コンフィギュレーション モードの Cisco ISE CLI コマンド

この章では、Cisco ISE コマンドライン インターフェイス（CLI）のコンフィギュレーション（config）モードで使用するコマンドについて説明します。この章では、コマンドごとに、その使用方法の簡単な説明、コマンドの構文、使用上のガイドライン、および使用例を示します。

EXEC モードでのコンフィギュレーション モードへの切り替え

EXEC モードで **configure** または **configure terminal (conf t)** コマンドを実行すると、コンフィギュレーション モードを開始できます。

Cisco ISE CLI から EXEC モードでコンフィギュレーション コマンドを直接入力することはできません。一部のコンフィギュレーション コマンドでは、コマンド コンフィギュレーションを完了するために、コンフィギュレーション サブモードを開始する必要があります。

コンフィギュレーション モードを終了するには、**exit**、**end**、または **Ctrl-z** コマンドを入力します。

コンフィギュレーションコマンドには **interface**、**Policy List**、**repository** が含まれます。

コンフィギュレーションモードで設定作業を実行できます。コンフィギュレーションの変更内容の保存をデフォルトで設定し、システムのリロードや停電時に変更内容が失われないようにします。

コンフィギュレーション モードでの Cisco ISE の設定

コンフィギュレーション コマンドおよびコンフィギュレーション サブモード コマンドを入力して、Cisco ISE サーバーの実際の設定をコンフィギュレーション モードで変更できます。

ステップ 1 **configure terminal** と入力してコンフィギュレーション モードを開始します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

ステップ 2 疑問符（?）を入力して、コンフィギュレーション モードのコマンドの一覧を表示します。

```
ise32/iseadmin#configure terminal
Entering configuration mode terminal
ise/iseadmin(config)#?
Possible completions:
cdp                CDP Configuration parameters
clock              Configure timezone
conn-limit         Configure a TCP connection limit from source IP
hostname           Configure hostname
icmp               Configure icmp echo requests
identity-store     Configure identity store for CLI users
interface          Configure interface
ip                 Configure IP features
ipv6               Configure IPv6 features
kron               Configure command scheduler
logging            Configure system logging
ntp                Specify NTP configuration
password-policy    Password Policy Configuration
rate-limit         Configure a TCP/UDP/ICMP packet rate limit from source IP
repository         Configure Repository
service            Modify use of network based services
snmp-server        Configure snmp server
synflood-limit     Average number of TCP SYN packets per second allowed
username           User creation
---
do                 Run an operational-mode command
end                Terminate configuration session
exit               Exit from current mode
no                 Negate a command or set its defaults
<cr>
```

ステップ 3 コンフィギュレーション サブモードを開始します。コンフィギュレーション モードには数種類のコンフィギュレーション サブモードがあります。各サブモードに入ると、プロンプト階層のさらに深いレベルで操作できます。このレベルから、Cisco ISE コンフィギュレーションに直接コマンドを入力できます。

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

ステップ 4 コンフィギュレーション モードと EXEC モードの両方を終了するには、コマンドプロンプトで **exit** を順に入力します。**exit** と入力すると、Cisco ISE はユーザーのレベルを 1 段階戻し、前のレベルに戻します。もう一度 **exit** と入力すると、Cisco ISE はユーザーを EXEC レベルに戻します。

```
ise/admin(config)# exit
ise/admin# exit
```

コンフィギュレーションサブモードでのCisco ISEの設定

コンフィギュレーションサブモードで特定の設定のコマンドを入力できます。このプロンプトを終了してコンフィギュレーション プロンプトに戻る場合は **exit** コマンドまたは **end** コマンドを使用できます。

ステップ 1 **configure terminal** と入力してコンフィギュレーション モードを開始します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

ステップ 2 コンフィギュレーション サブモードを開始します。

```
ise/admin# configure terminal
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  backup    Configure NIC bonding feature
  do        EXEC command
  end       Exit from configure mode
  exit      Exit from this submode
  ip        Configure IP features
  ipv6      Configure IPv6 features
  no        Negate a command or set its defaults
  shutdown  Shutdown the interface
ise/admin(config-GigabitEthernet)#
```

