CHAPTER 16

コンフィギュレーション ファイルの操作

この章では、コンフィギュレーション ファイルを表示、コピー、および消去するコマンドの使用方法について説明します。次のような構成になっています。

現在の設定の表示

現在の設定の内容を表示するには、**show configuration** または **more current-config** コマンドを使用します。

現在の設定の内容を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　現在の設定を表示します。

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2009
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
```

```
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

現在のサブモード設定の表示

サブモードの現在の設定を表示するには、サブモードで **show settings** コマンドを使用します。

サブモードの現在の設定を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　サービス分析エンジン サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -----------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   -----------------------------------------------
      <protected entry>
      name: vs0 <defaulted>
      -----------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         physical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
         logical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana)# exit
sensor(config)# exit
sensor#
```

ステップ 3　サービス異常検出サブモードの現在の設定を表示します。

```
sensor(config)# service anomaly-detection ad0
sensor(config-ano)# show settings
   worm-timeout: 600 seconds <defaulted>
   learning-accept-mode
   -----------------------------------------------
      auto
      -----------------------------------------------
         action: rotate <defaulted>
         schedule
         -----------------------------------------------
            periodic-schedule
            -----------------------------------------------
               start-time: 10:00:00 <defaulted>
               interval: 24 hours <defaulted>
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   internal-zone
   -----------------------------------------------
      enabled: true <defaulted>
```

```
ip-address-range: 0.0.0.0 <defaulted>
tcp
------------------------------------------------
   dst-port (min: 0, max: 65535, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   default-thresholds
   ------------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      ------------------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
         dest-ip-bin: high <defaulted>
         num-source-ips: 1 <defaulted>
      ------------------------------------------------
   ------------------------------------------------
   enabled: true <defaulted>
------------------------------------------------
udp
------------------------------------------------
   dst-port (min: 0, max: 65535, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   default-thresholds
   ------------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      ------------------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
         dest-ip-bin: high <defaulted>
         num-source-ips: 1 <defaulted>
      ------------------------------------------------
   ------------------------------------------------
   enabled: true <defaulted>
------------------------------------------------
other
------------------------------------------------
   protocol-number (min: 0, max: 255, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   default-thresholds
   ------------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      ------------------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
```

```
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      enabled: true <defaulted>
   ----------------------------------------------
----------------------------------------------
illegal-zone
----------------------------------------------
   enabled: true <defaulted>
   ip-address-range: 0.0.0.0 <defaulted>
   tcp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      default-thresholds
      ----------------------------------------------
         scanner-threshold: 100 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         ----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      enabled: true <defaulted>
   ----------------------------------------------
   udp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      default-thresholds
      ----------------------------------------------
         scanner-threshold: 100 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         ----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      enabled: true <defaulted>
   ----------------------------------------------
   other
   ----------------------------------------------
      protocol-number (min: 0, max: 255, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      default-thresholds
      ----------------------------------------------
```

```
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ---------------------------------------------
   ------------------------------------------------
   external-zone
   ------------------------------------------------
      enabled: true <defaulted>
      tcp
      ------------------------------------------------
         dst-port (min: 0, max: 65535, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
      udp
      ------------------------------------------------
         dst-port (min: 0, max: 65535, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
```

```
            enabled: true <defaulted>
         ----------------------------------------------
         other
         ----------------------------------------------
            protocol-number (min: 0, max: 255, current: 0)
            ----------------------------------------------
            ----------------------------------------------
            default-thresholds
            ----------------------------------------------
               scanner-threshold: 100 <defaulted>
               threshold-histogram (min: 0, max: 3, current: 3)
               ----------------------------------------------
                  <protected entry>
                  dest-ip-bin: low <defaulted>
                  num-source-ips: 10 <defaulted>
                  <protected entry>
                  dest-ip-bin: medium <defaulted>
                  num-source-ips: 1 <defaulted>
                  <protected entry>
                  dest-ip-bin: high <defaulted>
                  num-source-ips: 1 <defaulted>
               ----------------------------------------------
            ----------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      ignore
      ----------------------------------------------
         enabled: true <defaulted>
         source-ip-address-range: 0.0.0.0 <defaulted>
         dest-ip-address-range: 0.0.0.0 <defaulted>
      ----------------------------------------------
sensor(config-ano)# exit
sensor(config)# exit
sensor# exit
```

ステップ 4　サービス認証サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service authentication
sensor(config-aut)# show settings
   attemptLimit: 0 <defaulted>
sensor(config-aut)# exit
sensor(config)# exit
sensor#
```

