show cr ～ show cz

show crashinfo

フラッシュメモリに格納されている最新のクラッシュ情報ファイルの内容を表示するには、特権 EXEC モードで **show crashinfo** コマンドを使用します。

show crashinfo [**save**]

構文の説明

save （任意）クラッシュ情報をフラッシュメモリに保存するようにASAが設定されているかどうかを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(5)	出力に **show process** コマンド内のスレッド ID（TID）が表示されるようになりました。
9.4(1)	出力には、生成された syslog の最新の 50 行が表示されます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
9.7(1)	最新のシステム生成クラッシュ ファイルのみを表示するように出力が更新されました。

使用上のガイドライン

クラッシュファイルがテストクラッシュから生成された（**crashinfo test** コマンドで生成された）場合、クラッシュファイルの最初のストリングは「**: Saved_Test_Crash**」であり、最後のストリングは「**: End_Test_Crash**」です。クラッシュファイルが実際のクラッシュから生成されたる場合、クラッシュファイルの最初の行の文字列は「**: Saved_Crash**」で、最後の文字列は「**: End_Crash**」です（これには、**crashinfo force page-fault** または **crashinfo force watchdog** コマンドの使用によるクラッシュが含まれます）。

クラッシュデータがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュデータをクリアしていた場合は、**show crashinfo** コマンドを実行するとエラーメッセージが表示されます。

（注） **crashinfo test** コマンドを使用した結果としてフラッシュメモリに書き込まれたクラッシュ情報は、このコマンドの出力に表示できません。実際のクラッシュ ファイルのみが crashinfo_YYYYMMDD_HHMMSS 5_UTC の形式で表示されます。

例

次に、現在のクラッシュ情報コンフィギュレーションを表示する例を示します。

```
ciscoasa# show crashinfo save
crashinfo save enable
```

次に、クラッシュ ファイル テストの出力例を示します（このテストによって、ASA が実際にクラッシュすることはありません。このテストで提供されるのは、シミュレートされたサンプル ファイルです）。

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
F-flags  : 0x2
F-flags2 : 0x0
F-flags3 : 0x10000
F-flags4 : 0x0
F-bytes  : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
```

```
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
```

```
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
```

```
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008
Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X
Compiled on Fri 15-Nov-04 14:35 by root
hostname up 10 days 0 hours
Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
```

```
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
This XXX has a Restricted (R) license.
Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004
------------------ show clock ------------------
15:34:28.129 UTC Sun Nov 24 2004
------------------ show memory ------------------
Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes
------------------ show conn count ------------------
0 in use, 0 most used
------------------ show xlate count ------------------
0 in use, 0 most used
------------------ show vpn-sessiondb summary ------------------
Active Session Summary
Sessions:
                          Active : Cumulative : Peak Concurrent : Inactive
  SSL VPN               :       2 :          2 :               2
    Clientless only     :       0 :          0 :               0
    With client         :       2 :          2 :               2 :        0
  Email Proxy           :       0 :          0 :               0
  IPsec LAN-to-LAN      :       1 :          1 :               1
  IPsec Remote Access   :       0 :          0 :               0
  VPN Load Balancing    :       0 :          0 :               0
  Totals                :       3 :          3
License Information:
  Shared VPN License Information:
    SSL VPN                    :     1500
      Allocated to this device :       50
      Allocated in network     :       50
      Device limit             :      750
  IPsec   :    750    Configured :    750    Active :      1    Load :   0%
  SSL VPN :     52    Configured :     52    Active :      2    Load :   4%
                          Active : Cumulative : Peak Concurrent
  IPsec               :         1 :          1 :               1
  SSL VPN             :         2 :         10 :               2
    AnyConnect Mobile :         0 :          0 :               0
    Linksys Phone     :         0 :          0 :               0
  Totals              :         3 :         11
Tunnels:
                    Active : Cumulative : Peak Concurrent
  IKE         :          1 :          1 :               1
  IPsec       :          1 :          1 :               1
  Clientless  :          2 :          2 :               2
  SSL-Tunnel  :          2 :          2 :               2
  DTLS-Tunnel :          2 :          2 :               2
  Totals      :          8 :          8
```

```
------------------ show blocks ------------------
  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927
------------------ show interface ------------------
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
------------------ show cpu usage ------------------
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
------------------ show process ------------------
PC  SP       STATE    Runtime  SBASE Stack              Process   TID
Hsi 001e3329 00763e7c 0053e5c8 0     00762ef4 3784/4096 arp_timer 0x000000000000000a
Lsi 001e80e9 00807074 0053e5c8 0     008060fc 3792/4096 FragDBGC  0x000000000000006b
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPsec
```

```
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA
------------------ show failover ------------------
No license for Failover
------------------ show traffic ------------------
outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
------------------ show perfmon ------------------
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
```

```
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	すべてのクラッシュ情報ファイル、クラッシュ ファイルの内容を削除します。
crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo files	最後の 5 つのクラッシュ情報ファイルを日付とタイムスタンプに基づいて表示します。

show crashinfo console

crashinfo console コマンドのコンフィギュレーション設定を表示するには、show crashinfo console コマンドを入力します。

show crashinfo console

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

FIPS 140-2 に準拠していることにより、キーやパスワードなどのクリティカル セキュリティ パラメータをクリプト境界（シャーシ）の外側に配布することが禁止されています。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域には、機密データが含まれていることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。

コマンド	説明
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。

show crashinfo files

最新のシステム生成のクラッシュファイルを ASA に表示するには、特権 EXEC モードで **show crashinfo files** コマンドを使用します。出力には、フラッシュ メモリに書き込まれた最大 5 つのクラッシュ ファイルが日付とタイムスタンプに基づいて表示されます。クラッシュ ファイルがない場合、コマンド出力に情報は表示されません。

show crashinfo files

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

crashinfo test コマンドを使用した結果としてフラッシュメモリに書き込まれたクラッシュ情報は、**showcrashinfofiles** の出力に表示できません。実際のクラッシュ ファイルのみが crashinfo_YYYYMMDD_HHMMSS 5_UTC の形式で表示されます。クラッシュデータがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュデータをクリアしていた場合は、**show crashinfo files** コマンドを実行するとエラーメッセージが表示されます。

例

次に、実際のクラッシュ情報ファイルを表示する例を示します。

```
ciscoasa# show crashinfo files
crashinfo_20160725_012315_UTC
crashinfo_20160725_021353_UTC
crashinfo_20160725_022309_UTC
crashinfo_20160725_024205_UTC
```

関連コマンド

コマンド	説明
clear crashinfo	すべてのクラッシュ ファイルの内容を削除します。
crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
show crashinfo	最新のクラッシュ ファイルの内容を表示します。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。

show crypto accelerator load-balance

ハードウェア暗号化アクセラレータ MIB からのアクセラレータ固有のロードバランシング情報を表示するには、**show crypto accelerator load-balance** コマンドを使用します。

show crypto accelerator load-balance［ **ipsec | ssl | detail** ［ **ipsec | ssl** ］］

構文の説明

detail	（任意）詳細情報を表示します。このオプションの後に、ipsec または ssl キーワードを含めることができます。
ipsec	（任意）暗号化アクセラレータ IPSec ロードバランシングの詳細を表示します。
ssl	（任意）暗号化アクセラレータ SSL ロードバランシングの詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

show crypto accelerator statistics

ハードウェア クリプト アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権EXECモードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

