選択し、[リビジョン A（Revision A）] および [リビジョン B（Revision B）] ドロップダウン リストから、比較するタイムスタンプ付きリビジョンを選択します。

手順 5　ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

手順 6　必要に応じて、ネットワーク分析ポリシー比較レポートを生成するには、[比較レポート（Comparison Report）] をクリックします。

ネットワーク分析ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。