ステップ 5　サービス イベント アクション規則サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# show settings
   variables (min: 0, max: 256, current: 0)
   ----------------------------------------------
   ----------------------------------------------
   overrides (min: 0, max: 12, current: 0)
   ----------------------------------------------
   ----------------------------------------------
   filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
   ----------------------------------------------
   general
   ----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
```

```
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 30 <defaulted>
      max-denied-attackers: 10000 <defaulted>
   ------------------------------------------------
   target-value (min: 0, max: 5, current: 0)
   ------------------------------------------------
   ------------------------------------------------
sensor(config-rul)# exit
sensor(config)# exit
sensor# exit
```

ステップ 6　外部製品インターフェイス サブモードの現在の設定を表示します。

```
sensor(config)# service external-product-interface
sensor(config-ext)# show settings
   cisco-security-agents-mc-settings (min: 0, max: 2, current: 0)
   ------------------------------------------------
   ------------------------------------------------
sensor(config-ext)# exit
sensor(config)# exit
sensor#
```

ステップ 7　サービス グローバル相関サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service global-correlation
sensor(config-glo)# show settings
   network-participation: off <defaulted>
   global-correlation-inspection: on <defaulted>
   global-correlation-inspection-influence: standard <defaulted>
   reputation-filtering: on <defaulted>
   test-global-correlation: off <defaulted>
sensor(config-glo)# exit
sensor(config)# exit
sensor# exit
```

ステップ 8　サービス ヘルスモニタ サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service health-monitor
sensor(config-hea)# show settings
   enable-monitoring: true <defaulted>
   persist-security-status: 5 minutes <defaulted>
   heartbeat-events
   ------------------------------------------------
      enable: 300 seconds <defaulted>
   ------------------------------------------------
   application-failure-policy
   ------------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   ------------------------------------------------
   bypass-policy
   ------------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   ------------------------------------------------
   interface-down-policy
   ------------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   ------------------------------------------------
   inspection-load-policy
   ------------------------------------------------
```