出力統計情報は、次のように定義されます。

Accelerator 0 はソフトウェア ベースの暗号エンジンの統計情報を示します。

Accelerator 1 はハードウェア ベースの暗号エンジンの統計情報を示します。

RSA 統計情報には、デフォルトでソフトウェアで実行される、2048 ビット キーの RSA 処理が表示されます。つまり、2048 ビット キーがある場合、IKE/SSL VPN は、IPsec/SSL ネゴシエーション フェーズ中にソフトウェアで RSA 処理を実行します。実際の IPsec/SSL トラフィックは、引き続きハードウェアを使用して処理されます。これにより、同時に開始された同時セッションが数多くある場合、CPUの高使用となります。このため、RSA キー処理が複数発生し、CPU の高使用となる可能性があります。このようにして CPU の高使用状態となった場合は、1024 ビット キーを使用して、ハードウェアで RSA キー処理を実行する必要があります。このためには、アイデンティティ証明書を再度登録する必要があります。リリース 8.3(2) 以降では、5510 から 5550 のプラットフォームで crypto engine large-mod-accel コマンドを使用して、ハードウェアでこれらの処理を実行することもできます。

2048 ビットの RSA キーを使用しており、ソフトウェアで RSA 処理が実行されている場合は、CPU プロファイリングを使用して、CPU の高使用状況の原因となっている関数を特定できます。通常、bn_* 関数と BN_* 関数は RSA に使用される大規模なデータ セットでの数学的処理であり、ソフトウェアでの RSA 処理中に CPU の使用状況を確認する場合に最も役立ちます。次に例を示します。

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 統計情報には、ソフトウェアで 1024 より大きいモジュラス サイズの暗号処理が実行されたことが表示されます（DH5（Diffie-Hellman グループ 5 が 1536 を使用しています）など）。この場合、2048 ビット キー証明書はソフトウェアで処理されます。このため、数多くのセッションが実行されるときに CPU の高使用状況となります。

（注） ASA 5505（Cavium CN505 プロセッサ搭載）のみが、ハードウェアにより高速化される 768 ビットおよび 1024 ビットのキー生成の Diffie-Hellman グループ 1 および 2 をサポートしています。Diffie-Hellman グループ 5（1536 ビットのキー生成）は、ソフトウェアで実行されます。

適応型セキュリティ アプライアンスでは 1 つの暗号エンジンが IPsec 処理および SSL 処理を実行します。起動時にハードウェア クリプト アクセラレータにロードされたクリプト（Cavium）マイクロコードのバージョンを表示するには、**show version** コマンドを入力します。次に例を示します。

```
ciscoasa(config) show version
Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is “disk0:/interim/asa804-8-k8.bin”
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 統計情報には、2 つのフェーズでのキー生成が表示されます。最初のフェーズは、アルゴリズム パラメータの選択です。このパラメータは、システムの他のユーザーと共有することがあります。2 番めのフェーズは、1 人のユーザー用の秘密キーと公開キーの算出です。

SSL 統計情報には、ハードウェア クリプト アクセラレータへの SSL トランザクションで使用される、プロセッサ集約的な公開キーの暗号化アルゴリズムに関するレコードが表示されます。

RNG 統計情報には、キーとして使用する同じ乱数のセットを自動的に生成できる送信元とレシーバに関するレコードが表示されます。

例

次に、グローバル コンフィギュレーション モードでグローバルなクリプト アクセラレータ統計情報を表示する例を示します。

```
ciscoasa # show crypto accelerator statistics
Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
```

```
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
```

次の表に、各出力エントリの説明を示します。

出力	説明
Capacity	このセクションは、ASA がサポートできるクリプトアクセラレーションに関連しています。
Supports hardware crypto	（True/False）ASA はハードウェア クリプト アクセラレーションをサポートできます。

出力	説明
Supports modular hardware crypto	（True/False）サポートされている任意のハードウェア クリプト アクセラレータを個別のプラグイン カードまたはモジュールとして挿入できます。
Max accelerators	ASA でサポートされるハードウェア クリプト アクセラレータの最大数。
Mac crypto throughput	ASA の最大定格 VPN スループット。
Max crypto connections	ASA のサポート対象 VPN トンネルの最大数。
グローバル統計（Global Statistics）	このセクションは、ASA の複合ハードウェア クリプト アクセラレータに関連しています。
Number of active accelerators	アクティブなハードウェア アクセラレータの数。アクティブなハードウェア アクセラレータが初期化されており、crypto コマンドの処理に使用可能です。
Number of non-operational accelerators	非アクティブなハードウェア アクセラレータの数。非アクティブなハードウェア アクセラレータが検出されました。初期化が完了していないか、障害が発生して使用できなくなっています。
Input packets	すべてのハードウェア クリプト アクセラレータで処理される着信パケットの数。
Input bytes	処理される着信パケット内のデータのバイト数。
Output packets	すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output error packets	エラーが検出された、すべてのハードウェア暗号アクセラレータで処理される発信パケットの数。
Output bytes	処理される発信パケット内のデータのバイト数。
Accelerator 0	各セクションは、クリプト アクセラレータに関連しています。最初のセクション（Accelerator 0）は、常に、ソフトウェア クリプト エンジンです。ハードウェアアクセラレータではありませんが、ASA はこのソフトウェア クリプト エンジンを使用して、特定のクリプトタスクを実行します。ここには、その統計情報が表示されます。Accelerators 1 以上は、常に、ハードウェア クリプト アクセラレータです。
Status（ステータス）	アクセラレータのステータス。アクセラレータが初期化されているか、アクティブか、あるいは失敗したかを示します。

出力	説明
Software crypto engine	アクセラレータのタイプとファームウェア バージョン（該当する場合）。
スロット	アクセラレータのスロット番号（該当する場合）。
Active time	アクセラレータがアクティブ状態であった時間の長さ。
Total crypto transforms	アクセラレータによって実行された crypto コマンドの合計数。
Total dropped packets	エラーのためアクセラレータによってドロップされたパケットの合計数。
Input statistics	このセクションは、アクセラレータで処理された入力トラフィックに関連しています。入力トラフィックは、複合か認証、またはその両方を行う必要がある暗号文と見なされます。
Input packets	アクセラレータによって処理された入力パケットの数。
Input bytes	アクセラレータによって処理された入力バイト数。
Input hashed packets	アクセラレータがハッシュを実行したパケットの数。
Input hashed bytes	アクセラレータがハッシュを実行したバイト数。
Decrypted packets	アクセラレータが対称復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが対称復号化を実行したバイト数。
Output statistics	このセクションは、アクセラレータで処理された出力トラフィックに関連しています。入力トラフィックは、暗号化かハッシュ、またはその両方を実行する必要があるクリアテキストと見なされます。
Output packets	アクセラレータによって処理された出力パケットの数。
Output bad packets	エラーが検出された、アクセラレータで処理された出力パケットの数。
Output bytes	アクセラレータによって処理された出力バイト数。
Output hashed packets	アクセラレータが出力ハッシュを実行したパケットの数。
Output hashed bytes	アクセラレータが出力ハッシュを実行したバイト数。
Encyrpted packets	アクセラレータが対称暗号化を実行したパケットの数。
Encyrpted bytes	アクセラレータが対称暗号化を実行したバイト数。

出力	説明
Diffie-Hellman statistics	このセクションは、Diffie-Hellmanのキー交換処理に関連しています。
Keys generated	アクセラレータによって生成されたDiffie-Hellmanキー セットの数。
Secret keys derived	アクセラレータによって生成されたDiffie-Hellman共有秘密の数。
RSA statistics	このセクションは、RSA暗号処理に関連しています。
Keys generated	アクセラレータによって生成されたRSAキー セットの数。
Signatures	アクセラレータによって実行されたRSAシグニチャ処理の数。
Verifications	アクセラレータによって実行されたRSAシグニチャ確認の数。
Encrypted packets	アクセラレータがRSA暗号化を実行したパケットの数。
Decrypted packets	アクセラレータがRSA復号化を実行したパケットの数。
Decrypted bytes	アクセラレータがRSA復号化を実行したデータのバイト数。
DSA statistics	このセクションは、DSA処理に関連しています。DSAはバージョン8.2以上ではサポートされないため、この統計情報は表示されません。
Keys generated	アクセラレータによって生成されたDSAキー セットの数。
Signatures	アクセラレータによって実行されたDSAシグニチャ処理の数。
Verifications	アクセラレータによって実行されたDSAシグニチャ確認の数。
SSL statistics	このセクションは、SSLレコード処理に関連しています。
Outbound records	アクセラレータによって暗号化され、認証されたSSLレコードの数。
Inbound records	アクセラレータによって復号化され、認証されたSSLレコードの数。
RNG statistics	このセクションは、乱数生成に関連しています。
Random number requests	アクセラレータに対する乱数の要求の数。
Random number request failures	アクセラレータに対する乱数要求のうち、失敗した要求の数。

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合は、ASA にインストールされているすべての証明書が表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show crypto ca certificates** コマンドの出力例を示します。

