CHAPTER 16

コンフィギュレーション ファイルの操作

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、コンフィギュレーション ファイルの表示、コピー、および消去を実行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

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

現在の設定の内容を表示する手順は、次のとおりです。

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。

```
ips-ssp# show configuration
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
```

```
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
```

```
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
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
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
ips-ssp#
```

現在のサブモード コンフィギュレーションの表示

サブモードで **show settings** コマンドを使用して、そのサブモードの現在の設定を表示します。

サブモードの現在の設定を表示する手順は、次のとおりです。

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(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)
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ------------------------------------------------
ips-ssp(config-ana)# exit
ips-ssp(config)# exit
ips-ssp#
```

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。

```
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(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>
    -----------------------------------------------
ips-ssp(config-ano)# exit
ips-ssp(config)# exit
ips-ssp# 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。

```
ips-ssp# configure terminal
ips-ssp(config)# service authentication
ips-ssp(config-aut)# show settings
   attemptLimit: 0 <defaulted>
   password-strength
   -----------------------------------------------
      size: 8-64 <defaulted>
      digits-min: 0 <defaulted>
      uppercase-min: 0 <defaulted>
      lowercase-min: 0 <defaulted>
      other-min: 0 <defaulted>
      number-old-passwords: 0 <defaulted>
   -----------------------------------------------
ips-ssp(config-aut)#
```

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
ips-ssp(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)
   -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-rul)# exit
ips-ssp(config)# exit
ips-ssp# 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。

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

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service global-correlation
ips-ssp(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>
ips-ssp(config-glo)# exit
ips-ssp(config)# exit
ips-ssp# exit
```

ステップ 8　サービス ヘルスモニタリング サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service health-monitor
ips-ssp(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>
   ------------------------------------------------
ips-ssp(config-hea)# exit
ips-ssp(config)# exit
ips-ssp# 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。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp 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: 21765561422573021314159855351418723031625093380777053696638172895270605709325510654898181907137456721482605270300606672083666066038026793043906672414339062649547930055010161817958463728705293646569214657261265137596920354521585644221602944203520804404212975401970895119903756769601133853673296766452897957779734919840565870452145148201133669507313464000443084915946264347069994760866882281401483006339953420464706950905244343952536370652725522451077112223580181150460544783251498481432705991010069844368525754878413669427639752950801767999053092352324562955800867242032979140959842243284443915822231384237991008381919 <defaulted>
               ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
ips-ssp(config-hos)# exit
ips-ssp(config)# exit
ips-ssp#
```

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service interface
ips-ssp(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   -----------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: PortChannel0/0 <defaulted>
      -----------------------------------------------
         media-type: backplane <protected>
         description: <defaulted>
         admin-state: enabled <protected>
         duplex: full <protected>
         speed: 10000 <protected>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   command-control: Management0/0 <protected>
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   -----------------------------------------------
ips-ssp(config-int)#
```

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service logger
ips-ssp(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>
   ------------------------------------------------
ips-ssp(config-log)# exit
ips-ssp(config)# exit
ips-ssp#
```

