オブジェクト

オブジェクトは、ポリシーまたはその他の設定で使用する基準を定義した再利用可能なコンテナです。たとえば、ネットワーク オブジェクトはホストとサブネット アドレスを定義します。

オブジェクトでは、基準を定義することができ、同じ基準を異なるポリシーで簡単に再利用できるようになります。オブジェクトを更新すると、そのオブジェクトを使用するすべてのポリシーが自動的に更新されます。

オブジェクト タイプ

次のタイプのオブジェクトを作成できます。ほとんどの場合、ポリシーまたは設定によってオブジェクトを許可する場合、オブジェクトを使用する必要があります。

オブジェクトタイプ	主な用途	説明
アプリケーション フィルタ	アクセス コントロール ルール	アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネス関連性によってアプリケーションを定義するフィルタを定義します。ポートの仕様を使うのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 アプリケーション フィルタ オブジェクトの設定，（7 ページ）を参照してください。

オブジェクトタイプ	主な用途	説明
位置情報（GeoLocation）	セキュリティ ポリシー	地理位置情報オブジェクトは、トラフィックの送信元または宛先であるデバイスをホストする国および大陸を定義します。IP アドレスを使用するのではなく、ポリシーにこれらのオブジェクトを使用してトラフィックを制御できます。 地理位置情報オブジェクトの設定, （12 ページ）を参照してください。
ネットワーク	セキュリティ ポリシーおよびさまざまなデバイス設定	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。 ネットワーク オブジェクトとグループの設定, （3 ページ）を参照してください。
ポート	セキュリティ ポリシー	トラフィックのプロトコル、ポート、または ICMP サービスを定義するポート グループおよびポート オブジェクト（総称してポート オブジェクトと呼ばれます）。 ポート オブジェクトとグループの設定, （5 ページ）を参照してください。
セキュリティ ゾーン	セキュリティ ポリシー	セキュリティ ゾーンは、インターフェイスのグループです。ゾーンによって、ネットワークがトラフィックの管理や分類に役立つセグメントに分割されます。 セキュリティ ゾーンの設定, （6 ページ）を参照してください。
Syslog サーバ	アクセス コントロール ルール、診断ロギング	syslog サーバ オブジェクトは、コネクション型または診断システム ログ（syslog）メッセージを受信できるサーバを識別します。 syslog サーバの設定, （13 ページ）を参照してください。
URL	アクセス コントロール ルール	Web リクエストの URL または IP アドレスを定義する URL オブジェクトおよびグループ（総称して URLオブジェクトと呼ばれます）。 URL オブジェクトとグループの設定, （10 ページ）を参照してください。

オブジェクトの管理

オブジェクトは、[オブジェクト（Objects）] ページから直接設定することも、ポリシーの編集時に設定することもできます。いずれの方法でも同じく新規または更新されたオブジェクトが作成されるため、その時点で適した方法を使用します。

次の手順では、[オブジェクト（Objects）] ページから直接オブジェクトを作成および管理する方法について説明します。

（注） ポリシーまたは設定を編集すると、プロパティにオブジェクトが必要な場合、すでに定義されているオブジェクトのリストが表示されるため、適切なオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合は、リストに表示される [新規オブジェクトの作成（Create New Object）]リンクをクリックします。

手順

ステップ 1 [オブジェクト（Objects）]を選択します。
[オブジェクト（Objects）] ページには、使用可能なオブジェクト タイプが一覧表示される目次があります。オブジェクト タイプを選択すると、既存オブジェクトのリストが表示され、新しいオブジェクトを作成できます。オブジェクトの内容とタイプも確認できます。

ステップ 2 目次からオブジェクト タイプを選択し、次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。オブジェクトの内容はタイプによって異なります。具体的な情報については、各オブジェクト タイプの設定トピックを参照してください。
- グループ オブジェクトを作成するには、[グループの追加（Add Group）]（）ボタンをクリックします。グループ オブジェクトには複数の項目が含まれます。
- オブジェクトを編集するには、そのオブジェクトの編集（）アイコンをクリックします。定義済みオブジェクトの内容は編集できません。
- オブジェクトを削除するには、そのオブジェクトの削除（）アイコンをクリックします。ポリシーや別のオブジェクトで現在使用されているオブジェクト、または定義済みのオブジェクトは削除できません。

ネットワーク オブジェクトとグループの設定

ホストまたはネットワークのアドレスを定義するには、ネットワーク グループとネットワーク オブジェクト（ネットワーク オブジェクトと総称される）を使用します。これらのオブジェクト

は、トラフィックの一致条件を定義するためにセキュリティ ポリシーで使用するか、サーバその他のリソースのアドレスを定義するために設定で使用することができます。

ネットワーク オブジェクトは単一のホストまたはネットワーク アドレスを定義しますが、ネットワーク グループ オブジェクトは複数のアドレスを定義できます。

次に、[オブジェクト（Objects）] ページで直接オブジェクトを作成および編集する方法について説明します。アドレス プロパティの編集時に、オブジェクト リストに表示される [新しいネットワークの作成（Create New Network）]リンクをクリックして、ネットワーク オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から [ネットワーク（Network）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）]ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力してオブジェクトの内容を定義します。