```
ciscoasa(config)# show crypto ca certificates tp1
CA Certificate
Status: Available
Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
Certificate Usage: Signature
Issuer:
CN = ms-root-sha-06-2004
OU = rootou
O = cisco
L = franklin
ST - massachusetts
C = US
EA = a@b.con
Subject:
```

```
CN = ms-root-sha-06-2004
OU = rootou
O = cisco
L = franklin
ST = massachusetts
C = US
EA = example.com
CRL Distribution Point
ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
Validity Date:
start date: 14:11:40 UTC Jun 26 2004
end date: 14:01:30 UTC Jun 4 2022
Associated Trustpoints: tp2 tp1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント コンフィギュレーション モードを開始します。

show crypto ca crl

キャッシュされているすべてのCRL、または指定したトラストポイントでキャッシュされているすべてのCRLを表示するには、グローバルコンフィギュレーションモードまたは特権EXECモードで **show crypto ca crl** コマンドを使用します。

show crypto ca crl [**trustpool | trustpoint** <*trustpointname*>]

構文の説明

trustpoint *trustpointname*	（任意）トラストポイントの名前。名前を指定しない場合は、ASAにキャッシュされているすべてのCRLが表示されます。
trustpool	trustpoolの名前。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、 **show crypto ca crl** コマンドの出力例を示します。

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント コンフィギュレーション モードを開始します。

show crypto ca server

ASA でローカル CA コンフィギュレーションのステータスを表示するには、CA サーバー コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server** コマンドを使用します。

show crypto ca server

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、**show crypto ca server** コマンドの出力例を示します。

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
    CRL not present.
```

```
    Current primary storage dir: nvram:
ciscoasa#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
debug crypto ca server	ローカル CA サーバーを設定するときに、デバッグ メッセージを表示します。
show crypto ca server certificate	ローカル CA の証明書を Base-64 形式で表示します。
show crypto ca server crl	ローカル CA CRL のライフタイムを表示します。

show crypto ca server cert-db

ローカル CA サーバー証明書の全部またはサブセット（特定のユーザーに発行されたものも含む）を表示するには、CA サーバー コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server cert-db** コマンドを使用します。

show crypto ca server cert-db [**username** *username* **| allowed | enrolled | expired | on-hold**] [**serial** *certificate-serial-number*]

構文の説明

allowed	証明書のステータスに関係なく、登録を許可されたユーザーを表示するように指定します。
enrolled	有効な証明書を持つユーザーを表示するように指定します。
expired	期限切れの証明書を保持しているユーザーを表示するように指定します。
on-hold	まだ登録されていないユーザーを表示するように指定します。
serial certificate-serial-number	表示する特定の証明書のシリアル番号を指定します。シリアル番号は 16 進形式である必要があります。
username username	証明書の所有者を指定します。username は、ユーザー名または電子メール アドレスです。電子メール アドレスの場合、エンド ユーザーに連絡を取りワンタイム パスワード（OTP）を配布するために使用される電子メールアドレスになります。エンドユーザーの電子メール通知をイネーブルにするには、電子メール アドレスが必要です。

コマンド デフォルト

デフォルトでは、ユーザー名も証明書シリアル番号も指定されていない場合、発行された証明書のデータベース全体が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca server cert-db コマンドは、ローカル CA サーバーによって発行されたユーザー証明書のリストを表示します。1つ以上の任意の証明書タイプキーワードを付けて、または任意の証明書シリアル番号を付けて、特定のユーザー名を指定することで、証明書データベースのサブセットを表示できます。

キーワードまたはシリアル番号なしでユーザー名を指定すると、そのユーザーに対して発行された証明書がすべて表示されます。ユーザーごとに、出力には、ユーザー名、電子メールアドレス、ドメイン名、登録が許可される期間、およびユーザーに登録招待が通知された回数が表示されます。

また、出力には次の情報も表示されます。

- NOTIFIED フィールドは、複数のリマインダをサポートするために必要です。これにより、登録およびリマインダ通知を試行するためにユーザーに OTP の通知を行う必要があるタイミングが追跡されます。このフィールドは、最初は 0 に設定されています。ユーザー入力に登録許可のマークが付くと、このフィールドは増分して1になります。この時点で、最初の OTP 通知が生成されます。
- NOTIFYフィールドは、リマインダが送信されるたびに増分します。OTPが期限切れになるまでに3つの通知が送信されます。ユーザーが登録を許可されたとき、有効期間の中間点、および有効期間の 3/4 を経過した時点で通知が送信されます。このフィールドは、管理者が開始した登録でのみ使用されます。自動証明書更新の場合、証明書データベース内の NOTIFY フィールドが使用されます。

（注） 有効期限前に証明書の更新がユーザーに通知される回数を追跡する場合にはこのコマンドの通知カウンタが使用され、証明書の登録がユーザーに通知される回数を追跡する場合には show crypto ca server user-db の通知カウンタが使用されます。更新通知は、cert-db で追跡され、user-db には含まれません。

