SNMP

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

SNMP の概要

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。

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。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、モニタおよび表示される情報の源をユーザに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

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。

ftp://ftp.cisco.com/pub/mibs/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。

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

（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 5506 適応型セキュリティ アプライアンス	ciscoASA5506（ciscoProducts 2114）	ASA 5506-X
ASA 5506 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506sc（ciscoProducts 2115）	ASA 5506-X セキュリティ コンテキスト
ASA 5506 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5506sy（ciscoProducts 2116）	ASA 5506-X システム コンテキスト
ASA 5506W 適応型セキュリティ アプライアンス	ciscoASA5506W（ciscoProducts 2117）	ASA 5506W-X
ASA 5506W 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506Wsc（ciscoProducts 2118）	ASA 5506W-X セキュリティ コンテキスト
ASA 5506W 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5506Wsy（ciscoProducts 2119）	ASA 5506W-X システム コンテキスト
ASA 5508 適応型セキュリティ アプライアンス	ciscoASA5508（ciscoProducts 2120）	ASA 5508-X
ASA 5508 適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5508sc（ciscoProducts 2121）	ASA 5508-X セキュリティ コンテキスト
ASA 5508 適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5508sy（ciscoProducts 2122）	ASA 5508-X システム コンテキスト
ASA 5506 ペイロード暗号化なし適応型セキュリティ アプライアンス	ciscoASA5506K7（ciscoProducts 2123）	ASA 5506-X ペイロード暗号化なし適応型セキュリティ アプライアンス
ASA 5506 ペイロード暗号化なし適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5506K7sc（ciscoProducts 2124）	ASA 5506-X ペイロード暗号化なし適応型セキュリティアプライアンスのセキュリティ コンテキスト
ASA 5506 ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト	ciscoASA5506K7sy（ciscoProducts 2125）	ASA 5506-X ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンス	ciscoASA5508K7（ciscoProducts 2126）	ASA 5508-X ペイロード暗号化なし適応型セキュリティアプライアンスのシステム コンテキスト
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンスのセキュリティ コンテキスト	ciscoASA5508K7sc（ciscoProducts 2127）	ASA 5508-X ペイロード暗号化なし適応型セキュリティアプライアンスのセキュリティ コンテキスト

製品 ID	sysObjectID	モデル番号
ASA 5508 ペイロード暗号化なし適応型セキュリティ アプライアンスのシステム コンテキスト	ciscoASA5508K7sy（ciscoProducts 2128）	ASA 5508-X ペイロード暗号化なし適応型セキュリティ アプライアンスのシステム コンテキスト
ASA5585-SSP10	ciscoASA5585Ssp10（ciscoProducts 1194）	ASA 5585-X SSP-10
ASA5585-SSP20	ciscoASA5585Ssp20（ciscoProducts 1195）	ASA 5585-X SSP-20
ASA5585-SSP40	ciscoASA5585Ssp40（ciscoProducts 1196）	ASA 5585-X SSP-40
ASA5585-SSP60	ciscoASA5585Ssp60（ciscoProducts 1197）	ASA 5585-X SSP-60
ASA5585-SSP10	ciscoASA5585Ssp10sc（ciscoProducts 1198）	ASA 5585-X SSP-10 セキュリティ コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sc（ciscoProducts 1199）	ASA 5585-X SSP-20 セキュリティ コンテキスト
ASA5585-SSP40	ciscoASA5585Ssp40sc（ciscoProducts 1200）	ASA 5585-X SSP-40 セキュリティ コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sc（ciscoProducts 1201）	ASA 5585-X SSP-60 セキュリティ コンテキスト
ASA5585-SSP10	ciscoASA5585Ssp10sy（ciscoProducts 1202）	ASA 5585-X SSP-10 システム コンテキスト
ASA5585-SSP20	ciscoASA5585Ssp20sy（ciscoProducts 1203）	ASA 5585-X SSP-20 システム コンテキスト
ASA5585-SSP40	ciscoASA5585Ssp40sy（ciscoProducts 1204）	ASA 5585-X SSP-40 システム コンテキスト
ASA5585-SSP60	ciscoASA5585Ssp60sy（ciscoProducts 1205）	ASA 5585-X SSP-60 システム コンテキスト
Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1（ciscoProducts 1277）	Catalyst スイッチ/7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール

製品 ID	sysObjectID	モデル番号
Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sc（ciscoProducts 1275）	Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7sc（ciscoProducts 1334）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ セキュリティ コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
Catalyst スイッチ/7600 ルータ システム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1sy（ciscoProducts 1276）	Catalyst スイッチ/7600 ルータ システム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ システム コンテキスト/7600 ルータ向け ASA サービス モジュール	ciscoAsaSm1K7sy（ciscoProducts 1335）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ システム コンテキスト向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ システム コンテキスト向け ASA サービス モジュール	ciscoAsaSm1K7（ciscoProducts 1336）	ペイロード暗号化なし Catalyst スイッチ/7600 ルータ向け適応型セキュリティ アプライアンス（ASA）サービス モジュール
ASA 5512	ciscoASA5512（ciscoProducts 1407）	ASA 5512 適応型セキュリティ アプライアンス
ASA 5525	ciscoASA5525（ciscoProducts 1408）	ASA 5525 適応型セキュリティ アプライアンス
ASA 5545	ciscoASA5545（ciscoProducts 1409）	ASA 5545 適応型セキュリティ アプライアンス
ASA 5555	ciscoASA5555（ciscoProducts 1410）	ASA 5555 適応型セキュリティ アプライアンス
ASA 5512 セキュリティ コンテキスト	ciscoASA5512sc（ciscoProducts 1411）	ASA 5512 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5525 セキュリティ コンテキスト	ciscoASA5525sc（ciscoProducts 1412）	ASA 5525 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5545 セキュリティ コンテキスト	ciscoASA5545sc（ciscoProducts 1413）	ASA 5545 適応型セキュリティ アプライアンスのセキュリティ コンテキスト

製品 ID	sysObjectID	モデル番号
ASA 5555 セキュリティ コンテキスト	ciscoASA5555sc（ciscoProducts 1414）	ASA 5555 適応型セキュリティ アプライアンスのセキュリティ コンテキスト
ASA 5512 システム コンテキスト	ciscoASA5512sy（ciscoProducts 1415）	ASA 5512 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 システム コンテキスト	ciscoASA5515sy（ciscoProducts 1416）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5525 システム コンテキスト	ciscoASA5525sy（ciscoProducts1417）	ASA 5525 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5545 システム コンテキスト	ciscoASA5545sy（ciscoProducts 1418）	ASA 5545 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5555 システム コンテキスト	ciscoASA5555sy（ciscoProducts 1419）	ASA 5555 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515 セキュリティ コンテキスト	ciscoASA5515sc（ciscoProducts 1420）	ASA 5515 適応型セキュリティ アプライアンスのシステム コンテキスト
ASA 5515	ciscoASA5515（ciscoProducts 1421）	ASA 5515 適応型セキュリティ アプライアンス
ASAv	ciscoASAv（ciscoProducts 1902）	Cisco 適応型セキュリティ仮想アプライアンス（ASAv）
ASAv 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（ASAv）システム コンテキスト
ASAv 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（ASAv）セキュリティ コンテキスト
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
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

製品 ID	sysObjectID	モデル番号
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
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