ステップ 3 コマンドプロンプトで **exit** を入力して、コンフィギュレーション サブモードとコンフィギュレーション モードの両方を終了します。

```
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# exit
ise/admin#
```

CLI コンフィギュレーション コマンドのデフォルト設定

CLI コンフィギュレーション コマンドには、default 形式があることがあります。この形式は、コマンド設定をデフォルト値に戻します。ほとんどのコマンドはデフォルトでディセーブルに設定されているため、この場合はコマンドで default 形式を使用しても **no** 形式を使用しても同じ結果になります。

ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。そのような場合に default 形式のコマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

backup interface

高可用性のために単一の仮想インターフェイスに2つのイーサネットインターフェイスを設定（NIC ボンディング機能または NIC チーミング機能とも呼ばれる）するには、コンフィギュレーション サブモードで **backup interface** コマンドを使用します。NIC ボンディング設定を削除するには、このコマンドの **no** 形式を使用します。2 つのインターフェイスをボンディングすると、2 つの NIC は 1 つの MAC アドレスを持つ単一のデバイスとして認識されます。

Cisco ISE の NIC ボンディング機能は、ロード バランシングまたはリンク アグリゲーション機能をサポートしていません。Cisco ISE は、NIC ボンディングの高可用性機能だけをサポートします。

インターフェイスのボンディングでは、次の状況でも Cisco ISE サービスが影響を受けないことを保証します。

- 物理インタフェースの障害
- スイッチ ポート接続の喪失（シャットダウンまたは障害）
- スイッチ ラインカードの障害

2 つのインターフェイスをボンディングすると、インターフェイスの一方がプライマリ インターフェイスになり、もう一方はバックアップインターフェイスになります。2つのインターフェイスをボンディングすると、すべてのトラフィックは通常、プライマリ インターフェイスを通過します。プライマリ インターフェイスが何らかの理由で失敗すると、バックアップ インターフェイスがすべてのトラフィックを引き継いで処理します。ボンディングにはプライマリ インターフェイスの IP アドレスと MAC アドレスが必要です。

NIC ボンディング機能を設定する際に、Cisco ISE は固定物理 NIC を組み合わせて NIC のボンディングを形成します。ボンディング インターフェイスを形成するためにボンディングすることができる NIC について、次の表に概要を示します。

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 0	Eth0	プライマリ	ボンド 0
ギガビットイーサネット 1	Eth1	バックアップ	
ギガビットイーサネット 2	Eth2	プライマリ	ボンド 1
ギガビットイーサネット 3	Eth3	バックアップ	

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 4	Eth4	プライマリ	ボンド 2
ギガビットイーサネット 5	Eth5	バックアップ	

NIC ボンディング機能は、サポートされているすべてのプラットフォームとノード ペルソナでサポートされています。サポートされるプラットフォームは次のとおりです。

- SNS-3400 シリーズ アプライアンス：ボンド 0 および 1（Cisco ISE 3400 シリーズ アプライアンスは最大 4 個の NIC をサポート）
- SNS-3500 シリーズ アプライアンス：ボンド 0、1、および 2
- VMware 仮想マシン：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）
- Linux KVM ノード：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）

構文の説明

backup interface	NIC ボンディング機能を設定します。
GigabitEthernet	バックアップ インターフェイスとして指定されるギガビット イ ト インターフェイスを設定します。
0 ～ 3	バックアップ インターフェイスとして設定するギガビット イ ト ポートの数。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション サブモード (config-GigabitEthernet)#

