SNMP

この章では、Simple Network Management Protocol（SNMP）に ASA をモニターさせるための設定方法について説明します。

SNMP について

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。ASAは SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワーク デバイスをモニターできます。ASAは GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIB は定義の集合であり、ASAは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

（注） 集中的なワークロードでは、10 を超える NMS を展開すると、デバイスのパフォーマンスに影響を与える可能性があります。デバイスの安定性と応答性を確保するために、SNMP ウォークポーリングの実行とトラップトラフィックの管理には NMS を慎重に利用することを推奨します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *1 : SNMP* の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバー。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニターすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIB は、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMPイベントのモニターやASAなどのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニターおよび表示される情報の源をユーザーに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバーと SNMP エージェント間でデータをクリアテキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザーベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA は、SNMP グループとユーザーの作成、およびセキュアな SNMP 通信の転送の認証と暗号化を有効にするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザーとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザーは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザー

SNMP ユーザーは、指定されたユーザー名、ユーザーが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは SHA-1、SHA-224、SHA-256 HMAC および SHA-384 です。暗号化アルゴリズムのオプションは、3DES および AES（128、192、および 256 バージョンで使用可能）です。ユーザーを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザーはグループのセキュリティ モデルを継承します。

（注） SNMP v3 ユーザーアカウントを設定するときは、認証アルゴリズムの長さが暗号化アルゴリズムの長さ以上であることを確認してください。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザー名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA で一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザー クレデンシャルが ASA のクレデンシャルと一致するように設定してください。

（注） 最大 8,192 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。

ASA と Cisco IOS ソフトウェアの実装の相違点

ASA での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカルエンジン ID は、ASA が起動されたとき、またはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザーとグループを作成する必要があります。
- 正しい順序でユーザー、グループ、およびホストを削除する必要があります。
- snmp-server host コマンドを使用すると、着信 SNMP トラフィックを許可する ASA ルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、syslog メッセージガイドを参照してください。

（注） SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMP を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーとクラスタリングのガイドライン

- クラスタリングまたはフェールオーバーで SNMPv3 を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットに複製されません。ユーザを新しいユニットに強制的に複製するには、SNMPv3 ユーザを制御またはアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます（SNMPv3 ユーザおよびグループは、クラスタデータユニットで設定コマンドを入力できないというルールの例外です）。制御ユニットまたはアクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してデータユニットまたはスタンバイユニットに直接入力することにより、各ユーザを再設定します。

IPv6 ガイドライン（すべての ASA モデル）

SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリを実行でき、IPv6 ソフトウェアを実行するデバイスから SNMP 通知を受信できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

その他のガイドライン

- アプライアンスモードで動作しているシステムでは、電源トラップは発行されません。
- アプライアンス モードの Firepower 2100 では、ハードウェアモデルとシリアルをポーリングできません。ASA では、これらの詳細についてトラップは生成されません。そのため、ASA インスタンスのインターフェイスではなくシャーシ管理 IP をポーリングするように FXOS またはシャーシ マネージャの SNMP を設定します。
- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。

- VPN トンネル経由の管理アクセスは、SNMP（**management-access** コマンド）ではサポートされません。VPN 経由の SNMP の場合、ループバック インターフェイスで SNMP を有効にすることをお勧めします。ループバック インターフェイスで SNMP を使用するために、管理アクセス機能を有効にする必要はありません。ループバックは SSH でも機能します。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- 一部のデバイスでは、**snmpwalk** の出力に表示されるインターフェイスの順序（ifDescr）が再起動後に変わることが確認されています。ASA では、アルゴリズムを使用して SNMP が照会する ifIndex テーブルを決定します。ASA の起動時、ASA による設定の読み取りでロードされる順序でインターフェイスが ifIndex テーブルに追加されます。ASA に新しいインターフェイスが追加されると、ifIndex テーブルのインターフェイスのリストに追加されていきます。インターフェイスの追加、削除、または名前変更により、再起動時にインターフェイスの順序が変わることがあります。
- **snmpwalk** コマンドで OID を指定すると、snmpwalk ツールは、指定された OID の下にあるサブツリー内のすべての変数をクエリし、その値を表示します。そのため、デバイス上のオブジェクトの包括的な出力を表示するには、**snmpwalk** コマンドで OID を指定してください。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。
- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザー、ホストの順に行う必要があります。
- SecureFirewall モデルの場合、**snmpwalk** コマンドは、管理のコンテキストからのみ FXOS MIB をポーリングします。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザーが削除されていることを確認する必要があります。

