CHAPTER 30

SNMP の設定

この章では、ASA 1000V 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 1000V 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 1000V イーサネット インターフェイス上で実行される SNMP エージェントは、HP OpenView などのネットワーク管理システム（NMS）を介して ASA 1000V をモニタできるようにします。ASA 1000V は GET 要求の発行を通して 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 への特定のイベント（イベント通知）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であるトラップを送信するように ASA 1000V を設定したり、NMS を使用して ASA 1000V の MIB をブラウズしたりできます。MIB は定義の集合であり、ASA 1000V 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。

ASA 1000V 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。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 1000V 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 30-1 に、SNMP で頻繁に使用される用語を示します。

表 30-1　SNMP の用語

用語	説明
エージェント	ASA 1000V 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 1000V 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。

MIB およびトラップに関する情報

MIB は、標準またはエンタープライズ固有です。標準 MIB は Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワーク デバイスで発生する重要なイベント（多くの場合、エ

ラーまたは障害）を報告します。SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、ASA 1000V ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードすることもできます。

http://www.ietf.org/

ftp://ftp-sj.cisco.com/pub/mibs

次の場所から Cisco MIB、トラップ、および OID の完全なリストをダウンロードしてください。

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

また、Cisco OID を次の場所から FTP でダウンロードしてください。

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

（注）　SNMP によりアクセスされるインターフェイス情報は約 5 秒おきにリフレッシュされます。そのため、連続するポーリングの間に少なくとも 5 秒間は待機することをお勧めします。

SNMP オブジェクト ID

シスコのシステムレベルの各製品には、MIB-II の sysObjectID として使用される SNMP オブジェクト ID（OID）があります。CISCO-PRODUCTS-MIB には SNMPv2-MIB の sysObjectID オブジェクトで報告可能な OID が含まれます。モデル タイプを識別するためにこの値を使用できます。表 30-2 に、システムレベルの製品 OID を示します。

表 30-2　SNMP オブジェクト ID

製品 ID	sysObjectID	型番
ciscoASA1000Vsc	ciscoProducts 1613	Cisco Adaptive Security Appliance 1000V クラウド ファイアウォール セキュリティ コンテキスト
ciscoASA1000V	ciscoProducts 1614	Cisco Adaptive Security Appliance 1000V クラウド ファイアウォール

SNMP の物理ベンダー タイプ値

シスコの各シャーシまたはスタンドアロン システムには、SNMP で使用する一意のタイプ番号があります。entPhysicalVendorType OID は CISCO-ENTITY-VENDORTYPE-OID-MIB で定義されます。この値は、ASA 1000V SNMP エージェントから entPhysicalVendorType オブジェクトで返されます。この値を使用してコンポーネントのタイプ（モジュール、電源装置、ファン、センサー、CPU など）を識別できます。表 30-3 に、ASA 1000V の物理ベンダー タイプ値を示します。

表 30-3　SNMP の物理ベンダー タイプ値

項目	entPhysicalVendorType OID の説明	OID
cevChassis 1194	cevChassisASA100V	1.3.6.1.4.1.9.12.3.1.3.1194

MIB でサポートされているテーブルとオブジェクト

表 30-4 に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

表 30-4　MIB でサポートされているテーブルとオブジェクト

MIB 名	サポートされているテーブルとオブジェクト
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid、cempMemPoolUsed、cempMemPoolFree、cempMemPoolUsedOvrflw、cempMemPoolHCUsed、cempMemPoolFreeOvrflw、cempMemPoolHCFree
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
DISMAN-EVENT-MIB	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB	expExpressionTable、expObjectTable、expValueTable
NAT-MIB	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus

サポートされているトラップ（通知）

表 30-5 に、サポートされているトラップ（通知）および関連する MIB を示します。

表 30-5　サポートされているトラップ（通知）

トラップおよび MIB 名	変数バインド リスト	説明
authenticationFailure （SNMPv2-MIB）	—	SNMP バージョン 1 または 2 の場合は、SNMP 要求で指定されたコミュニティ ストリングが正しくありません。SNMP バージョン 3 では、auth または priv パスワードまたはユーザ名が間違っている場合、レポート PDU がトラップの代わりに生成されます。 **snmp-server enable traps snmp authentication** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cipSecTunnelStart （CISCO-IPSEC-FLOW-MONITOR-MIB）	cipSecTunLifeTime、cipSecTunLifeSize	**snmp-server enable traps ipsec start** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cipSecTunnelStop （CISCO-IPSEC-FLOW-MONITOR-MIB）	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** コマンドは、このトラップの送信をイネーブルにするために使用されます。

表 30-5　サポートされているトラップ（通知）（続き）

clogMessageGenerated （CISCO-SYSLOG-MIB）	clogHistFacility、clogHistSeverity、clogHistMsgName、clogHistMsgText、clogHistTimestamp	syslog メッセージが生成されます。 clogMaxSeverity オブジェクトの値は、トラップとして送信する syslog メッセージを決定するために使用されます。 **snmp-server enable traps syslog** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
clrResourceLimitReached （CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB）	crlResourceLimitValueType、crlResourceLimitMax、clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** コマンドは、接続制限に達した通知の送信をイネーブルにするために使用されます。
coldStart （SNMPv2-MIB）	—	SNMP エージェントが起動されました。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cpmCPURisingThreshold （CISCO-PROCESS-MIB）	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** コマンドは、cpu threshold rising 通知の送信をイネーブルにするために使用されます。cpmCPURisingThresholdPeriod オブジェクトは、他のオブジェクトとともに送信されます。
linkDown （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクダウン トラップ。 **snmp-server enable traps snmp linkdown** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
linkUp （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクアップ トラップ。 **snmp-server enable traps snmp linkup** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** コマンドは、memory threshold 通知をイネーブルにするために使用されます。mteHotOID が cempMemPoolHCUsed に設定されます。cempMemPoolName および cempMemPoolHCUsed オブジェクトは、他のオブジェクトとともに送信されます。

表 30-5　サポートされているトラップ（通知）（続き）

mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、ifHCInOctets、ifHCOutOctets、ifHighSpeed、entPhysicalName	**snmp-server enable traps interface-threshold** コマンドは、interface threshold 通知をイネーブルにするために使用されます。entPhysicalName オブジェクトは、他のオブジェクトと共に送信されます。
natPacketDiscard （NAT-MIB）	ifIndex	**snmp-server enable traps nat packet-discard** コマンドは、NAT packet discard 通知をイネーブルにするために使用されます。この通知は、マッピング スペースを使用できないため、5 分間にレート制限され、IP パケットが NAT により廃棄された場合に生成されます。ifIndex は、マッピング インターフェイスの ID を提供します。
warmStart （SNMPv2-MIB）	—	**snmp-server enable traps snmp warmstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

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」（P.30-6）
- 「セキュリティ モデル」（P.30-7）
- 「SNMP グループ」（P.30-7）
- 「SNMP ユーザ」（P.30-7）
- 「SNMP ホスト」（P.30-7）
- 「ASA 1000V と Cisco IOS の実装の違い」（P.30-7）

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 1000V 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 1000V 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-server host** コマンドを追加した後に、ASA 1000V 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 1000V と Cisco IOS の実装の違い

ASA 1000V での SNMP バージョン 3 の実装は、Cisco IOS 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 1000V が開始すると生成されます。
- 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 1000V 規則が作成されます。

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。

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 1000V 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。

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。
- 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。

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 1000V 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、次のコマンドを入力します。

コマンド	目的
snmp-server enable **例：** `hostname(config)# snmp-server enable`	ASA 1000V 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 トラップの設定」（P.30-10）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、次のコマンドを入力します。