コマンド履歴

リリース	変更内容
2.1.0.474	このコマンドが導入されました。

使用上のガイドライン

- Cisco ISE は最大 6 つのイーサネット インターフェイスをサポートするので、ボンドは 3 つ（ボンド 0、ボンド 1、ボンド 2）のみ設定できます。
- ボンドに含まれるインターフェイスを変更したり、ボンドのインターフェイスのロールを変更したりすることはできません。ボンディングできる NIC とボンドでの役割についての情報については、上記の表を参照してください。
- Eth0 インターフェイスは、管理インターフェイスとランタイム インターフェイスの両方として機能します。その他のインターフェイスは、ランタイムインターフェイスとして機能します。

- ボンドを作成する前に、プライマリ インターフェイス（プライマリ NIC）に IP アドレスを割り当てる必要があります。ボンド 0 を作成する前は、Eth0 インターフェイスに IPv4 アドレスを割り当てる必要があります。同様に、ボンド 1 と 2 を作成する前は、Eth2 と Eth4 インターフェイスに IPv4 または IPv6 アドレスをそれぞれ割り当てる必要があります。
- ボンドを作成する前に、バックアップ インターフェイス（Eth1、Eth3、および Eth5）に IP アドレスが割り当てられている場合は、バックアップ インターフェイスからその IP アドレスを削除します。バックアップ インターフェイスには IP アドレスを割り当てないでください。
- ボンドを 1 つのみ（ボンド 0）作成し、残りのインターフェイスをそのままにすることもできます。この場合、ボンド 0 は管理インターフェイスとランタイム インターフェイスとして機能し、残りのインターフェイスはランタイム インターフェイスとして機能します。
- ボンドでは、プライマリ インターフェイスの IP アドレスを変更できます。プライマリ インターフェイスの IP アドレスと想定されるので、新しい IP アドレスがボンディングされたインターフェイスに割り当てられます。
- 2 つのインターフェイス間のボンドを削除すると、ボンディングされたインターフェイスに割り当てられていた IP アドレスは、プライマリ インターフェイスに再び割り当てられます。
- デプロイメントに含まれる Cisco ISE ノードで NIC ボンディング機能を設定するには、そのノードをデプロイメントから登録解除し、NIC ボンディングを設定して、デプロイメントに再度登録する必要があります。
- ボンド（Eth0、Eth2、または Eth4 インターフェイス）のプライマリ インターフェイスとして機能する物理インターフェイスにスタティック ルートが設定されている場合は、物理インターフェイスではなくボンディングされたインターフェイスで動作するようにスタティック ルートが自動的に更新されます。

例 1：NIC ボンディングの設定

次の手順では、Eth0 と Eth1 インターフェイス間にボンド 0 を設定する方法を説明します。

（注） バックアップインターフェイスとして動作する物理インターフェイス（Eth1、Eth3、Eth5 インターフェイスなど）に IP アドレスが設定されている場合は、バックアップ インターフェイスからその IP アドレスを削除する必要があります。バックアップ インターフェイスには IP アドレスを割り当てないでください。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
```

```
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

例 2：NIC ボンディングの設定の確認

NIC ボンディング機能が設定されているかどうかを確認するには、Cisco ISE CLI から **show running-config** コマンドを実行します。次のような出力が表示されます。

```
!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
```

上記の出力では、「backup interface GigabitEthernet 1」は、ギガビット イーサネット 0 に NIC ボンディングが設定されていて、ギガビットイーサネット0がプライマリ インターフェイス、ギガビット イーサネット 1 がバックアップ インターフェイスとされていることを示します。また、ADE-OS 設定では、プライマリおよびバックアップのインターフェイスに効果的に同じ IP アドレスを設定していても、running config でバックアップ インターフェイスの IP アドレスは表示されません。

また、**show interfaces** コマンドを実行して、ボンディングされたインターフェイスを表示できます。

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::8a5a:92ff:fe88:4aea  prefixlen 64  scopeid 0x20<link>
        ether 88:5a:92:88:4a:ea  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfab00000-fabfffff