```
      enable: true <defaulted>
      yellow-threshold: 80 percent <defaulted>
      red-threshold: 91 percent <defaulted>
   ---------------------------------------------
   missed-packet-policy
   ---------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 1 percent <defaulted>
      red-threshold: 6 percent <defaulted>
   ---------------------------------------------
   memory-usage-policy
   ---------------------------------------------
      enable: false <defaulted>
      yellow-threshold: 80 percent <defaulted>
      red-threshold: 91 percent <defaulted>
   ---------------------------------------------
   signature-update-policy
   ---------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 30 days <defaulted>
      red-threshold: 60 days <defaulted>
   ---------------------------------------------
   license-expiration-policy
   ---------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 30 days <defaulted>
      red-threshold: 0 days <defaulted>
   ---------------------------------------------
   event-retrieval-policy
   ---------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 300 seconds <defaulted>
      red-threshold: 600 seconds <defaulted>
   ---------------------------------------------
   global-correlation-policy
   ---------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 86400 seconds <protected>
      red-threshold: 259200 seconds <protected>
   ---------------------------------------------
   network-participation-policy
   ---------------------------------------------
      enable: false <defaulted>
      yellow-threshold: 1 connection failures <protected>
      red-threshold: 6 connection failures <protected>
   ---------------------------------------------
sensor(config-hea)# exit
sensor(config)# exit
sensor# exit
```

ステップ 9　サービス ホスト サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings
   network-settings
   ---------------------------------------------
      host-ip: 10.89.149.27/25,10.89.149.126 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      ---------------------------------------------
         network-address: 10.0.0.0/8
         ---------------------------------------------
```

```
        network-address: 64.0.0.0/8
        ------------------------------------------------
     ------------------------------------------------
     ftp-timeout: 300 seconds <defaulted>
     login-banner-text: <defaulted>
  ------------------------------------------------
  time-zone-settings
  ------------------------------------------------
     offset: 0 minutes default: 0
     standard-time-zone-name: UTC default: UTC
  ------------------------------------------------
  ntp-option
  ------------------------------------------------
     disabled
     ------------------------------------------------
     ------------------------------------------------
  ------------------------------------------------
  summertime-option
  ------------------------------------------------
     disabled
     ------------------------------------------------
     ------------------------------------------------
  ------------------------------------------------
  auto-upgrade-option
  ------------------------------------------------
     disabled
     ------------------------------------------------
     ------------------------------------------------
  ------------------------------------------------
  crypto
  ------------------------------------------------
     key (min: 0, max: 10, current: 2)
     ------------------------------------------------
        <protected entry>
        name: realm-cisco.pub <defaulted>
        type
        ------------------------------------------------
           rsa-pubkey
           ------------------------------------------------
              length: 2048 <defaulted>
              exponent: 65537 <defaulted>
              modulus: 24442189989357747083874855335232628843599968934198559648
630199473878411519325039111726689401947545491553904076580203933306118912925083008594030403118601449963256881242806805808958161419633739962306062499005704910305590153955935086060008679776808073640186063435723252375575293126304558068704301863805621144374392890694566709220749958273902847616105915157520084051402436730831897782246996493459836701038938988829749080288411854373007629358970353591216199331947093130298688830012547215572646349623539468838641064915313947806852904082351955132172731380999653830397161301532707152200465671078281289241976924173320339117043 <defaulted>
           ------------------------------------------------
        ------------------------------------------------
        <protected entry>
        name: realm-trend.pub <defaulted>
        type
        ------------------------------------------------
           rsa-pubkey
           ------------------------------------------------
              length: 2048 <defaulted>
              exponent: 65537 <defaulted>
              modulus: 21765561422573021314159855351418723031625093380777053696638172895270605709325510654898181907137456721482605270300606672083666066038026793043906672414339062649547930055010161817958463728705293646569214657261265137596920354521585644221602944203520804404212975401970895119903756769601133853673296766
```

```
4528979577797349198405658704521451482006336695073134640004430849159462643470699947608668822814014830063399534204647069509052443439525363706527255224510771122235801811504605447832514984814327059910100698443685257548784136694276397529508017679990530923523245629558008672420329791409598422432844439158222313842379910083819191 <defaulted>
            ----------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
sensor(config-hos)# exit
sensor(config)# exit
sensor#
```

ステップ 10　サービス インターフェイス サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 4)
   ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: GigabitEthernet2/0 <defaulted>
```

```
      ------------------------------------------------
         media-type: xl <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet2/1 <defaulted>
      ------------------------------------------------
         media-type: xl <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   command-control: GigabitEthernet0/1 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   ------------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   ------------------------------------------------
sensor(config-int)# exit
sensor(config)# exit
sensor#
```

ステップ 11　サービス ロガー サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# show settings
   master-control
   ------------------------------------------------
      enable-debug: false <defaulted>
```

```
    individual-zone-control: false <defaulted>
  -----------------------------------------------
  zone-control (min: 0, max: 999999999, current: 14)
  -----------------------------------------------
    <protected entry>
    zone-name: Cid
    severity: debug <defaulted>
    <protected entry>
    zone-name: AuthenticationApp
    severity: warning <defaulted>
    <protected entry>
    zone-name: Cli
    severity: warning <defaulted>
    <protected entry>
    zone-name: csi
    severity: warning <defaulted>
    <protected entry>
    zone-name: ctlTransSource
    severity: warning <defaulted>
    <protected entry>
    zone-name: IdapiCtlTrans
    severity: warning <defaulted>
    <protected entry>
    zone-name: IdsEventStore
    severity: warning <defaulted>
    <protected entry>
    zone-name: MpInstaller
    severity: warning <defaulted>
    <protected entry>
    zone-name: nac
    severity: warning <defaulted>
    <protected entry>
    zone-name: sensorApp
    severity: warning <defaulted>
    <protected entry>
    zone-name: tls
    severity: warning <defaulted>
    <protected entry>
    zone-name: intfc
    severity: warning <defaulted>
    <protected entry>
    zone-name: cmgr
    severity: warning <defaulted>
    <protected entry>
    zone-name: cplane
    severity: warning <defaulted>
  -----------------------------------------------
sensor(config-log)# exit
sensor(config)# exit
sensor#
```

