SNMP の設定

この章では、ASA および ASASM をモニタするように SNMP を設定する方法について説明します。次の項目を取り上げます。

SNMP の概要

SNMP は、ネットワーク デバイス間の管理情報の交換を容易にするアプリケーションレイヤ プロトコルで、TCP/IP プロトコル スイートの一部です。ここでは SNMP について、次の内容を説明します。

ASA および ASASM は SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリング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 ASA および ASASM をモニタできます。ASA および ASASM は GET 要求の発行を通じた 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 への特定のイベントの管理ステーションに対する管理対象デバイスからの要求外のメッセージ（イベント通知）であるトラップを送信するように ASA および ASASM を設定したり、NMS を使用して ASA の MIB をブラウズしたりできます。MIB は定義の集合で、ASA および ASASM は各定義の値のデータベースを保持します。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。

ASA および ASASM には SNMP エージェントが含まれています。SNMP 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。SNMP 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 Object Identifier（OID; オブジェクト ID）が含まれています。ASA または ASASM SNMP 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 の用語に関する情報

表 43-1 に、SNMP で頻繁に使用される用語を示します。

表 43-1　SNMP の用語

用語	説明
エージェント	ASA で稼働する SNMP サーバ。SNMP エージェントには次の機能があります。 • 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、ほとんどのネットワーク 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規格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 イベントのモニタや ASA および ASASM 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、モニタおよび表示される情報の源をユーザに示すシステム。
トラップ	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条件が含まれます。

SNMP バージョン 3

この項では、SNMP バージョン 3 について説明します。説明する項目は次のとおりです。

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 SNMP 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 および ASASM は、SNMP グループとユーザの作成、およびセキュアな SNMP 通信の転送の認証と暗号化をイネーブル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

SNMP ユーザは、指定されたユーザ名、ユーザが属するグループ、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 MD5 と SHA です。暗号化アルゴリズムのオプションは DES、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、そのユーザはグループのセキュリティ モデルを継承します。

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 および ASA サービス モジュール で固有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、ASA および ASASM のユーザ クレデンシャルと NMS のユーザ クレデンシャルが確実に一致するように設定してください。

ASA、ASA サービス モジュール、Cisco IOS ソフトウェア間の実装の違い

ASA および ASASM 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 の実装とは次のように異なります。

- 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 または ASASM が起動されたとき、あるい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、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 または ASASM ルールが作成されます。

SNMP のライセンス要件

次の表に、この機能のライセンス要件を示します。

ライセンス要件
基本ライセンス：基本（DES）。
オプション ライセンス：強化（3DES、AES）

SNMP の前提条件

SNMP には次の前提条件があります。

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。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

- SNMP バージョン 3 でサポートされています。
- 各 ASA または ASASM の SNMP クライアントはそれぞれのピアとエンジン データを共有します。エンジン データには、SNMP-FRAMEWORK-MIB の engineID、engineBoots、および engineTime オブジェクトが含まれます。エンジン データはバイナリ ファイルとして flash:/snmp/*contextname* に書き込まれます。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- 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。
- 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。
- 既存の設定を変更すると、その結果により SNMP 機能が矛盾した状態になる場合、拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザ、ホストの順に行う必要があります。
- 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。
- ユーザを削除する前に、そのユーザ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を追加します。
- MIB オブジェクトのサブセットへのユーザ 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。
- 接続制限に達したトラップは、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、少なくとも 1 つの、接続制限に達したユーザ コンテキストで設定された snmp-server host がある必要があります。

- ASA 5585 SSP-40（NPE）のシャーシ温度を問い合わせることはできません。
- 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。

SNMP の設定

この項では、SNMP を設定する方法について説明します。次の項目を取り上げます。

SNMP のイネーブル化

ASA で動作する SNMP エージェントは、次の 2 つの機能を実行します。

- NMS からの SNMP 要求に応答する。
- トラップ（イベント通知）を NMS に送信する。

SNMP エージェントをイネーブルにし、SNMP サーバに接続できる NMS を識別するには、次のペインを確認します。

パス	目的
[Configuration] > [Device Management] > [Management Access] > [SNMP]	ASA または ASASM 上の SNMP サーバがイネーブルになっていることを確認します。デフォルトでは、SNMP サーバはイネーブルになっています。