それぞれの証明書には、証明書のシリアル番号、発行日付と有効期限日付、および証明書のステータス（Revoked/Not Revoked）が表示されます。

例

次に、CA サーバーが ASA に対して発行した証明書をすべて表示するよう要求する例を示します。

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

次に、ローカル CA サーバーによって発行された、シリアル番号が 0x2 の証明書をすべて表示するよう要求する例を示します。

ciscoasa# **show crypto ca server cert-db serial 2**

```
Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

次に、ローカル CA サーバーによって発行された証明書をすべて表示するよう要求する例を示します。

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
crypto ca server revoke	ローカルCAサーバーが発行した証明書を、証明書データベースとCRLの両方で失効としてマークします。
lifetime crl	CRL のライフタイムを指定します。

show crypto ca server certificate

ローカルCAサーバーの証明書をBase-64形式で表示するには、CAサーバーコンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権EXECモードで**show crypto ca server certificate** コマンドを使用します。

show crypto ca server certificate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca server certificate コマンドにより、ローカル CA サーバーの証明書が Base-64 形式で表示されます。この表示画面では、ローカルCAサーバーを信頼する必要がある他のデバイスに証明書をエクスポートするときに、その証明書をカット アンド ペーストできます。

例

次に、**show crypto ca server certificate** コマンドの出力例を示します。

```
ciscoasa# show crypto ca server certificate
The base64 encoded local CA certificate follows:
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+
MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAM
IIXHAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQ
Ijph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphs
```

```
UM+IG3SDOiDwZG9n1SvtMieoxd7Hxknxbum06JDruj
WKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzw
cRhl1KEZTS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeL
j3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwP
EdPQxaWZPrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3
Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d
5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI0b2AfCr6Pbw
fC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA
5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3qAXy1
GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj....
```

ciscoasa#

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザー証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA コンフィギュレーションを ASCII テキスト形式で表示します。

show crypto ca server crl

ローカル CA の現在の CRL を表示するには、CA サーバー コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server crl** コマンドを使用します。

show crypto ca server crl

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、**show crypto ca server crl** コマンドの出力例を示します。

```
ciscoasa
# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
```

```
ciscoasa
#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める CRL 分散ポイント（CDP）を指定します。
crypto ca server	CA サーバー コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
crypto ca server revoke	ローカルCAサーバーが発行した証明書を、証明書データベースとCRLで失効としてマークします。
lifetime crl	CRL のライフタイムを指定します。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

show crypto ca server user-db

ローカル CA サーバーのユーザーデータベースに含まれているユーザーを表示するには、CA サーバー コンフィギュレーション モード、グローバル コンフィギュレーション モード、または特権 EXEC モードで **show crypto ca server user-db** コマンドを使用します。

show crypto ca server user-db［ **expired | allowed | on-hold | enrolled** ］

構文の説明

allowed	（任意）証明書のステータスに関係なく、登録を許可されたユーザーを表示するように指定します。
enrolled	（任意）有効な証明書を持つユーザーを表示するように指定します。
expired	（任意）期限切れの証明書を保持しているユーザーを表示するように指定します。
on-hold	（任意）まだ登録されていないユーザーを表示するように指定します。

コマンド デフォルト

デフォルトでは、キーワードが入力されない場合にはデータベース内のすべてのユーザーが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、現在登録されているユーザーを表示する例を示します。

```
ciscoasa# show
            crypto ca server user-db enrolled
Username   DN     Certificate issued      Certificate expiration
exampleuser  cn=Example User,o=...     5/31/2009       5/31/2010
ciscoasa#
```

使用上のガイドライン

証明書の登録がユーザーに通知される回数を追跡する場合にはこのコマンドの通知カウンタが使用され、有効期限前に証明書の更新がユーザーに通知される回数を追跡する場合には show crypto ca server cert-db の通知カウンタが使用されます。更新通知は、cert-db で追跡され、user-db には含まれません。

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバーのユーザー データベースにユーザーを追加します。
crypto ca server user-db allow	CA サーバー データベース内の特定のユーザーまたはユーザーのサブセットに、ローカルCAへの登録を許可します。
crypto ca server user-db remove	CA サーバーのユーザー データベースからユーザーを削除します。
crypto ca server user-db write	ローカル CA データベースで設定されているユーザー情報をストレージに書き込みます。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

show crypto ca trustpool

trustpool を構成する証明書を表示するには、特権 EXEC モードで **show crypto ca trustpool** コマンドを使用します。

show crypto ca trustpool［ **detail** ］

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、すべての trustpool を省略形式で表示します。「detail」オプションを指定した場合は、追加の情報が含まれます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show crypto ca trustpool コマンドの出力には、各証明書のフィンガープリントの値が含まれます。これらの値は削除操作で必要です。

例

```
ciscoasa# show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
```

```
CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

関連コマンド

コマンド	説明
clear crypto ca trustpool	trustpool からすべての証明書を削除します。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
crypto ca trustpool remove	指定された 1 つの証明書を trustpool から削除します。

show crypto ca trustpool policy

設定済みのtrustpoolポリシーを表示し、適用された証明書マップを処理してそれらがポリシーに与える影響を表示するには、特権EXECモードで**show crypto ca trustpool policy**コマンドを使用します。

show crypto ca trustpool policy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(2)	trustpool 証明書の自動インポートのステータスと結果を表示する機能が追加されました。

例

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#
ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
auto-import url http://www.thawte.com
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
crl enforcenextupdate
auto-import
auto-import url http://www.thawte.com
auto-import time 22:00:00
ciscoasa(config)#
```

```
ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
 Last import result: SUCCESS
 Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpool policy	トラストプール ポリシーを定義するコマンドを提供するサブモードを開始します。

show crypto debug-condition

IPsec および ISAKMP のデバッグメッセージに対して現在設定されているフィルタ、一致しない状態、およびエラー状態を表示するには、グローバル コンフィギュレーション モードで **show crypto debug-condition** コマンドを使用します。

show crypto debug-condition

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、フィルタリング条件を表示する例を示します。

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON
IKE peer IP address filters:
1.1.1.0/24   2.2.2.2
IKE user name filters:
my_user
```

関連コマンド

コマンド	説明
debug crypto condition	IPsec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。

コマンド	説明
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPsec および ISAKMP のデバッグ メッセージを表示します。

show crypto ikev1 sa

IKEv1 ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev1 sa** コマンドを使用します。

show crypto ikev1 sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto ikev1 sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show crypto ikev2 sa	IKEv2 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブなISAKMPコンフィギュレーションをすべて表示します。

show crypto ikev2 sa

IKEv2 ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev2 sa** コマンドを使用します。

show crypto ikev2 sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.19(1)	IKEv2 サードパーティクライアントのデュアルスタックサポートが追加されました。子 SA が格納できるトラフィックセレクタの数が 2 に拡張されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE Peer	タイプ	Dir	Rky	状態
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE Peer	タイプ	Dir	Rky	状態	Encrypt	Hash	認証	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id                Local                Remote     Status         Role
671069399        10.0.0.0/500 10.255.255.255/500      READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify:
PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
      Mobile is enabled
      Assigned host addr: 192.168.0.12
      Assigned host addr IPv6: 2001:db8::2
      IKEv2 Fragmentation Configured MTU:576 bytes, Overhead: 28 bytes, Effective MTU:
548 bytes
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                          ::/0- ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:/65535
          remote selector 192.186.0.12/0 - 192.186.0.12/65535
                          2001:db8::2/0- 2001:db8::2/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

