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。

用語	説明
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。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）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 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/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

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。

https://github.com/cisco/cisco-mibs/tree/main/oid

（注） ソフトウェア バージョン 7.2(1)、8.0(2) 以降では、SNMP を介してアクセスされるインターフェイス情報は 5 秒ごと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。

MIB のすべての OID がサポートされているわけではありません。特定の ASA 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。

```
ciscoasa(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。

```
ciscoasa(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--
```

SNMP オブジェクト識別子

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 と CISCO-ENTITY-VENDORTYPE-OID-MIB は、SNMPv2-MIB、Entity Sensor MIB および Entity Sensor Threshold Ext MIB の sysObjectID オブジェクト内で報告できる OID が含まれています。モデル タイプを識別するためにこの値を使用できます。次の表に、ASA および ISA モデルの sysObjectID OID を示します。

表 *2 : SNMP* オブジェクト識別子

製品 ID	sysObjectID	モデル番号
ASA 仮想	ciscoASAv（ciscoProducts 1902）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）
ASA 仮想 システム コンテキスト	ciscoASAvsy（ciscoProducts 1903）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）のシステム コンテキスト
ASA 仮想 セキュリティ コンテキスト	ciscoASAvsc（ciscoProducts 1904）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）のセキュリティ コンテキスト。
Cisco Secure Firewall 1200	ciscoCsf1210ce（ciscoProducts 3303） ciscoCsf1210cp（ciscoProducts 3304） ciscoCsf1220cx（ciscoProducts 3305）	CSF1210CE、CSF1210CP、CSF1220CX
Cisco Secure Firewall 4200	ciscoFpr4215td（ciscoProducts 3043） ciscoFpr4225td（ciscoProducts 3042） ciscoFpr4245td（ciscoProducts 3041）	FPR4215、FPR4225、FPR4245
ISA 30004C 産業用セキュリティ アプライアンス	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C（4 GE Copper セキュリティ コンテキスト）	ciscoProducts 2139	ciscoISA30004Csc

製品 ID	sysObjectID	モデル番号
CISCO ISA30004C（4 GE Copper システム コンテキスト）	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F 産業用セキュリティ アプライアンス	ciscoProducts 2267	ciscoISA30002C2F
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ セキュリティ コンテキスト）	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ システム コンテキスト）	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco 産業用セキュリティ アプライアンス（ISA）30004C シャーシ	cevChassis 1677	cevChassisISA30004C
Cisco 産業用セキュリティ アプライアンス（ISA）30002C2F シャーシ	cevChassis 1678	cevChassisISA30002C2F
ISA30004C Copper SKU 向け中央演算処理装置温度センサー	cevSensor 187	cevSensorISA30004CCpuTempSensor
ISA30002C2F 光ファイバ向け中央演算処理装置温度センサー	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
ISA30004C Copper SKU 向けプロセッサ カード温度センサー	cevSensor 192	cevSensorISA30004CPTS
ISA30002C2F Fiber SKU 向けプロセッサ カード温度センサー	cevSensor 193	cevSensorISA30002C2FPTS
ISA30004C Copper SKU 向けパワー カード温度センサー	cevSensor 197	cevSensorISA30004CPowercardTS
ISA30002C2F Fiber SKU 向けパワー カード温度センサー	cevSensor 198	cevSensorISA30002C2FPowercardTS
ISA30004C 向けポート カード温度センサー	cevSensor 199	cevSensorISA30004CPortcardTS
ISA30002C2F 向けポート カード温度センサー	cevSensor 200	cevSensorISA30002C2FPortcardTS
ISA30004C Copper SKU 向け中央演算処理装置	cevModuleCpuType 329	cevCpuISA30004C

製品 ID	sysObjectID	モデル番号
ISA30002C2F 光ファイバ SKU 向け中央演算処理装置	cevModuleCpuType 330	cevCpuISA30002C2F
モジュール ISA30004C、ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Cisco ISA30004C/ISA30002C2F ハードウェア バイパス	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
Cisco Secure Firewall 1210CE	cevChassis 2580	cevChassisCsf1210ce
Secure Firewall 1210CP Chassis	cevChassis 2581	cevChassisCsf 1210cp
Secure Firewall 1220CX Chassis	cevChassis 2582	cevChassisCsf1220cx
Secure Firewall 1200 シリーズ ファン	cevFan 468	cevFanCsf1200
Cisco Secure Firewall 1220CX 向け中央演算処理装置	cevModuleCpuType 380	cevCpuCsf1220cx
Cisco Secure Firewall 1210CP 向け中央演算処理装置	cevModuleCpuType 381	cevCpuCsf1210cp
Cisco Secure Firewall 1210CE 向け中央演算処理装置	cevModuleCpuType 382	`cevCpuCsf 1210ce`
FirePOWER 4140 セキュリティ アプライアンス、1U（組み込みセキュリティ モジュール 36）	ciscoFpr4140K9（ciscoProducts 2293）	FirePOWER 4140
FirePOWER 4120 セキュリティ アプライアンス、1U（組み込みセキュリティ モジュール 24）	ciscoFpr4120K9（ciscoProducts 2294）	FirePOWER 4120