- ユーザーを削除する前に、そのユーザー名に関連付けられているホストが設定されていないことを確認する必要があります。
- 特定のセキュリティ モデルを使用して特定のグループに属するようにユーザーが設定されている場合にそのグループのセキュリティ レベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザーを追加します。
- MIB オブジェクトのサブセットへのユーザー アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザー コンテキストで設定された SNMP サーバー ホストが少なくとも 1 つ必要です。
- NMS が正常にオブジェクトを要求できない場合、または ASA からの着信トラップを適切に処理していない場合は、パケット キャプチャの実行が問題を判別する最も有効な方法となります。[Wizards] > [Packet Capture Wizard] を選択して、画面に表示される指示に従います。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホスト グループに指定した値が適用されます。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- ASA では、コンテキストごとに SNMP サーバーのトラップ ホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

SNMP の構成

ここでは、SNMP の設定方法について説明します。

手順

ステップ 1 ASA から要求を受信するように SNMP 管理ステーションを設定します。

ステップ 2 SNMP トラップを設定します。

ステップ 3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP 管理ステーションの設定

SNMP 管理ステーションを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。デフォルトでは、SNMP サーバーはイネーブルになっています。

ステップ 2 [SNMP Management Stations] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ホストが存在するインターフェイスを選択します。

ステップ 4 SNMP ホストの IP アドレスを入力します。

ステップ 5 SNMP ホストの UDP ポートを入力します。デフォルトのポート 162 をそのまま使用することもできます。

ステップ 6 SNMP ホストのコミュニティ ストリングを追加します。管理ステーションに対してコミュニティ ストリングが指定されていない場合は、[SNMP Management Stations] ペインの [Community String (default)] フィールドに設定されている値が使用されます。

ステップ 7 SNMP ホストで使用される SNMP のバージョンを選択します。

ステップ 8 前の手順で SNMP バージョン 3 を選択した場合は、設定済みユーザーの名前を選択します。

ステップ 9 [Poll] チェックボックスまたは [Trap] チェックボックスのいずれかをオンにして、NMS との通信に使用する方式を指定します。

ステップ 10 [OK] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

NMS が設定され、その変更内容が実行コンフィギュレーションに保存されます。SNMP バージョン 3 の NMS ツールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

SNMP トラップの設定

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

（注） すべての SNMP トラップまたは syslog トラップを有効にすると、SNMP プロセスがエージェントとネットワーク内で過剰にリソースを消費し、システムがハングアップする可能性があります。システムの遅延、未完了の要求、またはタイムアウトが発生した場合は、SNMP トラップと syslog トラップを選択して有効にすることができます。たとえば、情報 syslog トラップのシビラティ（重大度）レベルをスキップできます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [Configure Traps] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが表示されます。

ステップ 3 [SNMPサーバトラップ構成（SNMP Server Traps Configuration）] チェックボックスをオンにします。

デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。トラップ タイプを指定しない場合、デフォルトで **syslog** トラップに設定されます。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。デフォルトでは他のトラップはすべてディセーブルです。トラップをディセーブルにするには、該当するチェックボックスをオフにします。