コマンド	目的
snmp-server enable traps [**all** | **syslog** | **snmp** [*authentication* | *linkup* | *linkdown* | *coldstart* | *warmstart*] | **entity** [*config-change*] | **ikev2** [*start* | *stop*] |**ipsec** [*start* | *stop*] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [*packet-discard*] **例：** `hostname(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	個別のトラップ、トラップのセット、または NMS へのすべてのトラップを送信します。トラップとして NMS に送信する syslog メッセージをイネーブルにします。デフォルト コンフィギュレーションでは、例に示すように、すべての SNMP 標準トラップがイネーブルになっています。これらのトラップをディセーブルにするには、**no snmp-server enable traps snmp** コマンドを使用します。このコマンドを入力するときにトラップ 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。デフォルトでは、syslog トラップはイネーブルになっています。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。syslog MIB からのトラップを生成するには、**logging history** コマンドと **snmp-server enable traps syslog** コマンドの両方を設定する必要があります。SNMP トラップがイネーブルにされたデフォルトの状態を復元するには、**clear configure snmp-server** コマンドを使用します。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。 CPU 使用率が、設定されたモニタリング期間の設定されたしきい値を超える場合、**cpu threshold rising** トラップが生成されます。 **（注）**　SNMP は電圧センサーをモニタしません。

次の作業

「CPU 使用率しきい値の設定」（P.30-10）を参照してください。

CPU 使用率しきい値の設定

CPU 使用率しきい値を設定するには、次のコマンドを入力します。

コマンド	目的
snmp cpu threshold rising *threshold_value monitoring_period* **例：** `hostname(config)# snmp cpu threshold rising 75% 30 minutes`	高 CPU しきい値およびしきい値モニタリング期間のしきい値を設定します。CPU 使用率のしきい値およびモニタリング期間をクリアするには、このコマンドの **no** 形式を使用します。**snmp cpu threshold rising** コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70 % を超え、クリティカルしきい値レベルのデフォルトは 95 % を超えます。デフォルトのモニタリング期間は 1 分に設定されます。 CPU のクリティカルしきい値レベルは設定できません。この値は 95 % に固定されています。高 CPU しきい値の有効値の範囲は 10 ～ 94 % です。モニタリング期間の有効値は 1 ～ 60 分です。

次の作業

「物理インターフェイスのしきい値の設定」（P.30-11）を参照してください。

物理インターフェイスのしきい値の設定

物理インターフェイスのしきい値を設定するには、次のコマンドを入力します。

コマンド	目的
snmp interface threshold *threshold_value* **例：** `hostname(config)# snmp interface threshold 75%`	SNMP 物理インターフェイスのしきい値を設定します。SNMP 物理インターフェイスのしきい値をクリアするには、このコマンドの **no** 形式を使用します。しきい値は、インターフェイス帯域幅利用率の割合として定義されます。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。

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.30-12）を参照してください。
- 「SNMP バージョン 3 の使用」（P.30-13）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。

手順の詳細

	コマンド	目的

ステップ 1	**snmp-server host** *interface*) *hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | ***2c*** *username*}] [**udp-port** *port*]
	
	例：
	`hostname(config)# snmp-server host mgmt 10.7.14.90 version 2`
	
	`hostname(config)# snmp-server host corp 172.18.154.159 community public`
		SNMP 通知の受信者を指定し、トラップの送信元のインターフェイスを指定し、ASA 1000V に接続できる NMS または SNMP マネージャの名前および IP アドレスを指定します。**trap** キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA 1000V と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルト コミュニティ ストリングは public です。ASA 1000V は、このキーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、コミュニティ ストリングを使用してサイトを指定すると、ASA 1000V と管理ステーションを同じストリングを使用して設定できます。ASA 1000V は指定されたストリングを使用し、無効なコミュニティ ストリングを使用した要求には応答しません。SNMP ホストの詳細については、「SNMP ホスト」（P.30-7）を参照してください。
		
		（注） トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA 1000V で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。

ステップ 2	**snmp-server community** *community-string* **例：** `hostname(config)# snmp-server community onceuponatime`	SNMP バージョン 1 または 2c *だけ*で使用するコミュニティ ストリングを設定します。