FirePOWER 4K ファン ベイ	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K 電源ベイ	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Secure Firewall Threat Defense Virtual、VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firewall Threat Defense Virtual、AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

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、ASA 仮想、または ASASM の 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。次の表に、ASA モデルの物理ベンダータイプ値を示します。

表 *3*: 物理ベンダー タイプ値

項目	**entPhysicalVendorType OID** の説明
ギガビット イーサネット ポート	cevPortGe（cevPort 109）
Cisco 適応型セキュリティ仮想アプライアンス	cevChassisASAv（cevChassis 1451）
Cisco Secure Firewall 4200-X（FPR4215/FPR4225/FPR4245）	cevFPRNM4X200Gng および cevFPRNM2X100Gng（デュアル EPM 2X100G および 4X200G がスロット 2 およびスロット 3 に追加された場合）

MIB でサポートされるテーブルおよびオブジェクト

次の表 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。

マルチコンテキストモードでは、これらのテーブルとオブジェクトは単一のコンテキストに関する情報を提供します。コンテキスト全体のデータが必要な場合は、それらを合計する必要があります。たとえば、全体的なメモリ使用量を取得するには、各コンテキストの cempMemPoolHCUsed 値を合計します。

表 *4*: *MIB* でサポートされるテーブルおよびオブジェクト

MIB 名と **OID**	サポートされているテーブルとオブジェクト
ENTITY-MIB。OID：1.3.6.1.2.1.47	entPhysicalTable、entPhysicalDescr、entPhysicalVendorType、entPhysicalName

MIB 名と OID	サポートされているテーブルとオブジェクト
CISCO-ENHANCED-MEMPOOL-MIB、OID:1.3.6.1.4.1.9.9.221	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid 32 ビットメモリシステムの場合は、32 ビットメモリカウンタを使用してポーリング：cempMemPoolUsed、cempMemPoolFree、cempMemPoolUsedOvrflw、cempMemPoolFreeOvrflw、cempMemPoolLargestFree、cempMemPoolLowestFree、cempMemPoolUsedLowWaterMark、cempMemPoolAllocHit、cempMemPoolAllocMiss、cempMemPoolFreeHit、cempMemPoolFreeMiss、cempMemPoolLargestFreeOvrflw、cempMemPoolLowestFreeOvrflw、cempMemPoolUsedLowWaterMarkOvrflw、cempMemPoolSharedOvrflw 64 ビットメモリシステムの場合は、64 ビットメモリカウンタを使用してポーリング：cempMemPoolHCUsed、cempMemPoolHCFree、cempMemPoolHCLargestFree、cempMemPoolHCLowestFree、cempMemPoolHCUsedLowWaterMark、cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB、OID:1.3.6.1.4.1.9.9.392 （注） これら 3 つの MIB OID を使用して、リモートアクセス接続が失敗する理由を追跡できます。	crasNumTotalFailures、crasNumSetupFailInsufResources、crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB、OID:1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、OID:1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB、OID:1.3.6.1.4.1.9.9.720 （注） ASA 仮想 ではサポートされていません。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB、OID:1.3.6.1.2.1.88	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB、OID:1.3.6.1.2.1.90	expExpressionTable、expObjectTable、expValueTable
ENTITY-SENSOR-MIB、OID: 1.3.6.1.2.1.99 （注） シャーシの温度、ファンRPM、電源電圧などの物理センサーに関連する情報を提供します。ASA 仮想プラットフォームではサポートされません。	entPhySensorTable

MIB 名と OID	サポートされているテーブルとオブジェクト
NAT-MIB、OID:1.3.6.1.2.1.123	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus
CISCO-PTP-MIB、OID:1.3.6.1.4.1.9.9.760 （注） E2E トランスペアレント クロック モードに対応する MIB のみがサポートされます。	ciscoPtpMIBSystemInfo、cPtpClockDefaultDSTable、cPtpClockTransDefaultDSTable、cPtpClockPortTransDSTable
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 ～ 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev cpmCPUTotal1minRev の関連パラメータと値 例： • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - 集約システム CPU 使用率（この値は、シングルコンテキストモードの .3.6.1.4.1.9.9.109.1.1.1.1.7.1 のシステム CPU 使用率と同じです）。 • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort 平均 CPU 使用率（すべての snort インスタンスの合計値） • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - システムプロセス平均 %（「Sysproc」コアの平均）

サポートされるトラップ（通知）

次の表 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 *5:* サポートされるトラップ（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。
bgpBackwardTransition	bgpPeerLastError、bgpPeerState	**snmp-server enable traps peer-flap** コマンドは、BGP ピアフラップに関連する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。
ccmCLIRunningConfigChanged （CISCO-CONFIG-MAN-MIB）	ccmHistoryRunningLastChanged、ccmHistoryEventTerminalType	**snmp-server enable traps config** 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。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-insert** コマンドはこの通知をイネーブルにするために使用されます。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-remove** コマンドはこの通知をイネーブルにするために使用されます。

トラップおよび MIB 名	変数バインド リスト	説明