関連コマンド

コマンド	説明
show crypto ikev1 sa	IKEv1 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブなISAKMP コンフィギュレーションをすべて表示します。

show crypto ikev2 stats

IKEv2 の実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ikev2 stats** コマンドを使用します。

show crypto ikev2 stats

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.9(1)	ローカル IKEv2 の統計情報が提供されるようになりました。

使用上のガイドライン

このコマンドのローカルの出力は次のとおりです。

```
Global IKEv2 Statistics
  Active Tunnels:                          0
  Previous Tunnels:                        0
  In Octets:                               0
  In Packets:                              0
  In Drop Packets:                         0
  In Drop Fragments:                       0
  In Notifys:                              0
  In P2 Exchange:                          0
  In P2 Exchange Invalids:                 0
  In P2 Exchange Rejects:                  0
  In IPSEC Delete:                         0
  In IKE Delete:                           0
  Out Octets:                              0
```

```
  Out Packets:                              0
  Out Drop Packets:                         0
  Out Drop Fragments:                       0
  Out Notifys:                              0
  Out P2 Exchange:                          0
  Out P2 Exchange Invalids:                 0
  Out P2 Exchange Rejects:                  0
  Out IPSEC Delete:                         0
  Out IKE Delete:                           0
  SAs Locally Initiated:                    0
  SAs Locally Initiated Failed:             0
  SAs Remotely Initiated:                   0
  SAs Remotely Initiated Failed:            0
  System Capacity Failures:                 0
  Authentication Failures:                  0
  Decrypt Failures:                         0
  Hash Failures:                            0
  Invalid SPI:                              0
  In Configs:                               0
  Out Configs:                              0
  In Configs Rejects:                       0
  Out Configs Rejects:                      0
  Previous Tunnels:                         0
  Previous Tunnels Wraps:                   0
  In DPD Messages:                          0
  Out DPD Messages:                         0
  Out NAT Keepalives:                       0
  IKE Rekey Locally Initiated:              0
  IKE Rekey Remotely Initiated:             0
  Locally Initiated IKE Rekey Rejected:     0
  Remotely Initiated IKE Rekey Rejected:    0
  CHILD Rekey Locally Initiated:            0
  CHILD Rekey Remotely Initiated:           0

IKEV2 Call Admission Statistics
  Max Active SAs:                     No Limit
  Max In-Negotiation SAs:                15000
  Cookie Challenge Threshold:            Never
  Active SAs:                                0
  In-Negotiation SAs:                        0
  Incoming Requests:                         0
 Incoming Requests Accepted:                 0
  Incoming Requests Rejected:                0
  Outgoing Requests:                         0
  Outgoing Requests Accepted:                0
  Outgoing Requests Rejected:                0
  Rejected Requests:                         0
  Rejected Over Max SA limit:                0
  Rejected Low Resources:                    0
  Rejected Reboot In Progress:               0
  Cookie Challenges:                         0
  Cookie Challenges Passed:                  0
  Cookie Challenges Failed:                  0
```

関連コマンド

コマンド	説明
show crypto ikev2 sa	IKEv1 ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブなISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。同じ意味を持つ **show ipsec df-bit** コマンドも使用できます。

show crypto ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

d f ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
ciscoasa(config)# show
 crypto
 ipsec df-bit inside
```

```
df-bit inside copy
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの IPsec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。同じ意味を持つ **show ipsec fragmentation** コマンドも使用できます。

show crypto ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPNに対するパケットを暗号化する際、システムはパケット長をアウトバウンドインターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、グローバル コンフィギュレーション モードで、inside という名前のインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec policy

OSPFv3 に設定されている IPsec セキュアソケット API（SS API）セキュリティポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec policy** コマンドを使用します。このコマンドの代替形式である **show ipsec policy** を使用することもできます。

show crypto ipsec policy

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
ciscoasa# show crypto ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

コマンド	説明
ipv6 ospf encryption	OSPFv3 の認証と暗号方式ポリシーを設定します。
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3インターフェイスに関する情報を表示します。

show crypto ipsec sa

IPsec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec sa** コマンドを使用します。このコマンドの代替形式である **show ipsec sa** を使用することもできます。

show crypto ipsec sa [**entry | identity | map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

detail	（任意）表示されているものに対する詳細なエラー情報を表示します。
entry	（オプション）IPsec SA をピア アドレスの順に表示します。
identity	（オプション）IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	（オプション）指定されたクリプト マップの IPsec SA を表示します。
peer *peer-addr*	（オプション）指定されたピア IP アドレスの IPsec SA を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3、マルチ コンテキスト モード、トランスフォームと IV サイズ部分における Suite B アルゴリズム、および ESPV3 IPsec 出力に対するサポートが追加されました。

リリース	変更内容
9.13(1)	*show crypto ipsec sa detail* で発生するエラーのトラブルシューティング用として、次の新しいカウンタが追加されました。 • **#pkts invalid ip version (send)** • **#pkts invalid length (send)** • **#pkts invalid ctx (send) and #pkts invalid ctx (rcv)** • **#pkts invalid ifc (send) and #pkts invalid ifc (rcv)** • **#pkts failed (send) and #pkts failed (rcv)**
9.19(1)	IKEv2サードパーティクライアントのデュアルスタックサポートが追加されました。インバウンドおよびアウトバウンドの IPsec SA がサポートできるトラフィックセレクタの数が 2 に拡張されました。

例

次に、グローバル コンフィギュレーション モードで、OSPFv3 として識別されるトンネルを含む IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
```

```
        IV size: 8 bytes
        replay detection support: Y
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

（注） IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

```
The following example, entered in global configuration mode, shows IPsec SAs for the
keyword detail with the newly added counters to troubleshoot the errors in the traffic.
(config)# sh ipsec sa det
interface: outside
    Crypto map tag: outside_map, seq num: 10, local addr: 10.86.94.103
      access-list toASA-5525 extended permit ip host 10.86.94.103 host 10.86.95.135
      local ident (addr/mask/prot/port): (10.86.94.103/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (10.86.95.135/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.86.95.135
      dynamic allocated peer ip: 10.86.95.135
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0
      #pkts invalid pad (rcv): 0
      #pkts invalid ip version (send): 0, #pkts invalid ip version (rcv): 0
      #pkts invalid len (send): 0, #pkts invalid len (rcv): 0
      #pkts invalid ctx (send): 0, #pkts invalid ctx (rcv): 0
      #pkts invalid ifc (send): 0, #pkts invalid ifc (rcv): 0
      #pkts failed (send): 0, #pkts failed (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 10.86.94.103/500, remote crypto endpt.: 10.86.95.135/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 25356578
      current inbound spi : A1029CE2
    inbound esp sas:
      spi: 0xA1029CE2 (2701303010)
         SA State: active
         transform: esp-aes esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 195272704, crypto-map: outside_map
```

```
        sa timing: remaining key lifetime (kB/sec): (3962879/28782)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x25356578 (624256376)
        SA State: active
        transform: esp-aes esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, }
        slot: 0, conn_id: 195272704, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (4193279/28772)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
        0x00000000 0x00000001
```