ステップ 3	**snmp-server** [**contact** | **location**] *text*
	
	例：
	`hostname(config)# snmp-server location building 42`
	
	`hostname(config)# snmp-server contact EmployeeA`
		SNMP サーバの位置または接点情報を設定します。

次の作業

「SNMP のモニタリング」（P.30-17）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。

手順の詳細

	コマンド	目的
ステップ 1	**snmp-server group** *group-name* **v3** [**auth** | **noauth** | **priv**] **例：** hostname(config)# snmp-server group *testgroup1* v3 auth	SNMP バージョン 3 *だけ*で使用する、新しい SNMP グループを指定します。コミュニティ ストリングが設定されている場合は、コミュニティ ストリングに一致する名前を持つ 2 つの追加グループが自動生成されます。1 つはバージョン 1 のセキュリティ モデルのグループであり、もう 1 つはバージョン 2 のセキュリティ モデルのグループです。セキュリティ モデルの詳細については、「セキュリティ モデル」（P.30-7）を参照してください。**auth** キーワードは、パケット認証をイネーブルにします。**noauth** キーワードは、パケット認証または暗号化が使用されていないことを示します。**priv** キーワードは、パケット暗号化と認証をイネーブルにします。**auth** または **priv** キーワードには、デフォルト値はありません。

	コマンド	目的
ステップ 2	**snmp-server user** *username group-name* {**v3** [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv** [**des** | **3des** | **aes**] [**128** | **192** | **256**] *priv-password* **例：** hostname(config)# snmp-server user *testuser1 testgroup1* v3 auth md5 *testpassword* aes 128 *mypassword* hostname(config)# snmp-server user *testuser1* public v3 encrypted auth md5 *00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF*	SNMP バージョン 3 だけで使用する、SNMP グループの新しいユーザを設定します。*username* 引数は、SNMP エージェントに属するホスト上のユーザの名前です。*group-name* 引数は、ユーザが属するグループの名前です。**v3** キーワードは、SNMP バージョン 3 のセキュリティ モデルを使用することを指定し、**encrypted**、**priv**、および **auth** キーワードの使用をイネーブルにします。**encrypted** キーワードは、暗号化された形式でパスワードを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。**auth** キーワードは、使用する認証レベル（**md5** または **sha**）を指定します。**priv** キーワードは、暗号化レベルを指定します。**auth** または **priv** キーワードのデフォルト値はありません。また、デフォルト パスワードもありません。暗号化アルゴリズムには、**des**、**3des**、または **aes** のキーワードを指定できます。使用する AES 暗号化アルゴリズムのバージョンとして、**128**、**192**、**256** のいずれかを指定することもできます。*auth-password* 引数は、認証ユーザ パスワードを指定します。*priv-password* 引数は、暗号化ユーザ パスワードを指定します。 **（注）** パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。プレーン テキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム（MD5 または SHA にすることができます）に一致する必要があります。ユーザ設定がコンソールに表示される場合、またはファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます（2 番目の例を参照してください）。パスワードの最小長は、英数字 1 文字です。ただし、セキュリティを確保するために 8 文字以上の英数字を使用することを推奨します。
ステップ 3	**snmp-server host** *interface* {*hostname* | *ip_address*} [**trap** | **poll**] [**community** *community-string*] [**version** {***1*** | ***2c*** | ***3*** *username*}] [**udp-port** *port*] **例：** hostname(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1 hostname(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2	SNMP 通知の受信者を指定します。トラップの送信元となるインターフェイスを示します。ASA 1000V に接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。**trap** キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA 1000V と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルト コミュニティ ストリングは public です。ASA 1000V は、このキーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、コミュニティ ストリングを使用してサイトを指定すると、ASA 1000V と NMS を同じストリングを使用して設定できます。ASA 1000V は指定されたストリングを使用し、無効なコミュニティ ストリングを使用した要求には応答しません。SNMP ホストの詳細については、「SNMP ホスト」（P.30-7）を参照してください。 **（注）** SNMP バージョン 3 のホストを ASA 1000V に設定する場合は、ユーザをそのホストに関連付ける必要があります。トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA 1000V で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザを確実に設定するようにします。