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(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)
   ------------------------------------------------
   ------------------------------------------------
ips-ssp(config-net)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 13　通知サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(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>
ips-ssp(config-not)# exit
ips-ssp(config)# exit
ips-ssp#
```

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(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。

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

ステップ 16　信頼できる証明書サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service trusted-certificate
ips-ssp(config-tru)# show settings
   trusted-certificates (min: 0, max: 500, current: 1)
   -----------------------------------------------
      common-name: 192.0.2.3
      certificate: MIICJDCCAY0CCPbSkgXUchJIMA0GCSqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTA
lVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlTU00tSVBTMjAxFjAUBgNVB
AMTDTEwLjg5LjEzMC4xMDgwHhcNMDMwMTAzMDE1MjEwWhcNMDUwMTAzMDE1MjEwWjBXMQswCQYDVQQGE
wJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAGA1UECxMJU1NNLUlQUzIwMRYwFAYDV
QQDEw0xMC44OS4xMzAuMTA4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzldqLFG4MT4bfgh3mJ
fP/DCilnnaLfzHK9FdnhmWI4FY+9MVvAI7MOhAcuV6HYfyp6n6cYvH+Eswzl9uv7H5nouID9St9GI3Yr
SUtlIQAJ4QVL2DwWP230x6KdHrYqcj+Nmhc7AnnPypjidwGSfF+VetIJLEeRFh/mI2JcmwF2QIDAQABM
A0GCSqGSIb3DQEBBQUAA4GBAAUI2PLANTOehxvCfwd6UAFXvy8uifbjqKMC1jrrF+f9KGkxmR+XZvUaG
OS83FYDXlXJvB5Xyxms+Y01wGjzKKpxegBoan8OB8o193Ueszdpvz2xYmiEgywCDyVJRsw3hAFMXWMS5
XsBUiHtw0btHH0j7ElFZxUjZv12fGz8hlnY
      -----------------------------------------------
ips-ssp(config-tru)# exit
ips-ssp(config)# exit
ips-ssp#
```

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。

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

現在の設定の出力のフィルタ処理

more *keyword* | [**begin** | **exclude** | **include**] *regular-expression* コマンドを使用して、コマンドの出力をさらに検索します。

オプション

次のオプションが適用されます。

- *keyword* : current-config または backup-config を指定します。
  - **current-config** : 現在の実行コンフィギュレーションを指定します。コマンドが入力されると、この設定が維持されます。
  - **backup-config** : コンフィギュレーション バックアップ ファイル用の保管場所を指定します。
- | : 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** : **more** コマンドのフィルタリングされていない出力を、指定された正規表現が含まれる最初の行から開始します。
- **exclude** : **more** コマンドの出力で、特定の正規表現が含まれる行を除外します。
- **include** : **more** コマンドの出力で、指定する正規表現が含まれる行のみを含めます。
- *regular-expression* : **more** コマンドの出力で、検出される正規表現を指定します。

（注）　*regular-expression* オプションは、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。

More コマンドの使用によるフィルタ処理

more コマンドをフィルタ処理するには、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　たとえば、正規表現「ip」で始まる current-config の出力をフィルタ処理します。

```
ips-ssp# more current-config | begin ip
generating current config:
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
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）　Ctrl キーを押した状態で C キーを押して出力を停止して CLI プロンプトに戻ります。

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

```
ips-ssp# more current-config | exclude ip
generating current config:
! ------------------------------
! Version 7.1(1)
! Current configuration last modified Fri Aug 11 15:10:57 2010
! ------------------------------
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 ips-ssp
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
--MORE--
```

（注）　Ctrl キーを押した状態で C キーを押して出力を停止して CLI プロンプトに戻ります。

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

```
ips-ssp# more current-config | include ip
generating current config:
host-ip 192.0.2.0/24,192.0.2.17
engine atomic-ip
```

現在のサブモード コンフィギュレーションの出力のフィルタ処理

目的のサブモードで **show settings | [begin | exclude | include]** *regular_expression* コマンドを使用して、サブモード コンフィギュレーションの内容の出力の検索またはフィルタ処理を行います。

オプション

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** コマンドのフィルタリングされていない出力を、指定された正規表現が含まれる最初の行から開始します。
- **exclude** : **show settings** コマンドの出力で、特定の正規表現が含まれる行を除外します。
- **include** : **show settings** コマンドの出力で、指定する正規表現が含まれる行のみを含めます。
- *regular_expression* : **show settings** コマンドの出力で検出される任意の正規表現を指定します。

（注）　*regular_expression* オプションは、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。

サブモードの出力のフィルタ処理

サブモード コンフィギュレーションの内容の出力の検索またはフィルタ処理をするには、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　たとえば正規表現「filters」についてイベント アクション規則設定の出力を検索します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules
ips-ssp(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)
```

```
 ---------------------------------------------
 ---------------------------------------------
ips-ssp(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処理して正規表現を除外します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(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: 192.0.2.1
         -----------------------------------------------
            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処理して正規表現「ip.」を含めます。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# show settings | include ip
      host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
ips-ssp(config-hos)#
```