次の作業

「SNMP 管理ステーションの設定」（P.43-6）を参照してください。

SNMP 管理ステーションの設定

ASA から要求を受信するには、ASDM で SNMP 管理ステーションを設定する必要があります。

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。

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 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　[Interface Name] ドロップダウン リストから、SNMP ホストが常駐するインターフェイスを選択します。

ステップ 4　[IP Address] フィールドに、SNMP ホストの IP アドレスを入力します。

ステップ 5　[UDP Port] フィールドに 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　[Community String] フィールドに、SNMP ホストのコミュニティ ストリングを入力します。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 Version] ドロップダウン リストから、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 Version 3] を選択した場合は、[Username] ドロップダウン リストから、設定済みユーザ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

次の作業

「SNMP トラップの設定」（P.43-7）を参照してください。

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。

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　トラップは、[standard]、[IKEv2]、[entity MIB]、[IPsec]、[remote access]、[resource]、[NAT]、[syslog]、[CPU utilization]、[CPU utilization and monitoring interval]、および [SNMP interface threshold] のカテゴリに分類されます。SNMP トラップを介して通知を発行するための SNMP イベントを指定するため、目的の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、デフォルトでは syslog トラップになります。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。その他すべてのトラップは、デフォルトでディセーブルです。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。syslog トラップの重大度レベルを設定するには、[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 4　[OK] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが閉じます。

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。

次の作業

次のいずれかを選択します。

- 「SNMP バージョン 1 または 2c の使用」（P.43-8）を参照してください。
- 「SNMP バージョン 3 の使用」（P.43-9）を参照してください。

SNMP バージョン 1 または 2c の使用

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。

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

ステップ 2　（任意）[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、パスワードを基にして、受信する SNMP 要求が有効かどうかの判断が行われます。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。

ステップ 3　[Contact] フィールドに、ASA の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　[ASA Location] フィールドに、SNMP で管理されている 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　[Listening Port] フィールドに、NMS からの SNMP 要求をリッスンする ASA のポートの番号を入力します。ただし、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　[Apply] をクリックします。

SNMP バージョン 1 および 2c 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。

次の作業

「SNMP のモニタリング」（P.43-10）を参照してください。

SNMP バージョン 3 の使用

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。

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

ステップ 2　設定済みのユーザまたは新規ユーザをグループに追加する場合は、[SNMPv3 Users] ペインで [Add] をクリックします。ユーザ パラメータを変更する場合は、[Edit] をクリックします。設定済みユーザをグループから削除する場合は、[Delete] をクリックします。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。

（注）　ユーザが作成された後は、そのユーザ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　[Group Name] ドロップダウン リストから、SNMP ユーザを追加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には、認証も暗号化も設定されません。

ステップ 4　[Username] フィールドに、設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバ グループ内で一意であることが必要です。

ステップ 5　[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 6　[MD5] と [SHA] 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 7　認証に使用するパスワードを、[Authentication Password] フィールドに入力します。

ステップ 8　[DES]、[3DES]、[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 9　AES 暗号化を選択した場合は、[AES Size] ドロップダウン リストから、使用する AES 暗号化のレベル（[128]、[192]、または [256]）を選択します。

ステップ 10　暗号化に使用するパスワードを、[Encryption Password] フィールドに入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 11　[OK] をクリックすると、グループが作成され（指定したユーザがそのグループに属する最初のユーザである場合）、[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。

[SNMPv3 Users] ペインには、SNMP バージョン 3 のサーバ グループ名、指定したグループに属するユーザの名前、暗号化されたパスワードの設定内容、認証の設定内容、暗号化アルゴリズムの設定内容、および AES サイズの設定内容が一覧表示されます。