ステップ 12　サービス ネットワーク アクセス サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings
  general
  -----------------------------------------------
    log-all-block-events-and-errors: true <defaulted>
    enable-nvram-write: false <defaulted>
    enable-acl-logging: false <defaulted>
    allow-sensor-block: false <defaulted>
    block-enable: true <defaulted>
    block-max-entries: 250 <defaulted>
```

```
        max-interfaces: 250 <defaulted>
        rate-limit-max-entries: 250 <defaulted>
        master-blocking-sensors (min: 0, max: 100, current: 0)
        ---------------------------------------------
        ---------------------------------------------
        never-block-hosts (min: 0, max: 250, current: 0)
        ---------------------------------------------
        ---------------------------------------------
        never-block-networks (min: 0, max: 250, current: 0)
        ---------------------------------------------
        ---------------------------------------------
        block-hosts (min: 0, max: 250, current: 0)
        ---------------------------------------------
        ---------------------------------------------
        block-networks (min: 0, max: 250, current: 0)
        ---------------------------------------------
        ---------------------------------------------
    ---------------------------------------------
    user-profiles (min: 0, max: 250, current: 1)
    ---------------------------------------------
        profile-name: test
        ---------------------------------------------
            enable-password: <hidden>
            password: <hidden>
            username: <defaulted>
        ---------------------------------------------
    ---------------------------------------------
    cat6k-devices (min: 0, max: 250, current: 0)
    ---------------------------------------------
    ---------------------------------------------
    router-devices (min: 0, max: 250, current: 0)
    ---------------------------------------------
    ---------------------------------------------
    firewall-devices (min: 0, max: 250, current: 0)
    ---------------------------------------------
    ---------------------------------------------
sensor(config-net)# exit
sensor(config)# exit
sensor#
```

ステップ 13　通知サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)# show settings
    trap-destinations (min: 0, max: 10, current: 0)
    ---------------------------------------------
    ---------------------------------------------
    error-filter: error|fatal <defaulted>
    enable-detail-traps: false <defaulted>
    enable-notifications: false <defaulted>
    enable-set-get: false <defaulted>
    snmp-agent-port: 161 <defaulted>
    snmp-agent-protocol: udp <defaulted>
    read-only-community: public <defaulted>
    read-write-community: private <defaulted>
    trap-community-name: public <defaulted>
    system-location: Unknown <defaulted>
    system-contact: Unknown <defaulted>
sensor(config-not)# exit
sensor(config)# exit
sensor#
```

ステップ 14　シグニチャ定義サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings
   variables (min: 0, max: 256, current: 1)
   -----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
      -----------------------------------------------
         web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,2432
6-24326 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   application-policy
   -----------------------------------------------
      http-policy
      -----------------------------------------------
         http-enable: false <defaulted>
         max-outstanding-http-requests-per-connection: 10 <defaulted>
         aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
      -----------------------------------------------
      ftp-enable: false <defaulted>
   -----------------------------------------------
   fragment-reassembly
   -----------------------------------------------
      ip-reassemble-mode: nt <defaulted>
   -----------------------------------------------
   stream-reassembly
   -----------------------------------------------
--MORE--
```

ステップ 15　SSH 既知ホスト サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service ssh-known-hosts
sensor(config-ssh)# show settings
   rsa1-keys (min: 0, max: 500, current: 0)
   -----------------------------------------------
   -----------------------------------------------
sensor(config-ssh)# exit
sensor(config)# exit
sensor#
```