	コマンド	目的
ステップ 4	**snmp-server** [**contact** | **location**] *text* **例：** hostname(config)# snmp-server location building 42 hostname(config)# snmp-server contact EmployeeA	SNMP サーバの位置または接点情報を設定します。

次の作業

「SNMP のモニタリング」（P.30-17）を参照してください。

トラブルシューティングのヒント

NMS からの着信パケットを受信する SNMP プロセスが実行されていることを確認するには、次のコマンドを入力します。

```
hostname(config)# show process | grep snmp
```

SNMP からの syslog メッセージをキャプチャし、それらを ASA 1000V コンソールに表示するには、次のコマンドを入力します。

```
hostname(config)# logging list snmp message 212001-212015
hostname(config)# logging console snmp
```

SNMP プロセスがパケットを送受信していることを確認するには、次のコマンドを入力します。

```
hostname(config)# clear snmp-server statistics
hostname(config)# show snmp-server statistics
```

出力は SNMPv2-MIB の SNMP グループに基づきます。

SNMP パケットが ASA 1000V を通過し、SNMP プロセスに送信されていることを確認するには、次のコマンドを入力します。

```
hostname(config)# clear asp drop
hostname(config)# show asp drop
```

NMS が正常にオブジェクトを要求できない場合、または ASA 1000V からの着信トラップを処理していない場合は、次のコマンドを入力して、問題を分離するためにパケット キャプチャを使用します。

```
hostname (config)# access-list snmp permit udp any eq snmptrap any
hostname (config)# access-list snmp permit udp any any eq snmp
hostname (config)# capture snmp type raw-data access-list snmp interface mgmt
hostname (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

ASA 1000V が予期したとおりに実行していない場合は、次の操作を実行して、ネットワーク トポロジとトラフィックに関する情報を取得します。

- NMS の設定について、次の情報を取得します。
  - タイムアウトの回数
  - リトライ回数
  - エンジン ID キャッシング

  - 使用されるユーザ名とパスワード
- 次のコマンドを実行します。
  - **show block**
  - **show interface**
  - **show process**
  - **show cpu**

重大エラーが発生した場合は、エラーの再現を支援するために、Cisco TAC にトレースバック ファイルと **show tech-support** コマンドの出力を送信します。

SNMP トラフィックが ASA 1000V イーサネット インターフェイスを通過できない場合、**icmp permit** コマンドを使用して、リモート SNMP サーバからの ICMP トラフィックの許可が必要なこともあります。

インターフェイスの種類と例

SNMP トラフィック統計情報を生成するインターフェイスの種類には次のものがあります。

- 論理：物理統計情報のサブセットであり、ソフトウェア ドライバによって収集される統計情報。
- 物理：ハードウェア ドライバによって収集される統計情報。物理的な名前の付いた各インターフェイスは、それに関連付けられている論理統計情報と物理統計情報のセットを 1 つ持っています。各物理インターフェイスは、関連付けられている VLAN インターフェイスを複数持っている場合があります。VLAN インターフェイスは論理統計情報だけを持っています。

（注） 複数の VLAN インターフェイスが関連付けられている物理インターフェイスでは、ifInOctets と ifOutoctets の OID の SNMP カウンタがその物理インターフェイスの集約トラフィック カウンタと一致していることに注意してください。

- VLAN-only：SNMP は ifInOctets と ifOutOctets に対して論理統計情報を使用します。

表 30-6 の例で、SNMP トラフィック統計情報における差異を示します。例 1 では、**show interface** コマンドと **show traffic** コマンドの物理出力統計情報と論理出力統計情報の差異を示します。例 2 では、**show interface** コマンドと **show traffic** コマンドの VLAN だけのインターフェイスに対する出力統計情報を示します。この例は、統計情報が **show traffic** コマンドに対して表示される出力に近いことを示しています。

表 30-6　物理インターフェイスと VLAN インターフェイスの SNMP トラフィック統計情報

例 1