ステップ 12　[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。

次の作業

「SNMP のモニタリング」（P.43-10）を参照してください。

SNMP のモニタリング

NMS は、SNMP イベントのモニタおよびASA などのデバイスの管理用に設定した、PC またはワークステーションです。デバイスで設定された 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、NMS からデバイスのヘルスをモニタできます。SNMP エージェントから NMS への事前定義済みのイベントによって、syslog メッセージが生成されます。この項は、次の内容で構成されています。

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、SNMP 要求のステータス、SNMP トラップ、SNMP チャネル、ASA または ASASM から指定インターフェイスの指定ホストに対する SNMP 応答を表示します。

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 メッセージが高速（約 4000/秒）を超える場合、SNMP ポーリングは失敗します。

SNMP モニタリング

SNMP をモニタするには、次の手順を実行します。

パス	目的
[Tools] > [Command Line Interface] **show running-config snmp-server** コマンドを入力し、[Send] をクリックします。	すべての SNMP サーバ コンフィギュレーション情報を表示します。
[Tools] > [Command Line Interface] **show running-config snmp-server group** コマンドを入力し、[Send] をクリックします。	SNMP グループ コンフィギュレーション設定を表示します。
[Tools] > [Command Line Interface] **show running-config snmp-server host** コマンドを入力し、[Send] をクリックします。	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。
[Tools] > [Command Line Interface] **show running-config snmp-server user** コマンドを入力し、[Send] をクリックします。	SNMP ユーザベース コンフィギュレーション設定を表示します。

パス	目的
[Tools] > [Command Line Interface] **show snmp-server engineid** コマンドを入力し、[Send] をクリックします。	設定されている SNMP エンジンの ID を表示します。
[Tools] > [Command Line Interface] **show snmp-server group** コマンドを入力し、[Send] をクリックします。	設定されている SNMP グループの名前を表示します。 **（注）** 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。
[Tools] > [Command Line Interface] **show snmp-server statistics** コマンドを入力し、[Send] をクリックします。	SNMP サーバの設定済み特性を表示します。
[Tools] > [Command Line Interface] **show snmp-server user** コマンドを入力し、[Send] をクリックします。	ユーザの設定済み特性を表示します。

関連情報

syslog サーバを設定するには、第 41 章「ロギングの設定」を参照してください。

その他の参考資料

SNMP の実装に関するその他の情報については、次の項を参照してください。

- 「SNMP バージョン 3 の RFC」（P.43-11）
- 「MIB」（P.43-11）
- 「アプリケーション サービスとサードパーティ ツール」（P.43-13）

SNMP バージョン 3 の RFC

RFC	タイトル
3410	*『Introduction and Applicability Statements for Internet Standard Management Framework』*
3411	*『An Architecture for Describing SNMP Management Frameworks』*
3412	*『Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)』*
3413	*『Simple Network Management Protocol (SNMP) Applications』*
3414	*『User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMP)』*
3826	*『The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model』*

MIB

リリースごとの ASA および ASASM に対してサポートされている MIB とトラップのリストについては、次の URL を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIB のすべての OID がサポートされるわけではありません。特定の ASA または ASASM に対してサポートされている SNMP MIB および OID のリストを取得するには、[Tools] > [Command Line Interface] を選択し、次のコマンドを入力して [Send] をクリックします。

```
hostname(config)# show snmp-server oidlist
```

（注）　**oidlist** キーワードは **show snmp-server** コマンドのヘルプのオプション リストには表示されませんが、使用できます。ただし、このコマンドは Cisco TAC でのみ使用されます。このコマンドを使用する前に TAC にお問い合わせください。

次に、**show snmp-server oidlist** コマンドの出力例を示します。

```
hostname(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
```

```
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

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 の機能履歴

表 43-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 43-2　SNMP の機能履歴

機能名	プラットフォーム リリース	機能情報
SNMP バージョン 1 および 2c	7.0(1)	クリア テキスト コミュニティ ストリングを使用した SNMP サーバと SNMP エージェントの間でのデータ送信によって、ASA および ASASM ネットワーク モニタリングと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]。
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、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 は、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をレポートします。 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。

表 43-2　SNMP の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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。 **snmp-server enable traps** コマンドが変更されました。
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 がイネーブルになりました。 • 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。
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。