製品 ID	sysObjectID	モデル番号
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
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 4110 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 12）	ciscoFpr4110K9（ciscoProducts 2295）	FirePOWER 4110
FirePOWER 4110 セキュリティ モジュール 12	ciscoFpr4110SM12（ciscoProducts 2313）	FirePOWER 4110 セキュリティ モジュール 12
FirePOWER 4120 セキュリティ モジュール 24	ciscoFpr4120SM24（ciscoProducts 2314）	FirePOWER 4110 セキュリティ モジュール 24
FirePOWER 4140 セキュリティ モジュール 36	ciscoFpr4140SM36（ciscoProducts 2315）	FirePOWER 4110 セキュリティ モジュール 36
FirePOWER 4110 シャーシ	cevChassis 1714	cevChassisFPR4110
FirePOWER 4120 シャーシ	cevChassis 1715	cevChassisFPR4120
FirePOWER 4140 シャーシ	cevChassis 1716	cevChassisFPR4140
FirePOWER 4K ファン ベイ	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K 電源ベイ	cevContainer 364	cevContainerFPR4KPowerSupplyBay
FirePOWER 4120 スーパーバイザ モジュール	cevModuleFPRType 4	cevFPR4120SUPFixedModule
FirePOWER 4140 スーパーバイザ モジュール	cevModuleFPRType 5	cevFPR4140SUPFixedModule
FirePOWER 4110 スーパーバイザ モジュール	cevModuleFPRType 7	cevFPR4110SUPFixedModule
Cisco FirePOWER 4110 セキュリティ アプライアンス、Threat Defense	cevChassis 1787	cevChassisCiscoFpr4110td

製品 ID	sysObjectID	モデル番号
Cisco FirePOWER 4120 セキュリティ アプライアンス、Threat Defense	cevChassis 1788	cevChassisCiscoFpr4120td
Cisco FirePOWER 4140 セキュリティ アプライアンス、Threat Defense	cevChassis 1789	cevChassisCiscoFpr4140td
Cisco Firepower 9000 セキュリティ モジュール 24、Threat Defense	cevChassis 1791	cevChassisCiscoFpr9000SM24td
Cisco Firepower 9000 セキュリティ モジュール 24 NEBS、Threat Defense	cevChassis 1792	cevChassisCiscoFpr9000SM24Ntd
Cisco Firepower 9000 セキュリティ モジュール 36、Threat Defense	cevChassis 1793	cevChassisCiscoFpr9000SM36td
Cisco Firepower Threat Defense Virtual、VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firepower 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、ASAv 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
Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1（cevModuleCat6000Type 169）
ペイロード暗号化なし Catalyst スイッチ/7600 ルータ向け ASA サービス モジュール	cevCat6kWsSvcAsaSm1K7（cevModuleCat6000Type 186）
5506 適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5506（cevOther 10）
5506W 適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5506W（cevOther 11）

項目	entPhysicalVendorType OID の説明
5508適応型セキュリティアプライアンス向けアクセラレータ	cevAcceleratorAsa5508（cevOther 12）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5506K7（cevOther 13）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ	cevAcceleratorAsa5508K7（cevOther 14）
Cisco 適応型セキュリティ アプライアンス（ASA）5506 シャーシ	cevChassisAsa5506（cevChassis 1600）
Cisco 適応型セキュリティ アプライアンス（ASA）5506W シャーシ	cevChassisAsa5506W（cevChassis 1601）
Cisco 適応型セキュリティ アプライアンス（ASA）5508 シャーシ	cevChassisAsa5508（cevChassis 1602）
ペイロード暗号化なしCisco適応型セキュリティアプライアンス（ASA）5506 シャーシ	cevChassisAsa5506K7（cevChassis 1603）
ペイロード暗号化なしCisco適応型セキュリティアプライアンス（ASA）5508 シャーシ	cevChassisAsa5508K7（cevChassis 1604）
5506 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506（cevModuleCpuType 312）
5506W 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506W（cevModuleCpuType 313）
5508 適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5508（cevModuleCpuType 314）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5506K7（cevModuleCpuType 315）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置	cevCpuAsa5508K7（cevModuleCpuType 316）
cevModuleASA5506 型のシャーシ	cevModuleASA5506Type（cevModule 107）
5506 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506SSD（cevModuleASA5506Type 1）
5506W 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506WSSD（cevModuleASA5506Type 2）