GigabitEthernet 1
        flags=6147<UP,BROADCAST,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfaa00000-faafffff
```

cdp holdtime

受信デバイスが Cisco ISE サーバーからの Cisco Discovery Protocol パケットを廃棄するまでの保持時間を指定するには、コンフィギュレーション モードで **cdp holdtime** コマンドを使用します。

cdp holdtime *seconds*

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

no cdp holdtime

構文の説明

holdtime	アドバタイズされた Cisco Discovery Protocol の保持時間を指定
seconds	秒単位のアドバタイズされた保持時間値。値の範囲は、10 ～ す。

コマンド デフォルト

CDP 保持時間のデフォルト値は、180 秒です。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

Cisco Discovery Protocol パケットを存続可能時間、つまり保持時間の値とともに送信します。受信デバイスは、保持時間の経過後に、Cisco Discovery Protocol パケットの Cisco Discovery Protocol 情報を廃棄します。

cdp holdtime コマンドに指定できる引数は 1 つだけです。複数指定した場合は、エラーが発生します。

例

```
ise/admin(config)# cdp holdtime 60
ise/admin(config)#
```

cdp run

すべてのインターフェイスで Cisco Discovery Protocol を有効にするには、コンフィギュレーション モードで **cdp run** コマンドを使用します。

cdp run *GigabitEthernet*

Cisco Discovery Protocol を無効にするには、このコマンドの **no** 形式を使用します。

no cdp run

構文の説明

run	Cisco Discovery Protocol をイネーブルにします。**cdp run** コマン 形式を使用した場合は、Cisco Discovery Protocol が無効になりま
GigabitEthernet	（任意）。Cisco Discovery Protocol をイネーブルにする GigabitEt インターフェイスを指定します。
0-3	Cisco Discovery Protocol をイネーブルにする GigabitEthernet インタ イス番号を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、1 つのオプションの引数（インターフェイス名）を指定します。オプションのインターフェイス名が指定されない場合、コマンドはすべてのインターフェイスで Cisco Discovery Protocol をイネーブルにします。

（注） このコマンドのデフォルトでは、すでに実行されているインターフェイスで動作します。インターフェイスの起動時に、最初に Cisco Discovery Protocol を停止します。次に、Cisco Discovery Protocol を起動します。

例

```
ise/admin(config)# cdp run GigabitEthernet 0
ise/admin(config)#
```

cdp timer

Cisco ISE サーバーが Cisco Discovery Protocol アップデートを送信する頻度を指定するには、コンフィギュレーション モードで **cdp timer** コマンドを使用します。

cdp timer *seconds*

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

no cdp timer

構文の説明

timer	指定した間隔で更新されます。
seconds	Cisco ISE サーバーが Cisco Discovery Protocol 更新を送信する頻 位で指定します。値の範囲は、5 ～ 254 秒です。

コマンド デフォルト

更新間隔値のデフォルトは 60 秒です。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

Cisco Discovery Protocol パケットを存続可能時間、つまり保持時間の値とともに送信します。受信デバイスは、保持時間の経過後に、Cisco Discovery Protocol パケットの Cisco Discovery Protocol 情報を廃棄します。

cdp timer コマンドに指定できる引数は 1 つだけです。複数指定した場合は、エラーが発生します。

例

```
ise/admin(config)# cdp timer 60
ise/admin(config)#
```

clock timezone

時間帯を設定するには、コンフィギュレーション モードで **clock timezone** コマンドを実行します。

clock timezone タイムゾーン

（注） インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなるため、ISE を再起動する必要があります。初期設定ウィザードで時間帯の設定を求めるプロンプトが表示されたら、優先する時間帯（デフォルト UTC）をインストール中に設定することをお勧めします。

構文の説明

timezone	システムの時間帯を設定します。
タイムゾーン	標準時に表示する時間帯の名前。最大 64 文字の英数字をサポートします。

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、時間帯を設定する前にディセーブルにしてください。時間帯を設定した後でイネーブルに戻すことができます。

コマンド デフォルト

協定世界時（UTC）

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。
3.2	このコマンドの no 形式はサポートされなくなりました。

使用上のガイドライン

システムの内部的には、UTC での時刻が保持されます。特定の時間帯がわからない場合は、地域、国、都市を入力できます（システムに入力する共通の時間帯およびオーストラリアとアジアの時間帯については、表 4-1、4-2、4-3 を参照）。

（注） これ以外にも使用可能な時間帯がいくつかあります。**show timezones** を入力すると、使用可能なすべての時間帯のリストが Cisco ISE サーバーに表示されます。該当地域の時間帯に最も適した時間帯を選択します。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例