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName、 entPhysicalDescr、 entPhySensorValue、 entPhySensorType、 ceSensorExtThresholdValue	**snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] コマンドは、エンティティしきい値通知の伝送をイネーブルにするために使用されます。この通知は、電源障害に対して送信されます。送信されるオブジェクトは、ファンおよび CPU の温度を指定します。 **snmp-server enable traps entity fan-failure** コマンドは、ファン障害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。このトラップは、Firepower 2100 シリーズには適用されません。 **snmp-server enable traps entity power-supply-failure** コマンドは、電源障害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。 **snmp-server enable traps entity chassis-fan-failure** コマンドは、シャーシファン障害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。 **snmp-server enable traps entity cpu-temperature** コマンドは、高 CPU 温度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。 **snmp-server enable traps entity power-supply-presence** コマンドは、電源プレゼンス障害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。 **snmp-server enable traps entity power-supply-temperature** コマンドは、電源温度しきい値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。 **snmp-server enable traps entity chassis-temperature** コマンドは、シャーシ周囲温度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。 **snmp-server enable traps entity accelerator-temperature** コマンドは、シャーシアクセラレータ温度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。

トラップおよび MIB 名	変数バインド リスト	説明
cikeTunnelStart （CISCO-IPSEC-FLOW-MONITOR-MIB）	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunLifeTime	**snmp-server enable traps ikev2 start** コマンドは、ikev2 start 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。
cikeTunnelStop （CISCO-IPSEC-FLOW-MONITOR-MIB）	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunActiveTime	**snmp-server enable traps ikev2 stop** コマンドは、ikev2 stop 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。
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。
ciscoConfigManEvent （CISCO-CONFIG-MAN-MIB）	ccmHistoryEventCommandSource、 ccmHistoryEventConfigSource、 ccmHistoryEventConfigDestination	**snmp-server enable traps config** 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。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions、 crasNumUsers、 crasMaxSessionsSupportable、 crasMaxUsersSupportable、 crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** コマンドは、これら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。
ciscoUFwFailoverStateChanged （CISCO-UNIFIED-FIREWALL-MIB）	gid、FOStatus	**snmp-server enable traps failover-state** コマンドは、failover-state 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。
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、この connection-limit-reached 通知の伝送を有効にするために使用されます。clogOriginID オブジェクトには、トラップを発信したコンテキスト名が含まれています。

トラップおよび MIB 名	変数バインド リスト	説明
coldStart （SNMPv2-MIB）	—	SNMP の設定後に SNMP エージェントが起動するときに発生する ColdStart トラップ。このトラップは、システムの再起動後にエージェントが起動したときにも発生します。 （注） クラスタノードと HA ノードの場合、リロード後、インターフェイスのリブート時間が 5 分（プリセットしきい値）を超えると、トラップはドロップされます。クラスタおよびHA ノードが正常に再起動すると、他のすべてのトラップが想定どおりに送信されます。 **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 通知の伝送を有効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。
cufwClusterStateChanged （CISCO-UNIFIED-FIREWALL-MIB）	status	**snmp-server enable traps cluster-state** コマンドは、cluster-state 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。
entConfigChange （ENTITY-MIB）	—	**snmp-server enable traps entity config-change fru-insert fru-remove** コマンドは、この通知をイネーブルにするために使用されます。 （注） この通知は、セキュリティ コンテキストが作成または削除された場合にマルチ モードでのみ送信されます。
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。

トラップおよび MIB 名	変数バインド リスト	説明
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 通知を有効にするために使用されてます。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。
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 通知を有効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 通知を有効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。
ospfNbrStateChange	ospfRouterId、ospfNbrIpAddr、ospfNbrAddressLessIndex、ospfNbrRtrId、ospfNbrState	**snmp-server enable traps peer-flap** コマンドは、OSPF peer-flap に関連する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。 （注） ASA5585 モデルの場合、netsnmp バージョン 5.8 ライブラリを使用するように SNMP エンジンが変更されており、次の OID はライブラリで使用できません。 • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3

トラップおよび MIB 名	変数バインド リスト	説明
warmStart （SNMPv2-MIB）	—	SNMP エージェントが初めて再起動したときに発生するwarmStartトラップ。このトラップは、SNMP 設定の変更後にエージェントが再起動した場合にも発生し、すべてのSNMPホスト設定が削除され、新しいSNMP設定が行われます。 **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。

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。

次の表の例で、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 *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