トラップは、次のカテゴリに分類されます。

a) [標準SNMPトラップ（Standard SNMP Traps）]、該当するものをすべてチェックします。

[クリティカルCPU温度（Critical CPU temperature）]、[シャーシ温度（Chassis temperature）]、および [シャーシファンの障害（Chassis Fan Failure）] から選択します。

（注）
デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。

b) [環境トラップ（Environment Traps）]、該当するものをすべてチェックします。

[認証（Authentication）]、[リンクアップ（Link up）]、[リンクダウン（Link down）]、[コールドスタート（Cold start）]、および [ウォームスタート（Warm start）] から選択します。

c) [Ikev2トラップ（Ikev2 Traps）]、該当するものをすべてチェックします。

[開始（Start）] および [停止（Stop）] から選択します。

d) [エンティティMIB通知（Entity MIB Notifications）]。

現場交換可能ユニットに関する通知を受信するには、この項目をオンにします。

e) [IPSecトラップ（IPSec Traps）]、該当するものをすべてチェックします。

[開始（Start）] および [停止（Stop）] から選択します。

f) [リモートアクセストラップ（Remote Access Traps）]。

確立されたセッション数が設定されたしきい値を超えたときに通知を受信するには、この項目をオンにします。

g) [リソーストラップ（Resource Traps）]、該当するものをすべてチェックします。

[接続制限に達しました（Connection limit reached）]、[メモリのしきい値に達しました（Memory threshold reached）]、および [インターフェイスのしきい値に達しました（Interface threshold reached）] から選択します。

h) [NATトラップ（NAT Traps）]。

マッピングスペースが使用できないために IP パケットが NAT によって破棄されたときに通知を受信するには、この項目をオンにします。

i) [Syslog]。

確立されたセッション数が設定されたしきい値を超えたときに通知を受信するには、[syslogトラップを有効にする（Enable syslog traps）] をオンにします。

syslog トラップの重大度レベルを設定するには、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ロギング（Logging）] > [ロギングフィルタ（Logging Filters）]** の順に選択します

j) [CPU使用率トラップ（CPU Utilization Traps）]。

CPU 使用率が、設定された [モニタリング間隔（Monitoring interval）] に対して設定された [CPU使用率しきい値（CPU Utilization threshold）] を超えた場合に通知を受信するには、[CPU上昇しきい値に達しました（CPU rising threshold reached）] をオンにします。

k) [SNMPインターフェイスしきい値（SNMP interface threshold）]。

インターフェイスの帯域幅使用率が、設定された [SNMPインターフェイスしきい値（SNMP interface threshold）] を超えた場合に通知を受信するには、[しきい値と間隔の設定（Configure threshold and interval）] をオンにします。

有効なしきい値の範囲は 30～99 % です。デフォルト値は 70 % です。

l) [SNMPメモリしきい値（SNMP Memory threshold）]。

CPU 使用率が、[SNMPメモリしきい値（SNMP memory threshold）] に設定されたしきい値を超えた場合に通知を受信するには、[メモリしきい値の設定（Configure memory threshold）] をオンにします。

使用されたシステムコンテキストのメモリが総システムメモリの80%に達すると、メモリしきい値トラップが管理コンテキストから生成されます。他のすべてのユーザーコンテキストでは、このトラップは使用メモリが特定のコンテキストの総システム メモリの 80 % に到達した場合に生成されます。

m) [フェールオーバートラップ（Failover Traps）]。

フェールオーバーの SNMP syslog トラップを受信するには、[フェールオーバー関連のトラップを有効にする（Enable Failover related traps）] をオンにします。

n) [クラスタトラップ（Cluster Traps）]。

クラスタメンバーの SNMP syslog トラップを受信するには、[クラスタ関連のトラップを有効にする（Enable cluster related traps）] をオンにします。

o) [ピアフラップトラップ（Peer-Flap Traps）]。

クラスタピア MAC アドレスフラッピングの SNMP syslog トラップを受信するには、[bgp/ospfピアフラップ関連のトラップを有効にする（Enable bgp/ospf peer-flap related traps）] をオンにします。