ネットワーク オブジェクト

オブジェクトの [タイプ（Type）]を、[ネットワーク（Network）] と [ホスト（Host）]のいずれかから選択します。次に、ホストまたはネットワークのアドレスを入力します。次の形式を使用できます。

- IPv4 ホスト アドレス（10.100.10.10 など）。
- サブネット マスクを含む IPv4 ネットワーク（10.100.10.0/24、10.100.10.0/255.255.255.0 など）。
- IPv6 ホスト アドレス（2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A など）。
- プレフィックスを含む IPv6 ネットワーク（2001:DB8:0:CD30::/60 など）。

ネットワーク グループ

グループに追加するネットワーク オブジェクトを選択するには、[+]ボタンをクリックします。新しいオブジェクトを作成することもできます。

ステップ 4 （新しいオブジェクトの）[追加（Add）]をクリックするか、（オブジェクトの編集時に）[保存（Save）] をクリックして変更を保存します。

ポート オブジェクトとグループの設定

トラフィックのプロトコル、ポート、または ICMP サービスを定義するには、ポート グループとポートオブジェクト（まとめてポートオブジェクトと呼ぶ）を使用します。その後、トラフィックの一致基準を定義するためのセキュリティ ポリシーのオブジェクトを使用して、たとえばアクセス ルールを使用して特定の TCP ポートへのトラフィックを許可することができます。

ポート オブジェクトは単一のプロトコル、TCP/UDP ポートまたはポート範囲、または ICMP サービスを定義しますが、ポート グループ オブジェクトは、複数のサービスを定義できます。

システムには、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは、編集または削除ができません。

（注） ポート グループ オブジェクトを作成する場合、オブジェクトの組み合わせが有効であることを確認してください。たとえば、あるオブジェクトをアクセス ルールで送信元と宛先ポートの両方を指定するために使用する場合、そのオブジェクトに複数のプロトコルを組み合わせることはできません。すでに使用されているオブジェクトを編集する場合は注意してください。オブジェクトを使用するポリシーが無効（かつディセーブル）になる場合があります。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規ポートの作成（Create New Port）]リンクをクリックすることで、サービスのプロパティを編集しながらポート オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [ポート（Ports）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）]ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらに任意で説明を入力し、オブジェクトの内容を定義します。

ポート オブジェクト

[プロトコル（Protocol）]を選択し、次のようにプロトコルを設定します。

- TCP、UDP：単一のポートまたはポート範囲の番号を入力します（たとえば80（HTTPの場合）または 1-65535（すべてのポートをカバー））。
- ICMP、IPv6 ICMP：ICMPの[タイプ（Type）]を選択し、オプションで[コード（Code）]を選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）]を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：目的のプロトコルを選択します。

ポート グループ

[+]ボタンは、グループに追加するポート オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 4 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

セキュリティ ゾーンの設定

セキュリティ ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

システムは初期設定時に次のゾーンを作成します。これらのゾーンを編集してインターフェイスを追加または削除したり、使用しなくなったゾーンを削除したりすることができます。

- inside_zone：内部インターフェイスが含まれます。このゾーンは内部ネットワークを表すことを目的としています。
- outside_zone：外部インターフェイスが含まれます。このゾーンは、インターネットなどの制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターフェイスに接続するインターフェイスを outside_zone セキュリティ ゾーンに配置し、内部ネットワークに接続するすべてのインターフェイスを inside_zone セキュリティ ゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセス コントロール ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセス ルールや他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。4つの内部ネットワークがあり、1つだけ他の3つとは異なる処理をしたい場合、1つではなく2つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用することができます。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規セキュリティ ゾーンの作成（Create New Security Zone）]リンクをクリックすることで、セキュリティ ゾーンのプロパティを編集しながらセキュリティ ゾーンを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [セキュリティ ゾーン（Security Zones）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらに任意で説明を入力します。

ステップ 4 [インターフェイス（Interfaces）]リストで、[+] をクリックし、ゾーンに追加するインターフェイスを選択します。
このリストは、現在ゾーンに含まれていないすべての名前付きインターフェイスを表示します。インターフェイスをゾーンに追加するには、インターフェイスを設定して名前を付ける必要があります。

すべての名前付きインターフェイスがすでにゾーンにある場合、リストは空になります。別のゾーンにインターフェイスを移動しようとする場合、最初に現在のゾーンから削除する必要があります。

ステップ 5 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

アプリケーション フィルタ オブジェクトの設定

アプリケーションフィルタ オブジェクトでは、IP接続で使用されるアプリケーション、あるいはタイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性ごとにアプリケーションを定義するフィルタを定義します。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーション フィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せず、ポリシーのアプリケーションとアプリケーション フィルタを直接選択することができます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーション フィルタが含まれていて、これらは編集または削除できません。