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
```

```
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry** に対する IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
```

```
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry detail** を使用して IPsec SA を表示する例を示します。

```
ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
```

```
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 322
          IV size: 8 bytes
          replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 322
          IV size: 8 bytes
          replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 104
          IV size: 8 bytes
          replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 104
          IV size: 8 bytes
          replay detection support: Y
ciscoasa(config)#
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
```

```
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8:1
```

```
#pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
#pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0
local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35
```

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

IPSec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
ciscoasa(config)# show crypto ipsec stats
IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
```

```
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。
show ipsec sa summary	IPsec SA の要約を表示します。

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
```

```
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa ［ **detail** ］

構文の説明

detail	SA データベースに関する詳細出力を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	この **show isakmp sa** コマンドは廃止されました。**show crypto isakmp sa** コマンドは、それに置き換わるものです。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

Detail not specified

IKE Peer：209.165.200.225

Type：L2L または User

Dir：Init

Rky：No または Yes。Yes の場合は、キー再生成が発生しており、キー再生成が完了するまで、2 番目に一致する SA は異なる状態になります。

Role：Initiator または Responder State。SA のステート マシンの現在の状態を示します。

State：トンネルがアップしデータが受け渡しされている場合、値は MM_ACTIVE または AM_ACTIVE のいずれかになります。その他のアクティブ状態は、MM_BLD_MSG4、MM_BLD_MSG6、MM_FREE、MM_SND_MSG6_H、MM_START、MM_TM_INIT_MODECFG_H、MM_TM_PEND_QM、MM_WAIT_DELETE、MM_WAIT_MSG3、MM_WAIT_MSG5 などです。

Detail specified

IKE Peer：209.165.200.225

Type：L2L または User

Dir：Init

Rky：No または Yes。Yes の場合は、キー再生成が発生しており、キー再生成が完了するまで、2 番目に一致する SA は異なる状態になります。

Role：Initiator または Responder State。SA のステート マシンの現在の状態を示します。トンネルがアップしデータが受け渡しされている場合、値は MM_ACTIVE または AM_ACTIVE のいずれかになります。

State：MM_ACTIVE または AM_ACTIVE 以外。その他のアクティブ状態は、MM_BLD_MSG4、MM_BLD_MSG6、MM_FREE、MM_SND_MSG6_H、MM_START、MM_TM_INIT_MODECFG_H、MM_TM_PEND_QM、MM_WAIT_DELETE、MM_WAIT_MSG3、MM_WAIT_MSG5 などです。

Encrypt：3des

Hash：md5

Auth：preshrd

Lifetime：86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
ciscoasa(config)# show crypto isakmp sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。

コマンド	説明
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが廃止されました。**show crypto isakmp stats** コマンドは、それに置き換わるものです。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids

- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

次の例をグローバルコンフィギュレーションモードで入力すると、ISAKMP統計情報が表示されます。

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
```

```
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto key mypubkey

デフォルトのキー（「mypubkey」と呼ばれる）とそのキーに関する情報を表示するには、特権 EXEC モードで **show crypto key mypubkey** コマンドを使用します。

show crypto key mypubkey ｛ **ecdsa** ｜ **eddsa** ｜ **rsa** ｝

構文の説明

ecdsa	キータイプとしてECDSAを指定します。
eddsa	キータイプとしてEDDSAを指定します。
rsa	キータイプとして RSA を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ECDSA キーのサポートが追加されました。
9.16(1)	EDDSA キーのサポートが追加されました。

関連コマンド

コマンド	説明
cryto key generate	キーペアを作成します。
crypto key zeroize	キー ペアを削除します。

show crypto protocol statistics

クリプトアクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

構文の説明

protocol 統計情報を表示するプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。

ikev1：インターネット キー エクスチェンジ バージョン 1。

ipsec：IP セキュリティフェーズ 2 プロトコル。

ssl：セキュアソケットレイヤ。

other：新規プロトコル用に予約済み。

all：現在サポートされているすべてのプロトコル。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードで、指定したプロトコルに関するクリプト アクセラレータ統計情報を表示する例を示します。

```
ciscoasa
 #
```

```
show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3

SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0

Failed requests: 0
ciscoasa
 #
show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics ssl

[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics all
```

```
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91

 SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0

Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700

Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0

HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
```

```
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。

show crypto sockets

暗号セキュアソケット情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto sockets** コマンドを使用します。

show crypto sockets

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードで、暗号セキュア ソケット情報を表示する例を示します。

```
ciscoasa(config)# show crypto sockets
Number of Crypto Socket connections 1
       Gi0/1  Peers: (local): 2001:1::1
                      (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)
       Crypto Sockets in Listen state:
```

次の表で、**show crypto sockets** コマンド出力のフィールドについて説明します。

フィールド	説明
Number of Crypto Socket connections	システム内の暗号ソケットの数。
Socket State	この状態は、アクティブなIPsecセキュリティアソシエーション（SA）が存在することを意味するOpenか、またはアクティブなIPsec SAが存在しないことを意味するClosedのどちらかです。
クライアント	アプリケーションの名前とその状態。
Flags	このフィールドが「shared」になっている場合、ソケットは複数のトンネル インターフェイスで共有されます。
Crypto Sockets in Listen state	暗号IPsecプロファイルの名前。

関連コマンド

コマンド	説明
show crypto ipsec policy	暗号セキュア ソケットAPIでインストールされたポリシー情報を表示します。

show csc node-count

CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

show csc node-count [**yesterday**]

構文の説明

yesterday （任意）CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示します。

コマンド デフォルト

デフォルトで表示されるノード カウントは、午前 0 時からスキャンされたノード数です。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ノードとは、固有の送信元 IP アドレス、または ASA により保護されているネットワーク上のデバイスのアドレスです。ASA は、毎日のノードカウントを追跡し、ユーザーライセンスの強制のために CSC SSM に伝えます。

例

次に、CSC SSM が午前 0 時以降にスキャンしたノードの数を表示する **show csc node-count** コマンドの出力例を示します。

```
ciscoasa# show csc node-count
Current node count is 1
```

次に、CSC SSM が過去 24 時間（午前 0 時から翌日の午前 0 時まで）にスキャンしたトラフィックのノード数を表示する **show csc node-count** コマンドの出力例を示します。