ステップ 4 [OK] をクリックして、[SNMP Trap Configuration] ダイアログボックスを閉じます。

ステップ 5 [Apply] をクリックします。

SNMP トラップが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 SNMP バージョン 1 または 2c を使用する場合は、[Community String (default)] フィールドにデフォルトのコミュニティ ストリングを入力します。要求を ASA に送信するときに SNMP NMS で使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP NMS と管理対象のネットワーク ノード間の共有秘密です。ASA では、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。ただし、SNMP モニタリングが診断インターフェイスではなく管理インターフェイスを介している場合、ASA がコミュニティ文字列を検証せずにポーリングが実行されます。パスワードは、大文字と小文字が区別される、最大 32 文字の英数字です。スペースは使用できません。デフォルトは public です。SNMP バージョン 2c

では、NMS ごとに、別々のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの NMS にも設定されていない場合、ここで設定した値がデフォルトとして使用されます。

（注）
コミュニティストリングでは特殊文字（!、@、#、$、%、^、&、*、\）を使用しないでください。一般に、オペレーティングシステムで使用される関数用に予約されている特殊文字を使用すると、予期しない結果が生じる可能性があります。たとえば、バックスラッシュ（\）はエスケープ文字と解釈されるため、コミュニティストリングでは使用できません。

ステップ 3 ASA システム管理者の名前を入力します。テキストは、大文字と小文字が区別される、最大 127 文字の英数字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4 SNMP で管理している ASA の場所を入力します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5 NMS からの SNMP 要求をリッスンする ASA ポートの番号を入力します。デフォルトのポート番号 161 をそのまま使用することもできます。

ステップ 6 （オプション）[Enable Global-Shared pool in the walk] チェックボックスをオンにして、SNMP ウォーク操作によって空きメモリと使用済みメモリの統計情報を照会します。

重要
ASA がメモリ情報を照会すると、CPU は他のプロセスに開放される前に SNMP プロセスによって長時間にわたり保持されることがあります。これにより、SNMP 関連の CPU ホグ状態になり、パケットがドロップされることがあります。

ステップ 7 [SNMP Host Access List] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 8 トラップの送信元となるインターフェイスの名前をドロップダウン リストから選択します。

ステップ 9 ASA に接続できる NMS または SNMP マネージャの IP アドレスを入力します。

ステップ 10 UDP のポート番号を入力します。デフォルトは 162 です。

ステップ 11 使用する SNMP のバージョンをドロップダウン リストから選択します。バージョン 1 または 2c を選択した場合は、コミュニティ ストリングを入力する必要があります。バージョン 3 を選択した場合は、ドロップダウン リストからユーザー名を選択する必要があります。

バージョンは、トラップと要求（ポーリング）に使用される SNMP のバージョンを指定します。サーバとの通信は、選択したバージョンのみを使用して許可されます。

ステップ 12 要求の送信（ポーリング）だけに NMS を制限する場合は、[Server Poll/Trap Specification] 領域の [Poll] チェックボックスをオンにします。トラップの受信だけに NMS を制限する場合は、[Trap] チェックボックスをオンにします。両方のチェックボックスをオンにすると、SNMP ホストの両方の機能が実行されます。

ステップ 13 [OK] をクリックして、[Add SNMP Host Access Entry] ダイアログボックスを閉じます。

新しいホストが [SNMP Host Access List] ペインに表示されます。

ステップ 14 **Apply** をクリックします。

SNMP バージョン 1、2c、または 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User]** の順にクリックして、設定済みのユーザーまたは新規ユーザーをグループに追加します。グループ内に残る最後のユーザーを削除すると、そのグループは ASDM により削除されます。

（注）
ユーザーが作成された後は、そのユーザーが属するグループは変更できません。

[Add SNMP User Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ユーザーが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザーには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザーには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザーには、認証も暗号化も設定されません。