```
hostname# show interface GigabitEthernet3/2
interface GigabitEthernet3/2
    description fullt-mgmt
    nameif mgmt
    security-level 10
    ip address 10.7.14.201 255.255.255.0
    management-only

hostname# show traffic
(Condensed output)

Physical Statistics
GigabitEthernet3/2:
    received (in 121.760 secs)
        36 packets       3428 bytes
        0 pkts/sec      28 bytes/sec

Logical Statistics
mgmt:
    received (in 117.780 secs)
        36 packets       2780 bytes
        0 pkts/sec      23 bytes/sec
```

次の例は、管理インターフェイスと物理インターフェイスの SNMP 出力統計情報を示しています。ifInOctets 値は、**show traffic** コマンド出力で表示される物理統計情報出力に近くなりますが、論理統計情報出力には近くなりません。

管理インターフェイスの ifIndex 値：

```
IF_MIB::ifDescr.6 = ASA 1000V 'mgmt' interface
```

物理インターフェイス統計情報に対応する ifInOctets 値：

```
IF-MIB::ifInOctets.6 = Counter32:3246
```

例 2

```
hostname# show interface GigabitEthernet0/0.100
interface GigabitEthernet0/0.100
    vlan 100
    nameif inside
    security-level 100
    ip address 10.7.1.101 255.255.255.0 standby
    10.7.1.102

hostname# show traffic
inside
    received (in 9921.450 secs)
        1977 packets       126528 bytes
        0 pkts/sec      12 bytes/sec
    transmitted (in 9921.450 secs)
        1978 packets       126556 bytes
        0 pkts/sec      12 bytes/sec
```

VLAN の ifIndex 値、内部：

```
IF-MIB::ifDescr.9 = ASA 1000V 'inside' interface
IF-MIB::ifInOctets.9 = Counter32: 126318
```

SNMP のモニタリング

NMS は、SNMP イベントのモニタおよび ASA 1000V 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」（P.30-18）
- 「SNMP モニタリング」（P.30-18）

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 1000V 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 1 つ以上のコマンドを入力します。

コマンド	目的
show running-config [**default**] **snmp-server**	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。
show running-config snmp-server group	SNMP グループ 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 user	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。
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。 **（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。
show snmp-server statistics	SNMP サーバ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	ユーザの設定済み特性を表示します。

例

次の例は、SNMP サーバの統計情報を表示する方法を示しています。

```
hostname(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
```

```
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

次の例は、SNMP サーバの実行コンフィギュレーションを表示する方法を示しています。

```
hostname(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP の設定例

この項は、次の内容で構成されています。

SNMP バージョン 1 および 2c の設定例

次の例は、どのホストにも SNMP syslog 要求を送信せずに、ASA 1000V が内部インターフェイスでホスト 192.0.2.5 からの SNMP 要求を受信する方法を示しています。

```
hostname(config)# snmp-server host 192.0.2.5
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact EmployeeA
hostname(config)# snmp-server community ohwhatakeyisthee
```

SNMP バージョン 3 の設定例

次の例は、ASA 1000V が SNMP バージョン 3 のセキュリティ モデルを使用して SNMP 要求を受信する方法を示しています。このモデルでは、グループ、ユーザ、ホストという一定の順序で設定する必要があります。

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

関連情報

syslog サーバを設定するには、第 29 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.30-20）
- 「MIB」（P.30-20）
- 「アプリケーション サービスとサードパーティ ツール」（P.30-22）

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 1000V 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 1000V 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、次のコマンドを入力します。

```
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。

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 30-7 に、それぞれの機能変更を示します。

表 30-7　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	8.7(1)	オブジェクト ID および物理的なベンダー タイプ値が ASA 1000V をサポートするために追加されました。