```
ciscoasa(config)# show csc node-count yesterday
Yesterday's node count is 2
```

関連コマンド

csc	CSC SSM での設定に従って、FTP、HTTP、POP3、および SMTP をスキャンするためにネットワークトラフィックを CSC SSM に送信します。
show running-config class-map	現在のクラスマップ コンフィギュレーションを表示します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス ポリシー コンフィギュレーションを表示します。

show ctiqbe

ASA を越えて確立された CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show ctiqbe コマンドは ASA を越えて確立された CTIQBE セッションの情報を表示します**debug ctiqbe** や **show local-host** とともに、このコマンドは、CTIQBE インスペクションエンジンの問題のトラブルシューティングに使用されます。

（注） **show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次に、次の条件における **show ctiqbe** コマンドの出力例を示します。ASA を越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
ciscoasa# | show ctiqbe
Total: 1
       LOCAL           FOREIGN         STATE   HEARTBEAT
```

```
------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ----------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ----------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ----------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。RTCP 受信ポートは UDP 1029 に PAT 変換されています。

RTP/RTCP: PAT xlates: で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。ASA は 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show ctl-file

電話プロキシで使用されるCTLファイルの内容を表示するには、グローバル コンフィギュレーション モードで **show ctl-file** コマンドを使用します。

show ctl-file *filename* [**parsed**]

構文の説明

filename	データベースに格納されているセキュア モードに対応した電話を表示します。
parsed	（任意）指定した CTL ファイルの詳細情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	コマンドが追加されました。

使用上のガイドライン

フラッシュメモリに格納されている CTL ファイルのファイル名を指定する場合は、ディスク番号、ファイル名、および拡張を disk0:/testctl.tlv のように指定します。**show ctl-file** コマンドを使用すると、電話プロキシインスタンスの設定時のデバッグに役立ちます。

例

次に、**show ctl-file** コマンドを使用して、CTL ファイルの一般情報を表示する例を示します。

```
ciscoasa# show ctl-file
disk0:/ctlfile.tlv

Total Number of Records: 1
CTL Record Number 1
  Subject Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
     cucm
```

```
  IP Address:
     192.168.52.102
  Associated Trustpoint:
     cucm_primary
```

The following example shows the use of the **show ctl-file** command to show detailed information about the CTL file:

```
ciscoasa# show ctl-file
disk0:/ctlfile.tlv
 parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
    521debcf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267ce1a7 202b2c8b 2ac980d3
    9608f64d e7cd82df e205e5bf 74a1d9c4 fae20f90 f3d2746a e90f439e ef93fca7
    d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eecb ce37e4d1
    866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

 ### CTL RECORD No. 1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
    30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
    af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
    50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
    f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
    040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
    308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
    0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
    4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
    375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
    58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
    b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
    7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
    c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
    15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
    0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
    a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
    9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
    ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
    ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

関連コマンド

コマンド	説明
ctl-file (global)	電話プロキシを作成するためのCTLインスタンスを指定するか、またはフラッシュ メモリに格納されている CTL ファイルを解析します。
ctl-file (phone-proxy)	電話プロキシの設定時に使用する CTL インスタンスを指定します。
phone proxy	Phone Proxy インスタンスを設定します。

show ctl-provider

ユニファイド コミュニケーションで使用される CTL プロバイダーの設定を表示するには、特権 EXEC モードで **show ctl-provider** コマンドを使用します。

show ctl-provider [*name*]

構文の説明

name	（オプション）この CTL プロバイダーのみの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、CTL プロバイダーの設定を表示する例を示します。

```
ciscoasa# show ctl-provider

!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダーを設定します。

show cts environment-data

ASA に Cisco TrustSec の環境データのリフレッシュ処理のヘルス状態とステータスを表示するには、特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts environment-data** コマンドの出力例を示します。

```
ciscoasa# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 1200 secs
Last update time:          18:12:07 EST Feb 27 2012
```

```
Env-data expires in:       0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in:     0:00:02:24 (dd:hr:mm:sec)
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションのSXP接続を表示します。
show cts pac	PAC のコンポーネントを表示します。

show cts environment-data sg-table

ASA に Cisco TrustSec の常駐セキュリティ グループ テーブルを表示するには、特権 EXEC モードで **show cts environment-data sg-table** コマンドを使用します。

show cts environment-data sg-table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts environment-data sg-table** コマンドの出力例を示します。

```
ciscoasa# show cts environment-data sg-table
Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries
SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
```

```
ExampleSG1                        2     unicast
ExampleSG13                      14     unicast
ExampleSG14                      15     unicast
ExampleSG15                      16     unicast
ExampleSG16                      17     unicast
ExampleSG17                      18     unicast
ExampleSG18                      19     unicast
Unknown                           0     unicast
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションのSXP接続を表示します。
show cts pac	PAC のコンポーネントを表示します。

show cts pac

ASA に Cisco TrustSec の Protected Access Credential（PAC）のコンポーネントを表示するには、特権 EXEC モードで **show cts pac** コマンドを使用します。

show cts pac

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show cts pac コマンドは、PAC 情報（有効期間など）を表示します。PAC のライフタイムが経過すると ASA がセキュリティ グループ テーブルの更新を取得できなくなるため、有効期間は重要です。管理者は、Identity Services Engine のセキュリティ グループ テーブルとの同期を保つために、古い PAC の期限が切れる前に新しい PAC を要求する必要があります。

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。スタンバイ状態のデバイスでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
ERROR: This command is only permitted on the active device.
```

このコマンドは、クラスタリング コンフィギュレーションのマスター ユニットでのみサポートされます。スレーブ ユニットでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
This command is only permitted on the master device.
```

例

次に、**show cts pac** コマンドの出力例を示します。

```
ciscoasa# show cts pac
```

```
PAC-Info:
    Valid until: Jul 28 2012 08:03:23
    AID:         6499578bc0240a3d8bd6591127ab270c
    I-ID:        BrianASA36
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
    00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
    7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
    8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
    00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
    09100e1758
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sgt-map

制御パスのIPアドレスセキュリティグループテーブルマネージャエントリを表示するには、特権 EXEC モードで **show cts sgt-map** コマンドを使用します。

show cts sgt-map [**sgt** *sgt*] [**address** *ip4* [/ *mask*] | **address** *ipv6* [/ *prefix*] **| ipv4 | ipv6**] [**name**] [**brief | detail**]

構文の説明

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
brief	IP アドレス セキュリティ グループ テーブル マッピングの要約を表示します。
detail	IPアドレスセキュリティグループテーブルマッピングを表示します。
ipv4	IPv4 アドレス セキュリティ グループ テーブル マッピングを表示します。デフォルトで、IPv4アドレスセキュリティグループテーブルマップのみが表示されます。
ipv6	IPv6 アドレス セキュリティ グループ テーブル マッピングを表示します。
name	セキュリティ グループ名が一致する IP アドレス セキュリティ グループ テーブル マッピングを表示します。
sgt *sgt*	セキュリティ グループ テーブルが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。
9.3(1)	「CLI-HI」ソースからの IP-SGT バインディング情報が含まれるように出力が更新されました。これは、 **cts role-based sgt-map** コマンドにより移入されます。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

このコマンドは、制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。

例

次に、 **show cts sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
1.1.1.1       7 CLI-HI
10.10.10.1    7 CLI-HI
10.10.10.10   3 LOCAL
10.10.100.1   7 CLI-HI
198.26.208.31 7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

次に、いくつかのネットワークバインドを指定した **show cts sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map

Active IP-SGT Bindings Information
IP Address       SGT Source
============================================
10.1.1.1          7   CLI-HI
10.252.10.0/24   7   CLI-HI
10.252.10.10     3   LOCAL
10.252.100.1     7   CLI-HI
172.26.0.0/16    7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

次に、 **show cts sgt-map ipv6** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information
IP Address                              SGT     Source
```

```
=========================================================
3330::1                                 17      SXP
FE80::A8BB:CCFF:FE00:110                17      SXP
IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

次に、 **show cts sgt-map ipv6 detail** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information
IP Address                Security Group                                Source
=============================================================================
3330::1                    2345                                          SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP
IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