```
ciscoasa# 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

ciscoasa# 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。

mgmt インターフェイスの ifIndex：

```
IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface
```

物理インターフェイス統計情報に対応する物理インターフェイス統計：

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

例 2

```
ciscoasa# show interface GigabitEthernet
interface GigabitEthernet0/0.100
vlan 100
nameif inside
security-level 100
ip address 10.7.1.101 255.255.255.0 stan

ciscoasa# 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
```

内部の VLAN の ifIndex：

```
IF-MIB::ifDescr.9 = Adaptive Security Ap
IF-MIB::ifInOctets.9 = Counter32: 126318
```

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-server host** コマンドを追加した後に、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。
- 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。

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。

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

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

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(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。

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(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 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。

```
ciscoasa(config)# clear asp drop
ciscoasa(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 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、パケットキャプチャを使用して問題を切り離します。

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

- ASA が期待どおりに動作していない場合は、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

    使用されるユーザー名とパスワード

  - 次のコマンドを発行します。

    show block

    show interface

    show process

    show cpu

    show vm

- 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 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 サーバーから ICMP トラフィックを許可する必要がある場合があります。
- **snmp-server enable oid** でデバイスを設定している場合、SNMP ウォークの操作を実行すると、ASA は MEMPOOL_DMA プールと MEMPOOL_GLOBAL_SHARED プールからメモリ

情報を照会します。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。この問題を軽減するには、 **no snmp-server enable oid** コマンドを使用して、グローバル共有プールに関連する OID をポーリングしないようにしてください。無効にすると、mempool OID は 0 バイトを返します。

- ASP ドロップカウンタをポーリングするための単一の要求で多数の OID を指定して SNMPGET を使用する場合、ASP ドロップカウンタのポーリングを繰り返す必要があり、CPU 使用率が高くなります。そのため、モニターする重要なカウンタを特定し、カウンタごとに SNMPGET を使用してそれらの値を取得することで、CPU への影響を限定的なものにすることをお勧めします。
- マルチコンテキスト ASA の複数のコンテキストで SNMP が設定されている場合は、コンテキストを順番にポーリングし、snmpwalk ではなく SNMPBULKGET を使用してプラットフォームへの接続数を減らします。このアプローチにより、多数のコンテキストが同時にポーリングされている場合に、SNMP による遅延やタイムアウトを回避できます。
- ASA は、SNMP BULKGET などの SNMP get-response メッセージで SNMP ポーリングに応答する場合は、Don't Fragment（DF）ビットを常に設定します。この場合、ネットワークパス全体が、ASA で設定されている最大伝送ユニット（MTU）をサポートする必要があります。ネットワーク パスで設定された MTU の値を小さくすると、他のデバイスからフラグメンテーションを要求する ICMP パケットが送信されることがあります。ただし、DF ビットが設定されているため、ASA は応答せず、パケットをフラグメント化しません。その結果、ASA からの応答は失われます。

  この問題に対処するには、ASA またはネットワークパス全体で MTU を変更するか、SNMPBULKGET の代わりに複数の get 要求を使用するか、または SNMPBULKGET 要求のバルク サイズを小さくします。

- トラブルシューティングの追加情報については、次の URL を参照してください。
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

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 SNMP エージェントおよび SNMP サーバーをイネーブルにします。

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 エージェントおよび SNMP サーバーの有効化

SNMPエージェントおよびSNMPサーバーをイネーブルにするには、次の手順を実行します。

手順

ASA で SNMP エージェントおよび SNMP サーバーを有効にします。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。

snmp-server enable

例：