項目	entPhysicalVendorType OID の説明
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5506K7SSD（cevModuleASA5506Type 3）
cevModuleASA5508 型のシャーシ	cevModuleASA5508Type（cevModule 108）
5508 適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5508SSD（cevModuleASA5508Type 1）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け現場交換可能ソリッド ステート ドライブ	cevModuleAsa5508K7SSD（cevModuleASA5508Type 2）
適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン	cevFanAsa5508ChassisFan（cevFan 247）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン	cevFanAsa5508K7ChassisFan（cevFan 248）
適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン センサー	cevSensorAsa5508ChassisFanSensor（cevSensor 162）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5508 向けシャーシ冷却ファン センサー	cevSensorAsa5508K7ChassisFanSensor（cevSensor 163）
5506 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506CpuTempSensor（cevSensor 164）
5506W 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506WCpuTempSensor（cevSensor 165）
5508 適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5508CpuTempSensor（cevSensor 166）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5506K7CpuTempSensor（cevSensor 167）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向け中央演算処理装置温度センサー	cevSensorAsa5508K7CpuTempSensor（cevSensor 168）
5506適応型セキュリティアプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506AcceleratorTempSensor（cevSensor 169）
5506W 適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506WAcceleratorTempSensor（cevSensor 170）
5508適応型セキュリティアプライアンス向けアクセラレータ温度センサー	cevSensorAsa5508AcceleratorTempSensor（cevSensor 171）

項目	entPhysicalVendorType OID の説明
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5506K7AcceleratorTempSensor（cevSensor 172）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けアクセラレータ温度センサー	cevSensorAsa5508K7AcceleratorTempSensor（cevSensor 173）
5506 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506ChassisTempSensor（cevSensor 174）
5506W 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506WChassisTempSensor（cevSensor 175）
5508 適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5508ChassisTempSensor（cevSensor 176）
5506 ペイロード暗号化なし適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5506K7ChassisTempSensor（cevSensor 177）
5508 ペイロード暗号化なし適応型セキュリティ アプライアンス向けシャーシ周囲温度センサー	cevSensorAsa5508K7ChassisTempSensor（cevSensor 178）
Cisco Adaptive Security Appliance（ASA）5512 適応型セキュリティ アプライアンス	cevChassisASA5512（cevChassis 1113）
Cisco Adaptive Security Appliance（ASA）5512 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5512K7（cevChassis 1108）
Cisco Adaptive Security Appliance（ASA）5515 適応型セキュリティ アプライアンス	cevChassisASA5515（cevChassis 1114）
Cisco Adaptive Security Appliance（ASA）5515 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5515K7（cevChassis 1109）
Cisco Adaptive Security Appliance（ASA）5525 適応型セキュリティ アプライアンス	cevChassisASA5525（cevChassis 1115）
Cisco Adaptive Security Appliance（ASA）5525 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5525K7（cevChassis 1110）
Cisco Adaptive Security Appliance（ASA）5545 適応型セキュリティ アプライアンス	cevChassisASA5545（cevChassis 1116）
Cisco Adaptive Security Appliance（ASA）5545 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5545K7（cevChassis 1111）
Cisco Adaptive Security Appliance（ASA）5555 適応型セキュリティ アプライアンス	cevChassisASA5555（cevChassis 1117）

項目	entPhysicalVendorType OID の説明
Cisco Adaptive Security Appliance（ASA）5555 ペイロード暗号化なし適応型セキュリティ アプライアンス	cevChassisASA5555K7（cevChassis 1112）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512（cevModuleCpuType 229）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置	cevCpuAsa5512K7（cevModuleCpuType 224）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515（cevModuleCpuType 230）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置	cevCpuAsa5515K7（cevModuleCpuType 225）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525（cevModuleCpuType 231）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置	cevCpuAsa5525K7（cevModuleCpuType 226）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545（cevModuleCpuType 232）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置	cevCpuAsa5545K7（cevModuleCpuType 227）
Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555（cevModuleCpuType 233）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置	cevCpuAsa5555K7（cevModuleCpuType 228）
ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10（cevModuleCpuType 204）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU	cevCpuAsa5585Ssp10K7（cevModuleCpuType 205）
ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20（cevModuleCpuType 206）
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU	cevCpuAsa5585Ssp20K7（cevModuleCpuType 207）
ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40（cevModuleCpuType 208）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU	cevCpuAsa5585Ssp40K7（cevModuleCpuType 209）
ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60（cevModuleCpuType 210）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU	cevCpuAsa5585Ssp60K（cevModuleCpuType 211）