ステップ 16　信頼済み証明書サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service trusted-certificate
sensor(config-tru)# show settings
   trusted-certificates (min: 0, max: 500, current: 1)
   -----------------------------------------------
      common-name: 10.89.130.108
      certificate: MIICJDCCAY0CCPbSkgXUchJIMA0GCSqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTA
lVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlTU00tSVBTMjAxFjAUBgNVB
AMTDTEwLjg5LjEzMC4xMDgwHhcNMDMwMTAzMDE1MjEwWhcNMDUwMTAzMDE1MjEwWjBXMQswCQYDVQQGE
wJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAGA1UECxMJU1NNLUlQUzIwMRYwFAYDV
QQDEw0xMC44OS4xMzAuMTA4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzldqLFG4MT4bfgh3mJ
fP/DCilnnaLfzHK9FdnhmWI4FY+9MVvAI7MOhAcuV6HYfyp6n6cYvH+Eswzl9uv7H5nouID9St9GI3Yr
SUtlIQAJ4QVL2DwWP230x6KdHrYqcj+Nmhc7AnnPypjidwGSfF+VetIJLEeRFh/mI2JcmwF2QIDAQABM
A0GCSqGSIb3DQEBBQUAA4GBAAUI2PLANTOehxvCfwd6UAFXvy8uifbjqKMC1jrrF+f9KGkxmR+XZvUaG
OS83FYDXlXJvB5Xyxms+Y01wGjzKKpxegBoan8OB8o193Ueszdpvz2xYmiEgywCDyVJRsw3hAFMXWMS5
XsBUiHtw0btHH0j7ElFZxUjZv12fGz8hlnY
   -----------------------------------------------
sensor(config-tru)# exit
```

```
sensor(config)# exit
sensor#
```

ステップ 17　Web サーバ サブモードの現在の設定を表示します。

```
sensor# configure terminal
sensor(config)# service web-server
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)# exit
sensor(config)# exit
sensor#
```

現在の設定の出力のフィルタリング

more *keyword* | [**begin** | **exclude** | **include**] *regular-expression* コマンドを使用すると、more コマンドの出力を検索できます。

次のオプションが適用されます。

- *keyword* : current-config または backup-config のどちらか。
  - **current-config** : 現在実行中の設定。コマンドを入力すると、この設定が永続化されます。
  - **backup-config** : 設定バックアップ ファイルの保管場所。
- | : パイプ記号は、そのあとに出力処理の指定が続くことを示します。
- **begin** : **more** コマンドの出力から、指定された正規表現を含む行以降をフィルタリングなしで出力します。
- **exclude** : **more** コマンドの出力から、特定の正規表現を含む行を除外します。
- **include** : **more** コマンドの出力から、指定された正規表現を含む行だけを出力します。
- *regular-expression* : **more** コマンドの出力から検索する任意の正規表現。

（注）　*regular-expression* オプションには大文字と小文字の区別があり、複雑な検索要件に対応できます。

more コマンドをフィルタリングするには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、current-config の出力をフィルタリングして、正規表現「ip」が見つかった行以降を出力します。

```
sensor# more current-config | begin ip
generating current config:
host-ip 10.89.149.185/25,10.89.149.254
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
```

```
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
service logger
master-control
enable-debug true
exit
exit
! ------------------------------
service network-access
general
log-all-block-events-and-errors true
--MORE--
```

（注）　出力を中断して CLI プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

ステップ 3　current-config 出力から正規表現「ip」を除外します。

```
sensor# more current-config | exclude ip
generating current config:
! ------------------------------
! Version 7.0(1)
! Current configuration last modified Fri Feb 11 15:10:57 2009
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface FastEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
--MORE--
```

（注）　出力を中断して CLI プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

ステップ 4　current-config 出力に正規表現「ip」を含めます。