次に、 **show cts sgt-map ipv6 brief** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information
IP-SGT Active Bindings Summary
==================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

次に、 **show cts sgt-map address** コマンドの出力例を示します。

```
ciscoasa# show cts sgt-map address 10.10.10.5
Active IP-SGT Bindings Information
IP Address              SGT     Source
=========================================================
10.10.10.5              1234    SXP
IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sxp connections

ASA に Security eXchange Protocol（SXP）接続を表示するには、特権 EXEC モードで **show cts sxp connections** コマンドを使用します。

show cts sxp connections [**peer** *peer addr*] [**local** *local addr*] [**ipv4 | ipv6**] [**status** { **on | off | delete-hold-down | pending-on** }] [**mode** { **speaker | listener** }] [**brief**]

構文の説明

brief	（オプション）SXP 接続の要約を表示します。
delete-hold-down	（オプション）TCP 接続は ON 状態であったときに終了しました（TCP がダウンしています）。この状態になる可能性があるのは、リスナーモードで設定された ASA のみです。
ipv4	（オプション）IPv4 アドレスとの SXP 接続を表示します。
ipv6	（オプション）IPv6 アドレスとの SXP 接続を表示します。
listener	（オプション）リスナーモードで設定された ASA を表示します。
local *local addr*	（オプション）一致したローカル IP アドレスとの SXP 接続を表示します。
mode	（オプション）一致したモードとの SXP 接続を表示します。
off	（オプション）TCP 接続は開始されていません。ASA は、この状態のときのみ TCP 接続を再試行します。
on	（オプション）SXP OPEN または SXP OPEN RESP メッセージを受信しました。SXP 接続が正常に確立されました。ASA は、この状態のときのみ SXP メッセージを交換します。
peer *peer addr*	（オプション）一致したピア IP アドレスとの SXP 接続を表示します。
pending-on	（オプション）SXP OPEN メッセージがピアに送信されました。ピアからの応答を待機しています。
speaker	（オプション）スピーカーモードで設定された ASA を表示します。
status	（オプション）一致したステータスとの SXP 接続を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。

使用上のガイドライン

次の条件に該当する場合、SXP 状態が変わります。

- ピアが SXP の設定を解除したり、SXP をディセーブルにしたために、SXP リスナーがその SXP 接続をドロップした場合、SXP リスナーは OFF 状態に移行します。
- ピアがクラッシュしたり、インターフェイスがシャットダウンしたために、SXP リスナーがその SXP 接続をドロップした場合、SXP リスナーは DELETE_HOLD_DOWN 状態に移行します。
- 最初の 2 つの条件のいずれかが発生すると、SXP スピーカーは OFF 状態に移行します。

このコマンドは、フェールオーバー モードのアクティブなデバイスとマスター ユニット クラスタのみでサポートされます。

例

次に、 **show cts sxp connections** コマンドの出力例を示します。

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Delete hold down period : 120 secs
Reconcile period   : 120 secs
Retry open period : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
----------------------------------------------
Peer IP            : 2.2.2.1
Local IP           : 2.2.2.2
Conn status        : On
Local mode         : Listener
Ins number         : 1
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer    : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 3.3.3.1
Local IP           : 3.3.3.2
```

```
Conn status       : On
Local mode        : Listener
Ins number        : 2
TCP conn password : None
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
---------------------------------------------
Peer IP           : 4.4.4.1
Local IP          : 4.4.4.2
Conn status       : On
Local mode        : Speaker
Ins number        : 1
TCP conn password : Set
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show cts sxp sgt-map

ASA に、Cisco TrustSec の Security eXchange Protocol（SXP）モジュール内の現在の IP アドレス セキュリティ グループ テーブル マッピング データベース エントリを表示するには、特権 EXEC モードで **show cts sxp sgt-map** コマンドを使用します。

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *sgt*] [**address** *ipv4* [/ *mask*] | **address** *ipv6* [/ *prefix*] **| ipv4 | ipv6**] [**name**] [**brief | detail**] [**status**]

構文の説明

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	特定の IPv4 または IPv6 アドレスの IP アドレス セキュリティ グループ テーブルマッピングのみを表示します。ネットワークのマッピングを表示するには IPv4 サブネット マスクまたは IPv6 プレフィックスを含めます。
brief	IP アドレス セキュリティ グループ テーブル マッピングの要約を表示します。
detail	セキュリティ グループテーブル情報を表示します。セキュリティ グループの名前が使用できない場合、セキュリティ グループ テーブル値のみが角カッコなしで表示されます。
ipv4	IPv4 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングを表示します。デフォルトで、IPv4 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングのみが表示されます。
ipv6	IPv6 アドレスとの IP アドレス セキュリティ グループ テーブル マッピングを表示します。
name	セキュリティ グループ名が一致する IP アドレス セキュリティ グループ テーブル マッピングを表示します。
peer *peer addr*	ピア IP アドレスが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。
sgt *sgt*	セキュリティ グループ テーブルが一致する IP アドレス セキュリティ グループ テーブル マッピングのみを表示します。
status	アクティブまたは非アクティブなマッピング済みエントリを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	コマンドが追加されました。
9.6(1)	ネットワーク マッピングを表示する機能が追加されました。

使用上のガイドライン

このコマンドは、SXP から統合されたアクティブな IP アドレス セキュリティ グループ テーブルのマッピング済みエントリを表示します。

このコマンドは、フェールオーバー コンフィギュレーションのスタンバイ状態のデバイスではサポートされません。クラスタでは、マスター ユニットでコマンドを入力します。

例

次に、 **show cts sxp sgt-map** コマンドの出力例を示します。

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3
SGT        : 7
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
SGT        : 7
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
SGT        : 7
IPv6       : FE80::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
```

次に、 **show cts sxp sgt-map detail** コマンドの出力例を示します。

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3
SGT        : STBU(7)
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
SGT        : STBU(7)
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
Status     : Inactive
SGT        : 6
IPv6       : 1234::A8BB:CCFF:FE00:110
```

```
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
```

次に、 **show cts sxp sgt-map brief** コマンドの出力例を示します。一部のマッピングはネットワークに繋がります。

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.0/24
SGT, IPv4: 7, 3.3.3.3
SGT, IPv6: 7, FE80::0/64
```

関連コマンド

コマンド	説明
show running-config cts	実行コンフィギュレーションの SXP 接続を表示します。
show cts environment	環境データのリフレッシュ処理のヘルス状態とステータスを表示します。

show curpriv

現在のユーザー特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応
特権 EXEC	• 対応	• 対応	—	—	• 対応
ユーザー EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように変更されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次に、enable_15 という名前のユーザーが異なる特権レベルにある場合の **show curpriv** コマンドの出力例を示します。ユーザー名は、ユーザーがログインしたときに入力した名前を示しています。P_PRIV は、ユーザーが **enable** コマンドを入力したことを示しています。P_CONF は、ユーザーが **config terminal** コマンドを入力したことを示します。

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
```

```
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

次に、既知の動作の例を示します。イネーブルモードからディセーブルモードに移行した場合、最初にログインしたユーザー名が enable_1 に置き換わります。

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit
Logoff
Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show running-config privilege	コマンドの特権レベルを表示します。

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。