項目	entPhysicalVendorType OID の説明
Catalyst スイッチ/7600 ルータ向け Cisco ASA サービス モジュールの CPU	cevCpuAsaSm1（cevModuleCpuType 222）
Catalyst スイッチ/7600 ルータ向けペイロード暗号化なし Cisco ASA サービス モジュールの CPU	cevCpuAsaSm1K7（cevModuleCpuType 223）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512ChassisFan（cevFan 163）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファン	cevFanASA5512K7ChassisFan（cevFan 172）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515ChassisFan（cevFan 164）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファン	cevFanASA5515K7ChassisFan（cevFan 171）
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525ChassisFan（cevFan 165）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファン	cevFanASA5525K7ChassisFan（cevFan 170）
適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545ChassisFan（cevFan 166）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファン	cevFanASA5545K7ChassisFan（cevFan 169）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545K7PSFan（cevFan 161）
適応型セキュリティ アプライアンス 5545 電源ファン	cevFanASA5545PSFan（cevFan 159）
適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555ChassisFan（cevFan 167）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファン	cevFanASA5555K7ChassisFan（cevFan 168）
適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFan（cevFan 160）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファン	cevFanASA5555PSFanK7（cevFan 162）
ASA 5585-X 向け電源ファン	cevFanASA5585PSFan（cevFan 146）

項目	entPhysicalVendorType OID の説明
10 ギガビット イーサネット インターフェイス	cevPort10GigEthernet（cevPort 315）
ギガビット イーサネット ポート	cevPortGe（cevPort 109）
適応型セキュリティ アプライアンス 5545 電源装置	cevPowerSupplyASA5545PSInput（cevPowerSupply 323）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevPowerSupplyASA5545PSPresence（cevPowerSupply 321）
適応型セキュリティ アプライアンス 5555 電源装置	cevPowerSupplyASA5555PSInput（cevPowerSupply 324）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevPowerSupplyASA5555PSPresence（cevPowerSupply 322）
ASA 5585 向け電源入力	cevPowerSupplyASA5585PSInput（cevPowerSupply 304）
Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512ChassisFanSensor（cevSensor 120）
Cisco Adaptive Security Appliance（ASA）5512 向けシャーシ周囲温度センサー	cevSensorASA5512ChassisTemp（cevSensor 107）
Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512CPUTemp（cevSensor 96）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 シャーシ ファン センサー	cevSensorASA5512K7ChassisFanSensor（cevSensor 125）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5512 向け中央演算処理装置温度センサー	cevSensorASA5512K7CPUTemp（cevSensor 102）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512K7PSFanSensor（cevSensor 116）
適応型セキュリティ アプライアンス 5512 シャーシ冷却ファンのセンサー	cevSensorASA5512PSFanSensor（cevSensor 119）
Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515ChassisFanSensor（cevSensor 121）
Cisco Adaptive Security Appliance（ASA）5515 向けシャーシ周囲温度センサー	cevSensorASA5515ChassisTemp（cevSensor 98）
Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515CPUTemp（cevSensor 97）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 シャーシ ファン センサー	cevSensorASA5515K7ChassisFanSensor（cevSensor 126）