```
ise/admin(config)# clock timezone EST
ise/admin(config)# exit
ise/admin# show timezone
EST
ise/admin#
```

Cisco ISE ノードの時間帯の変更

インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなります。ただし、初期設定ウィザードで時間帯の設定を求めるプロンプトが表示されたら、優先する時間帯（デフォルト UTC）をインストール中に設定できます。

時間帯の変更は、導入の異なる Cisco ISE ノード タイプに影響を与えます。

影響から回復するには、次の手順を使用します。

スタンドアロンまたはプライマリ Cisco ISE ノード

インストール後にタイムゾーンを変更するには、ノードのイメージを再作成する必要があります。

最新の設定のバックアップがあることを確認し、必要な証明書とキーをエクスポートします。

タイムゾーンを変更する場合は、次の操作を行います。

- プライマリ Cisco ISE ノードを再イメージ化します。
- インストール中に、適切なタイムゾーンを選択します。
- バックアップと証明書を復元します。
- Active Directory に再参加し、ISE プロファイラプローブ、LDAP などのノードごとの設定を適用します。

セカンダリ ISE ノード

プライマリ ノードの時間帯と同じになるようにセカンダリ ノードの時間帯を変更する場合、次の手順を実行します。

- 必要な証明書をエクスポートします。
- セカンダリ ノードの登録を解除します。
- ノードを再イメージ化します。
- 必要に応じて、必要な証明書をインポートします。
- ノードをプライマリノードにセカンダリノードとして再登録します。

- Active Directory に再参加し、ISE プロファイラプローブ、LDAP などのノードごとの設定を適用します。

共通の時間帯

表 *1:* 表 *4-1* 共通の時間帯（続き）

略語または名前	時間帯名
欧州	
GMT、GMT0、GMT-0、GMT+0、UTC、Greenwich、Universal、Zulu	グリニッジ標準時（UTC）
GB	英国
GB-Eire、Eire	アイルランド
WET	西ヨーロッパ時間（UTC）
CET	中央ヨーロッパ標準時（UTC + 1 時間）
EET	東ヨーロッパ時間（UTC + 2 時間）
米国およびカナダ	
EST、EST5EDT	東部標準時、UTC - 5 時間
CST、CST6CDT	中央標準時、UTC - 6 時間
MST、MST7MDT	山岳部標準時、UTC - 7 時間
PST、PST8PDT	太平洋標準時、UTC - 8 時間
HST	ハワイ標準時、UTC - 10 時間

オーストラリアのタイム ゾーン

（注） オーストラリアの時間帯では、国と都市をスラッシュ（/）で区切って入力します（例：Australia/Currie）。

表 *2 :* 表 *4-2* オーストラリアの時間帯（続き）

Australia			
Australian Capital Territory（ACT）	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	Lord Howe Island（LHI）	Melbourne
North	New South Wales（NSW）	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

アジアのタイム ゾーン

（注） アジアの時間帯には、東アジア、南アジア、東南アジア、西アジア、および中央アジアがあります。地域と都市または国をスラッシュ（/）で区切って入力します（例：Asia/Aden）。

表 *3 :* 表 *4-3* アジアの時間帯（続き）

Asia			
Aden	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

cls

端末画面の内容をクリアするには、コンフィギュレーション モードで **cls** コマンドを使用します。

cls

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

cls は隠しコマンドです。**cls** は Cisco ISE で使用できますが、コマンドラインで疑問符を入力して表示しようとした場合、CLI インタラクティブヘルプには表示されません。

例

次の例は、端末の内容をクリアする方法を示しています。