（注）
グループ名は変更できません。

ステップ 4 ユーザー セキュリティ モデル（USM）グループを使用する場合は、[USM Model]]タブをクリックします。

ステップ 5 [Add] をクリックします。

[Add SNMP USM Entry] ダイアログボックスが表示されます。

ステップ 6 グループ名を入力します。

ステップ 7 ドロップダウン リストからセキュリティ レベルを選択します。設定済みの USM グループをセキュリティ レベルとして SNMPv3 ユーザーに割り当てることができます。

ステップ 8 設定済みユーザーまたは新規ユーザーの名前を入力します。ユーザー名は、選択した SNMP サーバー グループ内で一意であることが必要です。

ステップ 9 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 10 [SHA]、[SHA224]、[SHA256]、または [SHA384] のいずれかのオプションボタンをクリックして、使用する認証のタイプを指定します。,

ステップ 11 認証に使用するパスワードを入力します。

ステップ 12 [3DES]、または [AES] の中からいずれかのオプションボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 AES 暗号化を選択した場合は、使用する AES 暗号化のレベルとして、128、192、256 のいずれかを選択します。

ステップ 14 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 15 [OK] をクリックすると、グループが作成され（指定したユーザーがそのグループに属する最初のユーザーである場合）、[Group Name] ドロップダウン リストにそのグループが表示されます。またそのグループ内にユーザーが作成されます。

[Add SNMP User Entry] ダイアログボックスが閉じます。

ステップ 16 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

ユーザーのグループの設定

指定したユーザーのグループからなる SNMP ユーザー リストを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User Group]** の順にクリックし、設定済みのユーザー グループまたは新規ユーザー グループを追加します。グループ内に残る最後のユーザーを削除すると、そのグループは ASDM により削除されます。

[Add SNMP User Group] ダイアログボックスが表示されます。

ステップ 3 ユーザー グループ名を入力します。

ステップ 4 既存のユーザーまたはユーザー グループを選択する場合は、[Existing User/User Group] オプション ボタンをクリックします。

ステップ 5 新規ユーザーを作成する場合は、[Create new user] オプション ボタンをクリックします。

ステップ 6 SNMP ユーザーが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザーには、認証と暗号化が設定されます。

- [Authentication_Only]：このグループに属するユーザーには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザーには、認証も暗号化も設定されません。

ステップ 7 設定済みユーザーまたは新規ユーザーの名前を入力します。ユーザー名は、選択した SNMP サーバー グループ内で一意であることが必要です。

ステップ 8 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 9 [SHA]、[SHA224]、[SHA256]、または [SHA384] のいずれかのオプションボタンをクリックして、使用する認証のタイプを指定します。

ステップ 10 認証に使用するパスワードを入力します。

ステップ 11 認証に使用するパスワードを確認のためにもう一度入力します。

ステップ 12 [3DES]、または [AES] の中からいずれかのオプションボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 14 暗号化に使用するパスワードを確認のためにもう一度入力します。

ステップ 15 [Members in Group] ペインの指定したユーザー グループに新規ユーザーを追加するには、[Add] をクリックします。[Members in Group] ペインから既存のユーザーを削除するには、[Remove] をクリックします。

ステップ 16 [OK] をクリックすると、指定したユーザー グループに新規ユーザーが作成されます。

[Add SNMP User Group] ダイアログボックスが閉じます。

ステップ 17 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP モニタリング

次の SNMP モニタリング用のコマンドを参照してください。**[Tools] > [Command Line Interface]** を使用して次のコマンドを入力できます。

- **show running-config snmp-server** [**default**]

  すべての SNMP サーバーのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

  リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

  SNMP ユーザーベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザー リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは2つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMPサーバーの設定済み特性を表示します。すべてのSNMPカウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザーの設定済み特性を表示します。