論理ファイルの内容の表示

more *keyword* コマンドを使用して、現在のシステム設定または保存されたバックアップのシステム設定など、論理ファイルの内容を表示します。

オプション

次のオプションが適用されます。

- *keyword* : current-config または backup-config を指定します。
  - **current-config** : 現在の実行コンフィギュレーションを指定します。コマンドが入力されると、この設定が維持されます。
  - **backup-config** : コンフィギュレーション バックアップ ファイル用の保管場所を指定します。

（注）　オペレータとビューアは、現在の設定のみ表示できます。管理者のみがパスワードなどの非表示フィールドを表示できます。

terminal length 0 コマンドを使用してターミナル長をゼロに設定することにより、**more current-config** または **more backup-config** で more prompt をディセーブルにできます。その結果、**more** コマンドは、ファイルの内容全体を一時停止せずに表示します。

論理ファイルの内容の表示

論理ファイルの内容を表示するには、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　現在のコンフィギュレーション ファイルの内容を表示します。

```
ips-ssp# more current-config
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
```

```
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
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
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
```

```
ips-ssp#
```

詳細情報

terminal コマンドを使用する手順については、「ターミナル プロパティの変更」（P.17-12）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。

copy [**/erase**] *source_url destination_url keyword* コマンドを使用して、コンフィギュレーション ファイルをリモート サーバにコピーします。その後、リモート サーバから現在の設定を復元できます。まず現在の設定をバックアップす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**：コピーする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 は、常に上書きされます。このキーワードがコピー先の current-config に対して指定されている場合、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。このキーワードがコピー先の current-config に対して指定されていない場合、コピー元の設定がその current-config にマージされます。

- *source_url*：コピー元のファイルの場所です。URL またはキーワードを使用できます。
- *destination_url*：コピー先のファイルの場所です。URL またはキーワードを使用できます。
- **current-config**：現在の実行コンフィギュレーションです。コマンドが入力されると、設定が維持されます。
- **backup-config**：コンフィギュレーション バックアップの保管場所です。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの場合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 サーバの場合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、パスワードの入力を求められます。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 リストに追加することも必要です。

- http: : Web サーバの場合のコピー元 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 サーバの場合のコピー元 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） Web サイトにアクセスするのにユーザ名が必要な場合、HTTP および HTTPS によってパスワードが要求されます。HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

注意 センシング インターフェイスおよび仮想センサーが同じ設定になっていない場合、別のセンサーからのコンフィギュレーション ファイルのコピーは、エラーにな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** を入力して、現在の設定をバックアップの設定にコピーします。

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

バックアップ ファイルからの現在の設定の復元

バックアップ ファイルから現在の設定を復元するには、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** を入力して、現在の設定をバックアップの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　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 リストを保持するには、**no** を入力します。残りの設定が復元された後、センサーへのアクセスを確保するために、この情報を保持することを推奨します。

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 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- リモート ホストを TLS の信頼できるホストの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.4-40）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。現在の設定がバックアップ ファイルに保存されます。

```
ips-ssp# copy current-config backup-config
```

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。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。

```
ips-ssp# more backup-config
```

ステップ 4　バックアップの設定を現在の設定とマージしたり、現在の設定を上書きしたりすることができます。

- バックアップの設定を現在の設定とマージします。

  ```
  ips-ssp# 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。

  ```
  ips-ssp# copy /erase backup-config current-config
  ```

コンフィギュレーション ファイルの消去

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

次のオプションが適用されます。

- **current-config**：現在の実行コンフィギュレーションです。コマンドが入力されると、設定が維持されます。
- **backup-config**：コンフィギュレーション バックアップの保管場所です。

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。

```
ips-ssp# 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　Enter を押して、続行するか、**no** を入力して停止します。