```
ciscoasa(config)# snmp-server enable
```

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

個別のトラップ、トラップのセット、またはすべてのトラップを NMS に送信します。

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

このコマンドでは、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ています。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。このトラップを無効にするには、**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。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。

管理コンテキストでのみ使用できるトラップ：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してだけ管理コンテキストを介して生成されたトラップ：

- **interface-threshold**

その他すべてのトラップは、シングル モードの管理およびユーザー コンテキストで使用できます。

config トラップを指定すると、ciscoConfigManEvent 通知と ccmCLIRunningConfigChanged 通知がイネーブルになります。これらの通知は、コンフィギュレーション モードを終了した後に生成されます。

CPU 使用率が、設定されたモニタリング期間に設定済みしきい値を超えると、**cpu threshold rising** トラップが生成されます。

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、**memory-threshold** 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。

一部のトラップは、特定のハードウェア モデルに適用できません。トラップキーワードの代わりに ? を使用すると、デバイスで使用可能なトラップを確認できます。次に例を示します。

- Firepower 1000 シリーズ は、次のエンティティトラップのみをサポートします：**chassis-temperature**、**config-change**、および **cpu-temperature**。

（注）
SNMP は電圧センサーをモニターしません。

CPU 使用率のしきい値の設定

CPU 使用率のしきい値を設定するには、次の手順を実行します。

手順

高 CPU しきい値の値とモニタリング期間を設定します。

snmp cpu threshold rising *threshold_value monitoring_period*

例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

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。

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、次の手順を実行します。

手順

SNMP 物理インターフェイスのしきい値を設定します。

snmp interface threshold *threshold_value*

例：

```
ciscoasa(config)# snmp interface threshold 75%
```

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。

snmp interface threshold コマンドを使用できるのは、管理コンテキストのみです。

物理インターフェイスの使用状況はシングル モードおよびマルチ モードでモニターされ、システム コンテキストの物理インターフェイスのトラップは管理コンテキストを通して送信されます。物理インターフェイスだけがしきい値の使用状況を計算するために使用されます。

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 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。

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

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 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。デフォルトのコミュニティ ストリングは public です。ASA では、このキーを使用して着信 SNMP 要求が有効かどうかを判別します。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し、同じストリングを使って ASA と管理ステーションを設定できます。ASA 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。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。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

version キーワードは、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。

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 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 でユーザーを確実に設定するようにします。

ステップ 2 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。

snmp-server community *community-string*

例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

（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 SNMP サーバーの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前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 4 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

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 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。

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

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。**auth** キーワードは、パケット認証を有効にします。**noauth** キーワードは、パケット認証や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有効にします。**auth** または **priv** キーワードには、デフォルト値がありません。

ステップ 2 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ーを設定します。

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(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
```

username 引数は、SNMP エージェントに属するホスト上のユーザーの名前です。ユーザー名を 32 文字までで入力します。名前の先頭は文字である必要があります。有効な文字は、文字、数字、_（アンダースコア）です。.（ピリオド）、@（アットマーク）、-（ハイフン）も指定できます。

group-name 引数は、ユーザー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有効化します。**engineID** キーワードはオプションで、ユーザーの認証と暗号化の情報をローカライズするために使用される ASA のエンジン ID を指定します。engineID 引数には、有効な ASA エンジン ID を指定する必要があります。

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、次の要件を満たしている必要があります。

- 16 進数形式。
- 8 ～ 80 文字を含む。
- 文字、数字、および ~`!@#%^&*()_-+{}[]|\:;"'<,>./ のみを含む。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。

- 5 つ以上の異なる文字を含める必要があります。
- 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は 4 つ、「ZYXW」は 3 つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。

（注）
連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。

auth キーワードは、使用する認証レベル（**sha**、**sha224**、**sha256**、または **sha384**）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、**3des** または **aes** 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、認証ユーザー パスワードを指定します。priv-password 引数は、暗号化ユーザー パスワードを指定します。

パスワードを忘れた場合は、回復できないため、ユーザー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（SHA、SHA-224、SHA-256、または SHA-384）に一致する必要があります。ユーザー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。

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。

制御ユニットまたはアクティブユニットで **encrypted** キーワードを使用してユーザを入力すると、SNMPv3 ユーザコマンドがレプリケートされないことを通知するエラーメッセージが表示されます。この動作は、既存の SNMPv3 ユーザおよびグループコマンドがレプリケーション中にクリアされないことも意味します。