```
sensor# more current-config | include ip
generating current config:
host-ip 10.89.149.185/25,10.89.149.254
engine atomic-ip
```

現在のサブモード設定の出力のフィルタリング

サブモード設定の内容の出力を検索またはフィルタリングするには、対象のサブモードで **show settings | [begin | exclude | include]** *regular_expression* コマンドを使用します。

次のオプションが適用されます。

- **|** : パイプ記号は、そのあとに出力処理の指定が続くことを示します。
- **begin** : **show settings** コマンドの出力から、指定された正規表現を含む行以降をフィルタリングなしで出力します。
- **exclude** : **show settings** コマンドの出力から、特定の正規表現を含む行を除外します。
- **include** : **show settings** コマンドの出力から、指定された正規表現を含む行だけを出力します。
- *regular_expression* : **show settings** コマンドの出力から検索する任意の正規表現。

（注） *regular_expression* オプションには大文字と小文字の区別があり、複雑な検索要件に対応できます。

サブモード設定の内容の出力を検索またはフィルタリングするには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、イベント アクション規則設定の出力で正規表現「filters」を検索します。

```
sensor# configure terminal
sensor(config)# service event-action-rules
sensor(config-rul)# show settings | begin filters
filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
 ------------------------------------------------
 general
 ------------------------------------------------
    global-overrides-status: Enabled <defaulted>
    global-filters-status: Enabled <defaulted>
    global-summarization-status: Enabled <defaulted>
    global-metaevent-status: Enabled <defaulted>
    global-deny-timeout: 3600 <defaulted>
    global-block-timeout: 15 default: 30
    max-denied-attackers: 10000 <defaulted>
 ------------------------------------------------
 target-value (min: 0, max: 5, current: 0)
 ------------------------------------------------
 ------------------------------------------------
sensor(config-rul)#
```

ステップ 3　ネットワーク アクセス設定の出力をフィルタリングして、正規表現を除外します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings | exclude false
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true default: true
      block-enable: true default: true
      block-max-entries: 11 default: 250
```

```
      max-interfaces: 13 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 1)
      ---------------------------------------------
         ipaddress: 10.89.149.124
         ---------------------------------------------
            password: <hidden>
            port: 443 default: 443
            tls: true default: true
            username: cisco default:
         ---------------------------------------------
      ---------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ---------------------------------------------
         ip-address: 10.89.146.112
         ---------------------------------------------
      ---------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ---------------------------------------------
         ip-address: 88.88.88.0/24
--MORE--
```

ステップ 4　ホスト設定の出力をフィルタリングして、正規表現「ip」を出力に含めます。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings | include ip
      host-ip: 10.89.149.185/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
sensor(config-hos)#
```

論理ファイルの内容の表示

現在のシステム設定や保存されているバックアップ システム設定などの論理ファイルの内容を表示するには、**more** *keyword* コマンドを使用します。

次のオプションが適用されます。

- *keyword*：current-config または backup-config のどちらか。
  - **current-config**：現在実行中の設定。コマンドを入力すると、この設定が永続化されます。
  - **backup-config**：設定バックアップ ファイルの保管場所。

more current-config または **more backup-config** で「more」プロンプトを無効にするには、**terminal length 0** コマンドを使用してターミナル長をゼロに設定します。そうすると、**more** コマンドが途中で一時停止することなく、ファイルの内容がすべて表示されるようになります。

論理ファイルの内容を表示するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

（注）　オペレータおよびビューアは、現在の設定だけを表示できます。パスワードなどの隠しフィールドを表示できるのは、管理者だけです。

ステップ 2　現在のコンフィギュレーション ファイルの内容を表示します。

```
sensor# more current-config
Generating current config:
```

現在の設定が表示されます。

```
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2009
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
```