```
ise/admin(config)# cls
ise/admin#
```

conn-limit

送信元 IP アドレスからの着信 TCP 接続の制限を設定するには、コンフィギュレーション モードで **conn-limit** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

構文の説明

name	設定する conn-limit の名前を入力します。
<1-2147483647>	TCP 接続の数。
ip	（任意）。TCP 接続制限を適用する送信元 IP アドレス。
mask	（任意）。TCP 接続制限を適用する送信元 IP マスク。
port	（任意）。TCP 接続制限を適用する宛先ポート番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。
3.2	このコマンドが更新され、構成する conn-limit に名前を割り当てになりました。

使用上のガイドライン

この **conn-limit** コマンドは、TCP 接続が 99 を超える場合に使用します。100 未満の接続の場合は、次の警告が表示されます。

```
% Warning: Setting a small conn-limit may adversely affect system performance
```

例

```
ise/admin(config)# conn-limit lablimit 25000 ip 10.0.0.1 port 22
ise/admin(config)# end
ise/admin
```

service cache

ホストの DNS 要求をキャッシュするには、コンフィギュレーション モードで **service cache enable** コマンドを使用します。この機能を有効にすると、DNS サーバーの負荷が軽減されます。

service cache enable hosts ttl *ttl*

この機能をディセーブルにするには、このコマンドの no 形式を使用します。

構文の説明

ttl	キャッシュを有効にしながら、キャッシュ内のホストの存続可能時間（TTL）値を秒単位で設定できます。ttlのデフォルト設定はありません。ttl では 1 ～ 2147483647 の範囲の値を指定できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

使用上のガイドライン

TTL 値は、否定応答に対して受け入れられます。DNS サーバーで設定された TTL 値は、肯定応答に対して受け入れられます。DNS サーバーで TTL が定義されていない場合は、コマンドで設定された TTL が受け入れられます。機能を無効にするとキャッシュも無効になります。

例