たとえば、暗号化されたキーで入力されたコマンドを使用する制御ユニットまたはアクティブユニットは次のようになります。

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

クラスタ複製時のデータユニットの場合の例（**snmp-server user** コマンドが設定にある場合にのみ表示されます）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

ステップ 3 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指定します。ASA 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。

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

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 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 は、このキーを使用して、着信 SNMP 要求が有効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 と NMS を同じストリングを使用して設定できます。ASA 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。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリアテキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

version キーワードは、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。

SNMP バージョン 3 のホストを ASA に設定する場合は、ユーザー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 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 でユーザーを確実に設定するようにします。

ステップ 4 SNMP サーバーの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前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 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

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

SNMP ユーザー リストを設定します。

snmp-server user-list *list_name* **username** *user_name*

例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 引数には、ユーザー リストの名前を指定します。最大 33 文字まで指定できます。**username** *user_name* のキーワードと引数のペアで、ユーザー リストに設定するユーザーを指定します。ユーザー リストのユーザーは、**snmp-server user** *username* コマンドで設定します。

このコマンドは、SNMP バージョン 3 を使用している場合にのみ使用できます。ユーザー リストには複数のユーザーを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

ネットワーク オブジェクトへのユーザーの関連付け

ユーザー リストの単一のユーザーまたはユーザーのグループをネットワーク オブジェクトに関連付けるには、次の手順を実行します。

手順

ユーザー リストの単一のユーザーまたはユーザーのグループをネットワーク オブジェクトに関連付けます。

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 引数は、ユーザーまたはユーザー グループを関連付けるインターフェイスのネットワーク オブジェクト名を指定します。

trap キーワードは、トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。SNMP トラップはデフォルトでイネーブルになっています。

poll キーワードは、ホストでブラウズ（ポーリング）が可能であるものの、トラップの送信はできないことを指定します。

community キーワードは、NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。このキーワードは、SNMP バージョン 1 または 2c でのみ使用できます。*community-string* 引数には、通知または NMS からの要求で送信されるコミュニティ ストリングを指定します。コミュニティ ストリングはパスワードのような役割を果たします。このコミュニティ ストリングは最大 32 文字です。

version キーワードは、トラップの送信と要求の受け入れ（ポーリング）に使用する SNMP 通知のバージョン（バージョン 1、2c、または 3）を設定します。デフォルトのバージョンは 1 です。

username 引数には、SNMP バージョン 3 を使用する場合にユーザーの名前を指定します。

user-list キーワードと *list_name* 引数で、ユーザー リストの名前を指定します。

udp-port *port* のキーワードと引数の組み合わせは、NMS ホストへの SNMP トラップの送信にデフォルト以外のポートを使用する場合に、NMS ホストの UDP ポート番号を設定します。デフォルトの UDP ポートは 162 です。

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。

- **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。

例

次の例は、SNMP サーバーの統計情報を表示する方法を示しています。

```
ciscoasa(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 サーバー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。

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

SNMP の例

次の項では、すべての SNMP バージョンの参考として使用できる例を示します。

SNMP バージョン 1 および 2c

次の例は、どのホストにも SNMP syslog 要求を送信せずに、ASA 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。

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

SNMP バージョン 3

次の例は、ASA 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、ユーザー、ホストという一定の順序で設定する必要があります。

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

SNMP の履歴

表 *7 : 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。
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。 次のコマンドが導入または変更されました。**show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**, **snmp-server user**、**snmp-server host**
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-server community**、**snmp-server host** コマンドが変更されました。

機能名	バージョン	説明
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。 **snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps** コマンドが導入または変更されました。
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。 **snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server** の各コマンドが導入または変更されました。
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。 次のコマンドが変更されました。**snmp-server enable traps**。
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。 **show snmp-server host** コマンドが変更されました。
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。 次のコマンドが変更されました。**snmp-server enable traps entity**

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コマンド：**snmp-server host** （注） **snmp-server host-group** コマンドは IPv6 をサポートしていません。
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。 新規/変更されたコマンド：**snmp-server enable oid**

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。 変更されたコマンドはありません。
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/変更されたコマンド：**snmp-server user**
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/変更されたコマンド：**snmp-server user**
SNMP over IPv6	9.17(1)	**snmp-server host-group** コマンドは、IPv6 ホスト、範囲、およびサブネットオブジェクトをサポートするようになりました。
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**
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。