項目	entPhysicalVendorType OID の説明
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5515 向け中央演算処理装置温度センサー	cevSensorASA5515K7CPUTemp（cevSensor 103）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515K7PSFanSensor（cevSensor 115）
適応型セキュリティ アプライアンス 5515 シャーシ冷却ファンのセンサー	cevSensorASA5515PSFanSensor（cevSensor 118）
Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525ChassisFanSensor（cevSensor 122）
Cisco Adaptive Security Appliance（ASA）5525 向けシャーシ周囲温度センサー	cevSensorASA5525ChassisTemp（cevSensor 108）
Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525CPUTemp（cevSensor 99）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 シャーシ ファン センサー	cevSensorASA5525K7ChassisFanSensor（cevSensor 127）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5525 向け中央演算処理装置温度センサー	cevSensorASA5525K7CPUTemp（cevSensor 104）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525K7PSFanSensor（cevSensor 114）
適応型セキュリティ アプライアンス 5525 シャーシ冷却ファンのセンサー	cevSensorASA5525PSFanSensor（cevSensor 117）
Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545ChassisFanSensor（cevSensor 123）
Cisco Adaptive Security Appliance（ASA）5545 向けシャーシ周囲温度センサー	cevSensorASA5545ChassisTemp（cevSensor 109）
Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545CPUTemp（cevSensor 100）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 シャーシ ファン センサー	cevSensorASA5545K7ChassisFanSensor（cevSensor 128）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向けシャーシ周囲温度センサー	cevSensorASA5545K7ChassisTemp（cevSensor 90）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5545 向け中央演算処理装置温度センサー	cevSensorASA5545K7CPUTemp（cevSensor 105）

項目	entPhysicalVendorType OID の説明
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 シャーシ冷却ファンのセンサー	cevSensorASA5545K7PSFanSensor（cevSensor 113）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545K7PSPresence（cevSensor 87）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545K7PSTempSensor（cevSensor 94）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5545 電源ファンのセンサー	cevSensorASA5545PSFanSensor（cevSensor 89）
適応型セキュリティ アプライアンス 5545 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 130）
適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5545PSPresence（cevSensor 131）
適応型セキュリティ アプライアンス 5545 電源ファンの温度センサー	cevSensorASA5545PSTempSensor（cevSensor 92）
Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555ChassisFanSensor（cevSensor 124）
Cisco Adaptive Security Appliance（ASA）5555 向けシャーシ周囲温度センサー	cevSensorASA5555ChassisTemp（cevSensor 110）
Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555CPUTemp（cevSensor 101）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 シャーシ ファン センサー	cevSensorASA5555K7ChassisFanSensor（cevSensor 129）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向けシャーシ周囲温度センサー	cevSensorASA5555K7ChassisTemp（cevSensor 111）
ペイロード暗号化なし Cisco Adaptive Security Appliance（ASA）5555 向け中央演算処理装置温度センサー	cevSensorASA5555K7CPUTemp（cevSensor 106）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 シャーシ冷却ファンのセンサー	cevSensorASA5555K7PSFanSensor（cevSensor 112）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源入力のプレゼンス センサー	cevSensorASA5555K7PSPresence（cevSensor 88）
ペイロード暗号化なし適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555K7PSTempSensor（cevSensor 95）