```
exit
sensor#
```

詳細情報

terminal コマンドの使用手順については、「ターミナル プロパティの変更」（P.17-16）を参照してください。

リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元

（注）　アップグレードする前に、現在のコンフィギュレーション ファイルをリモート サーバにコピーすることを推奨します。

コンフィギュレーション ファイルをリモート サーバにコピーするには、**copy** [**/erase**] *source_url destination_url keyword* コマンドを使用します。後で、そのリモート サーバから現在の設定を復元することができます。最初に、現在のコンフィギュレーション ファイルのバックアップを求めるプロンプトが表示されます。

オプション

次のオプションが適用されます。

- **/erase**：コピー前にコピー先ファイルを消去します。

  このキーワードは current-config だけに適用されます。backup-config の場合は必ず上書きされます。コピー先の current-config に対してこのキーワードを指定すると、コピー元の設定がシステムのデフォルト設定に適用されます。コピー先の current-config に対して指定しなかった場合、コピー元の設定はコピー先の current-config とマージされます。

- *source_url*：コピー元のファイルの場所。URL またはキーワードです。
- *destination_url*：コピー先ファイルの場所。URL またはキーワードです。
- **current-config**：現在実行中の設定。コマンドを入力すると、設定が永続化されます。
- **backup-config**：設定のバックアップの保管場所。

コピー元およびコピー先の URL の形式は、ファイルによって変わります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバのコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバのコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注） FTP または SCP プロトコルを使用する場合は、パスワードの入力を求めるプロンプトが表示されます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加する必要もあります。

- http: : Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。
  http:[[/[username@]location]/directory]/filename
- https: : Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。
  https:[[/[username@]location]/directory]/filename

（注） HTTP および HTTPS では、Web サイトへのアクセスにユーザ名が必要な場合、パスワードの入力を求めるプロンプトが表示されます。HTTPS プロトコルを使用する場合は、リモート ホストが TLS 信頼済みホストになっている必要があります。

注意 別のセンサーのコンフィギュレーション ファイルをコピーする場合、検知インターフェイスおよび仮想センサーが同じように設定されていないと、エラーが発生する可能性があります。

現在の設定のリモート サーバへのバックアップ

現在の設定をリモート サーバにバックアップするには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** と入力して、現在の設定をバックアップ設定にコピーします。

```
cfg            100% |***********************************************| 36124       00:00
```

現在の設定のバックアップ ファイルからの復元

現在の設定をバックアップ ファイルから復元するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** と入力して、現在の設定をバックアップ設定にコピーします。

```
cfg            100% |***********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
```

```
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

ステップ 4　**no** と入力すると、現在設定されているホスト名、IP アドレス、サブネット マスク、管理インターフェイス、およびアクセス リストが保持されます。これらの情報は保持することを推奨します。保持すれば、それ以外の設定を復元してもセンサーへのアクセスが維持されます。

詳細情報

- リモート ホストを SSH 既知ホスト リストに追加する手順については、「SSH の既知ホスト リストへのホストの追加」（P.4-49）を参照してください。
- リモート ホストを TLS 信頼済みホスト リストに追加する手順については、「TLS の信頼できるホストの追加」（P.4-54）を参照してください。

バックアップ コンフィギュレーション ファイルの作成と使用

設定を保護するために、現在の設定のバックアップを作成し、表示することによってそれが保存したい設定であることを確認できます。この設定を復元する必要があるときは、バックアップ コンフィギュレーション ファイルを現在の設定とマージするか、現在のコンフィギュレーション ファイルにバックアップ コンフィギュレーション ファイルを上書きします。

現在の設定をバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定を保存します。

```
sensor# copy current-config backup-config
```

現在の設定がバックアップ ファイルに保存されます。

ステップ 3　バックアップ コンフィギュレーション ファイルを表示します。

```
sensor# more backup-config
```

バックアップ コンフィギュレーション ファイルが表示されます。

ステップ 4　バックアップの設定を現在の設定とマージすることも、現在の設定を上書きすることもできます。

- バックアップの設定を現在の設定とマージします。

  ```
  sensor# copy backup-config current-config
  ```

- バックアップの設定で現在の設定を上書きします。

  ```
  sensor# copy /erase backup-config current-config
  ```

コンフィギュレーション ファイルの消去

論理ファイルを削除するには、**erase** {**backup-config** | **current-config**} コマンドを使用します。

次のオプションが適用されます。

- **current-config**：現在実行中の設定。コマンドを入力すると、設定が永続化されます。
- **backup-config**：設定のバックアップの保管場所。

現在の設定を消去してすべての設定をデフォルトに戻すには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset to
default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no username"
command.
Continue? []:
```

ステップ 2　続行する場合は Enter を押します。取り消す場合は **no** と入力します。