SNMP の履歴

表 *2 : SNMP* の履歴

機能名	バージョン	説明
SNMP バージョン 1 および 2c	7.0(1)	クリアテキストのコミュニティストリングを使用したSNMPサーバーと SNMP エージェント間のデータ送信によって、ASA ネットワークのモニタリングおよびイベント情報を提供します。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。

機能名	バージョン	説明
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザー、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
IF-MIB ifAlias OID のサポート	8.2(5) / 8.4(2)	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。

機能名	バージョン	説明
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。

機能名	バージョン	説明
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザー リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB および OID	9.2(1)	ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASA 仮想 が追加されました。 新しいプラットフォームである ASA 仮想 をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 VPN 共有ライセンスの使用状況をモニターするための新しい SNMP MIB が追加されました。
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。

機能名	バージョン	説明
SNMP の MIB およびトラップ	9.3(2)	ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP] > [Configure Traps] > [SNMP Trap Configuration]。
SNMP の MIB およびトラップ	9.4(1)	SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。
コンテキストごとに無制限の SNMP サーバー トラップ ホスト	9.4(1)	ASA は、コンテキストごとに無制限の SNMP サーバー トラップ ホストをサポートします。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 変更された ASDM 画面はありません。
ISA 3000 のサポートが追加されました。	9.4(1.225)	ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。**snmp-server enable traps entity** コマンドが変更され、新しい変数 *l1-bypass-status* が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。 変更された ASDM 画面はありません。

機能名	バージョン	説明
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。
Precision Time Protocol（PTP）の E2E トランスペアレント クロック モード MIB のサポート	9.7(1)	E2E トランスペアレント クロック モードに対応する MIB がサポートされます。 （注） SNMP の bulkget、getnext、walk 機能のみがサポートされています。
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバーとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.10(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 変更された ASDM 画面はありません。

機能名	バージョン	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.12(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**
SNMPv3 認証	9.14(1)	ユーザー認証に SHA-256 HMAC を使用できるようになりました。 新規/変更された画面：**[構成（Configuration）]**>**[デバイス管理（Device Management）]** > **[管理アクセス（Management Access）]** > **[SNMP]**
9.14(1) 以降のフェールオーバーペアの場合、ASA は SNMP クライアントエンジンデータをピアと共有しません。	9.14(1)	ASA は、SNMP クライアントのエンジンデータをピアと共有しなくなりました。
サイト間 VPN 経由の SNMP ポーリング	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。
CISCO-MEMORY-POOL-MIB OID のサポートの廃止	9.15(1)	64 ビットカウンタを使用するシステムの CISCO-MEMORY-POOL-MIB OID（ciscoMemoryPoolUsed、ciscoMemoryPoolFree）が廃止されました。 64 ビットカウンタを使用するシステムのメモリ プール モニタリング エントリは、CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable で提供されます。
SNMPv3 認証	9.16(1)	ユーザー認証に SHA-224 および SHA-384 を使用できるようになりました。ユーザー認証に MD5 を使用できなくなりました。 暗号化に DES を使用できなくなりました。 新規/変更された画面：**[構成（Configuration）]**>**[デバイス管理（Device Management）]** > **[管理アクセス（Management Access）]** > **[SNMP]**
SNMP のループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、SNMP に使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**snmp-server host** 新規/変更された画面：[設定（Configuration）] > [デバイスのセットアップ（Device Setup）]>[インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [ループバックインターフェイスの追加（Add Loopback Interface）] ASDM サポートは 7.19 で追加されました。

機能名	バージョン	説明
SNMP の MIB およびトラップ	9.20(1)	Cisco Secure Firewall 4200 モデルデバイス（FPR4215、FPR4225、FPR4245）が、SNMP の sysObjectID OID および entPhysicalVendorType OID の表に、新しい製品として追加されました。これらの Cisco Secure Firewall 4200 シリーズデバイスの 2 つの EPM カード（4X200G および 2X100G）の SNMP サポートが追加されました。

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