（注） シスコでは、システムおよび脆弱性データベース（VDB）の更新を通じて、アプリケーション ディテクタを頻繁に更新し、追加します。したがって、リスクの高いアプリケーションをブロックするルールは、手動でルールを更新しなくても、新しいアプリケーションに自動的に適用されます。

次の手順では、[オブジェクト（Objects）] ページから直接オブジェクトを作成および編集する方法について説明します。[アプリケーション（Applications）] タブにアプリケーション基準を追加した後、[フィルタとして保存（Save As Filter）]リンクをクリックして、アクセス コントロール ルールを編集しながら、アプリケーション フィルタ オブジェクトも作成できます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から [アプリケーション フィルタ（Application Filters）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 [アプリケーション（Applications）]リストで [追加＋（Add＋）] をクリックし、オブジェクトに追加するアプリケーションとフィルタを選択します。
最初のリストには、継続的にスクロールするリストでアプリケーションが表示されます。[フィルタの詳細設定（[フィルタの詳細設定]）]をクリックすると、フィルタ オプションが表示され、アプリケーションを容易に選択できます。選択したら、[追加（Add）]をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注） 1 つのフィルタ条件内での複数の選択は OR 関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりすることができます。

リスク

アプリケーションが組織のセキュリティ ポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーション プロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアント プロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- [Web アプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは [SSL プロトコル（SSL Protocol）]とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）]タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

ステップ 5 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトの編集の場合）をクリックして変更を保存します。

URL オブジェクトとグループの設定

URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス コントロール ポリシーで手動フィルタリングを実装することができます。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。

URL オブジェクトを作成する場合、次の点に注意してください。

- ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の一部に一致すると、URL が一致したと見なされます。したがって、example.com は、www.example.com や ads.example.com など、そのネットワーク上の任意のホストに一致します。また、badexample.com と一致します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィックがブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com/ ではなく、example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

（注） 特定のサイトをターゲットとする URL オブジェクトを設定する前に、アクセス コントロールの章に記載されている URL のフィルタリングに関する情報をよく確認してください。URL のマッチングは想定されるようには行われないため、意図せずにサイトをブロックしてしまう可能性があります。たとえば、ゲーム サイト ign.com を明示的にブロックしようとすると、verisign.com、およびその他の「ign」で終わる任意のサイトもブロックしてしまいます。

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [新規 URL の作成（Create New URL）]リンクをクリックすることで、URL のプロパティを編集しながら URL オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [URL] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）]ボタン（  ）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらに任意で説明を入力します。

ステップ 4 オブジェクトの内容を定義します。

URL オブジェクト

URL または IP アドレスを [URL]ボックスに入力します。URL にはワイルドカードを使用できません。

URL グループ

[+]ボタンは、グループに追加する URL オブジェクトを選択するためにクリックします。新しいオブジェクトを作成することもできます。

ステップ 5 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。

地理位置情報オブジェクトの設定

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。たとえば、地理的な場所を使用して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

（注） 常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

次に、[オブジェクト（Objects）] ページで直接オブジェクトを作成および編集する方法について説明します。ネットワーク プロパティの編集時に、オブジェクト リストに表示される [新しい地理位置情報の作成（Create New Geolocation）]リンクをクリックして、地理位置情報オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、目次から [地理位置情報（Geolocation）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 [大陸または国（Continents/Countries）]リストで[+ を追加（Add+）] をクリックして、オブジェクトに追加する大陸や国を選択します。
大陸を選択すると、大陸内のすべての国が選択されます。

ステップ 5 （新しいオブジェクトの）[追加（Add）]をクリックするか、（オブジェクトの編集時に） [保存（Save）] をクリックして変更を保存します。

syslog サーバの設定

syslog サーバのオブジェクトはコネクション型メッセージまたは診断システム ログ（syslog）メッセージを受信できるサーバを指定します。ログのコレクションと分析用に設定された syslog サーバがある場合、それらを定義するオブジェクトを作成し、そのオブジェクトをアクセス ルールまたは診断ロギング システム設定で使用します。システム ロギングの設定の詳細については、次のトピックを参照してください。

- ロギングの設定
- 診断ロギングの設定

次に、オブジェクト ページからオブジェクトを直接作成および編集する方法について説明します。オブジェクト リストに表示される [syslog サーバの追加（Add Syslog Server）] リンクをクリックすることで、syslog サーバのプロパティを編集しながら syslog サーバを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）]を選択し、次に目次から [Syslog サーバ（Syslog Server）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+]ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 syslog サーバのプロパティを設定します。

- [デバイス インターフェイス（Device Interface）]：syslog サーバにアクセスするインターフェイスを選択します。
- [IP アドレス（IP Address）]：syslog サーバの IP アドレスを入力します。
- [ポート（Port）]：サーバが syslog メッセージを受信するために使用する UDP ポートを入力します。デフォルトは 514 です。

ステップ 4 [追加（Add）]（新規オブジェクトの場合）または [保存（Save）]（オブジェクトを編集する場合）をクリックして変更を保存します。