項目	entPhysicalVendorType OID の説明
適応型セキュリティ アプライアンス 5555 電源ファンのセンサー	cevSensorASA5555PSFanSensor（cevSensor 91）
適応型セキュリティ アプライアンス 5555 電源ファンの温度センサー	cevSensorASA5555PSTempSensor（cevSensor 93）
ASA 5585-X 向け電源ファン	cevSensorASA5585PSFanSensor（cevSensor 86）
ASA 5585-X 向け電源入力のセンサー	cevSensorASA5585PSInput（cevSensor 85）
ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10CPUTemp（cevSensor 77）
ペイロード暗号化なし ASA 5585 SSP-10 向け CPU 温度センサー	cevSensorASA5585SSp10K7CPUTemp（cevSensor 78）
ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20CPUTemp（cevSensor 79）
ペイロード暗号化なし ASA 5585 SSP-20 向け CPU 温度センサー	cevSensorASA5585SSp20K7CPUTemp（cevSensor 80）
ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40CPUTemp（cevSensor 81）
ペイロード暗号化なし ASA 5585 SSP-40 向け CPU 温度センサー	cevSensorASA5585SSp40K7CPUTemp（cevSensor 82）
ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60CPUTemp（cevSensor 83）
ペイロード暗号化なし ASA 5585 SSP-60 向け CPU 温度センサー	cevSensorASA5585SSp60K7CPUTemp（cevSensor 84）
適応型セキュリティ アプライアンス 5555-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5555XFRSSD (cevModuleCommonCards 396)
適応型セキュリティ アプライアンス 5545-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5545XFRSSD (cevModuleCommonCards 397)
適応型セキュリティ アプライアンス 5525-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5525XFRSSD (cevModuleCommonCards 398)
適応型セキュリティ アプライアンス 5515-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5515XFRSSD (cevModuleCommonCards 399)
適応型セキュリティ アプライアンス 5512-X 現場交換可能ソリッド ステート ドライブ	cevModuleASA5512XFRSSD (cevModuleCommonCards 400)
Cisco 適応型セキュリティ仮想アプライアンス	cevChassisASAv（cevChassis 1451）

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。

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	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 cempMemPoolPlatformMemory、cempMemPoolLargestFree、cempMemPoolLowestFree、cempMemPoolUsedLowWaterMark、cempMemPoolAllocHit、cempMemPoolAllocMiss、cempMemPoolFreeHit、cempMemPoolFreeMiss、cempMemPoolShared、cempMemPoolLargestFreeOvrflw、cempMemPoolHCLargestFree、cempMemPoolLowestFreeOvrflw、cempMemPoolHCLowestFree、cempMemPoolUsedLowWaterMarkOvrflw、cempMemPoolHCUsedLowWaterMark、cempMemPoolSharedOvrflw、cempMemPoolHCShared
CISCO-ENTITY-SENSOR-EXT-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB （注） Cisco 適応型セキュリティ仮想アプライアンス（ASAv）ではサポートされていません。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	expExpressionTable、expObjectTable、expValueTable

MIB 名	サポートされているテーブルとオブジェクト
ENTITY-SENSOR-MIB （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。 （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。Cisco ASAv プラットフォームではサポートされていません。	entPhySensorTable
NAT-MIB	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus
CISCO-PTP-MIB （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

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。
ccmCLIRunningConfigChanged （CISCO-CONFIG-MAN-MIB）	—	**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。

トラップおよび MIB 名	変数バインド リスト	説明
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL -MIB)	—	**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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL -MIB)	—	**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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。

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) （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	ceSensorExtThresholdValue、entPhySensorValue、entPhySensorType、entPhysicalName	

トラップおよび MIB 名	変数バインド リスト	説明
		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、ASA 5506-X および ASA 5508-X 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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。 **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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。

トラップおよび MIB 名	変数バインド リスト	説明
		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。このトラップは、ASA 5506-X および ASA 5508-X には適用されません。
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）	—	**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。
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。

トラップおよび MIB 名	変数バインド リスト	説明
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。
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。
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） （注） Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。	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。
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。

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 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

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 Appliance 'inside'
 interface
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 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 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。

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 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。

フェールオーバーのガイドライン

各 ASA 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 flash:/snmp/*contextname* にバイナリ ファイルとして書き込まれます。

その他のガイドライン

- 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。
- 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。
- 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、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。
- 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 コンテキストで設定された SNMP サーバ ホストが少なくとも 1 つ必要です。
- 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。
- 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。
- SNMPv3 エンジン ID はクラスタのメンバー間で同期されません。そのため、SNMPv3 については、クラスタの各ユニットでそれぞれ設定する必要があります。
- バージョン 9.4(1) では、ASA がサポートするコンテキストあたりの SNMP サーバのトラップ ホスト数に制限はありません。**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。
- 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 の設定

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 サーバの有効化

SNMP エージェントおよび SNMP サーバ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 サーバを有効にします。デフォルトでは、SNMP サーバはイネーブルになっています。

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。

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-failure**] | *chassis-temperature* | *power-supply-presence* | *power-supply-temperature* | *accelerator-temperature* | *l1-bypass-status*] | **ikev2** [*start* | *stop*] | **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**

（注） **interface-threshold** トラップは、Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

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 コンテキストで使用できます。

マルチ コンテキスト モードでは、**fan-failure** トラップ、**power-supply-failure** トラップ、および **cpu-temperature** トラップは、ユーザ コンテキストではなく管理コンテキストからのみ生成されます（ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X にのみ適用されます）。

accelerator-temperature しきい値トラップは、ASA 5506-X および ASA 5508-X にのみ適用されます。

chassis-fan-failure トラップは、ASA 5506-X には適用されません。

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。

次のトラップは ASA 5506-x および ASA 5508-x に適用されません：**fan-failure**、 **fru-insert**、**fru-remove**、 **power-supply**、 **power-supply-failure**、 **power-supply-presence**、および **power-supply-temperature**。

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 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。

（注） SNMP は電圧センサーをモニタしません。

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。

（注） このコマンドは、Catalyst 6500 スイッチ/7600 ルータ向け ASA サービス モジュールではサポートされていません。

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：

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。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。

（注） ASAソフトウェアをバージョン8.3(1)から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

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
```

ステップ 3 SNMP サーバ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を設定します。

snmp-server user*username group-name* {**v3** [**engineID** *engineID*] [**encrypted**]] [**auth** {**md5** | **sha**]} *auth-password* [**priv**] [**des** | **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有効化します。**engineID** キーワードはオプションで、ユーザ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、16 進数の形式である必要があります。**auth** キーワードは、使用される認証レベル（**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** 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。

クラスタリング環境では、クラスタ化されたそれぞれの ASA について手動で SNMPv3 ユーザを更新する必要があります。これを行うには、マスター ユニットに対する **snmp-server user** *username group-name* **v3** コマンドを入力し、ローカライズされていない形式で *priv-password* オプションおよび *auth-password* オプションを指定します。

クラスタリングの複製または設定時に、SNMPv3 ユーザ コマンドが複製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。この場合、SNMPv3 ユーザおよびグループのコマンドをスレーブの ASA に対して個別に設定します。また、複製の実行時に既存の SNMPv3 ユーザおよびグループのコマンドがクリアされない場合にもメッセージが表示されます。この場合は、クラスタのすべてのスレーブに対して SNMPv3 ユーザおよびグループのコマンドを入力します。次に例を示します。

マスター ユニットに対するコマンドで入力したキーがすでにローカライズされている場合：

```
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.
```

クラスタ複製時のスレーブ ユニットの場合（**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：

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。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

version キーワードは、SNMP トラップのバージョンを指定します。ASA では、SNMP 要求（ポーリング）に基づくフィルタリングはサポートされません。

SNMP バージョン 3 のホストを ASA 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 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 4 SNMP サーバ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。

ユーザのグループの設定

指定したユーザのグループからなる SNMP ユーザ 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 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 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 リストに設定するユーザを指定します。ユー

ザ リストのユーザは、**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 リストには複数のユーザ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の関連付け

ユーザ リストの単一のユーザまたはユーザ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 リストの単一のユーザまたはユーザ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、ユーザまたはユーザ 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。**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。*username* 引数には、SNMP バージョン 3 を使用する場合にユーザ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 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。デフォルトのバージョンは 1 です。SNMP トラップはデフォルトでイネーブルになっています。

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 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。

```
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、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 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 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。
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。
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。
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。

機能名	バージョン	説明
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 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 ASAv が追加されました。 新しい ASAv プラットフォームをサポートするよう、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。
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**。

機能名	バージョン	説明
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 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 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**
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。

機能名	バージョン	説明
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバとの通信、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**
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。