```
ise/admin(config)# service cache enable hosts ttl 10000
Enabling dns cache
ise/admin(config)# exit
```

do

コンフィギュレーション モードまたは任意のコンフィギュレーション サブモードから EXEC システムレベルのコマンドを実行するには、いずれかのコンフィギュレーション モードで **do** コマンドを使用します。

do *EXEC commands*

構文の説明

EXEC commands	EXEC システム レベルのコマンドを実行することを指定しま 表 4-4 do コマンドのコマンド オプション（続き） を参照）。

表 *4*：表 *4-4 do* コマンドのコマンド オプション（続き）

コマンド	説明
application configure	特定のアプリケーションを設定します。
application install	特定のアプリケーションをインストールします。
application remove	特定のアプリケーションを削除します。
application reset-config	アプリケーション コンフィギュレーションを工場出荷時のデ 定にリセットします。
application reset-passwd	指定したユーザーのアプリケーション パスワードをリセット
application start	特定のアプリケーションを起動またはイネーブルにします。
application stop	特定のアプリケーションを停止またはディセーブルにします
application upgrade	特定のアプリケーションをアップグレードします。
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、その プをリポジトリに保存します。
backup-logs	Cisco ISE サーバーに記録されているすべてのログをリモート バックアップします。
clock	Cisco ISE サーバーのシステム クロックを設定します。
configure	設定モードを開始します。
copy	コピー元からコピー先に任意のファイルをコピーします。
debug	さまざまなコマンド状況（たとえば、バックアップと復元、 ギュレーション、コピー、リソースのロック、ファイル転送、 管理など）で、エラーまたはイベントを表示します。
delete	Cisco ISE サーバー上のファイルを削除します。

コマンド	説明
dir	Cisco ISE サーバーのファイルを一覧表示します。
forceout	特定の Cisco ISE ノード ユーザーのすべてのセッションを強制的 アウトします。
halt	Cisco ISE サーバーをディセーブルにするか、シャットダウンし
mkdir	新しいディレクトリを作成します。
nslookup	リモート システムの IPv4 または IPv6 アドレス、あるいはホスト い合わせます。
password	CLI アカウント パスワードを更新します。
patch	パッチ バンドルをインストールする、またはアプリケーションの をアンインストールします。
ping	リモート システムの IPv4 アドレスまたはホスト名を特定します
ping6	リモート システムの IPv6 アドレスを特定します。
reload	Cisco ISE サーバーを再起動します。
restore	復元を実行して、リポジトリからバックアップを取得します。
rmdir	既存のディレクトリを削除します。
show	Cisco ISE サーバーに関する情報を提供します。
ssh	リモート システムとの暗号化されたセッションを開始します。
tech	Technical Assistance Center（TAC）コマンドを提供します。
terminal length	端末回線のパラメータを設定します。
terminal session-timeout	すべてのターミナル セッションに対して、無活動タイムアウトを ます。
terminal session-welcome	すべてのターミナル セッションで表示される初期メッセージをシ に設定します。
terminal terminal-type	現在のセッションの現在の回線に接続されている端末のタイプを ます。
traceroute	リモート IP アドレスのルートをトレースします。

コマンド	説明
undebug	さまざまなコマンド状況（たとえば、バックアップと復元、ギュレーション、コピー、リソースのロック、ファイル転送、管理など）で、debug コマンドの出力（エラーまたはイベン をディセーブルにします。
write	強制的にセットアップユーティリティを実行してネットワーク ギュレーションをプロンプトするスタートアップ コンフィギ ンを消去し、実行コンフィギュレーションをスタートアップ ギュレーションにコピーし、コンソールに実行コンフィギュ を表示します。 （注） Cisco ISE リリース 3.2 以降はこのコマンドが変更 running-config および startup-config 機能がサポート ん。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）# または任意のコンフィギュレーション サブモード（config-GigabitEthernet）# と（config-Repository）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

この **do** コマンドは、Cisco ISE サーバーの設定中に、EXEC コマンド（**show**、**clear**、および **debug** コマンドを含む）を実行する場合に使用します。EXEC コマンドの実行後、システムは使用していたコンフィギュレーション モードに戻ります。

例

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 10.0.0.1
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
```

```
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--
ise/admin(config)#
```

end

現在のコンフィギュレーション セッションを終了して、EXEC モードに戻るには、コンフィギュレーション モードで **end** コマンドを使用します。

このコマンドには、キーワードおよび引数はありません。

end

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在のコンフィギュレーション モードやサブモードにかかわらず、EXEC モードに移行します。

このコマンドは、システム設定を終了し、EXEC モードに戻って、検証手順を実行する場合に使用します。

例

```
ise/admin(config)# end
ise/admin#
```

exit

コンフィギュレーション モードを終了して、CLI モード階層で次に高いモードに移行するには、コンフィギュレーション モードで **exit** コマンドを使用します。

exit

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

exit コマンドは、Cisco ISE サーバーで現在のコマンドモードを終了して、CLI モード階層の次に高いコマンドモードに移行する場合に使用します。

たとえば、EXEC モードに戻るには、コンフィギュレーション モードで **exit** コマンドを使用します。コンフィギュレーション サブモードで **exit** コマンドを使用すると、コンフィギュレーション モードに戻ります。最上位の EXEC モードで **exit** コマンドを使用すると、EXEC モードを終了して、Cisco ISE サーバーから接続解除されます。

例

```
ise/admin(config)# exit
ise/admin#
```

hostname

システムのホスト名を設定するには、コンフィギュレーション モードで **hostname** コマンドを使用します。

hostname *hostname*

構文の説明

hostname	ホストの名前。19 文字までの英数字と下線（_）をサポート スト名はスペース以外の文字で始める必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

（注） 「hostname」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、一部のアプリケーション コンポーネントは古いホスト名を持ち、他のコンポーネントは新しいホスト名を使用する状態になる可能性があります。これにより、Cisco ISE ノードは機能していない状態になります。

この問題を回避するには、「hostname」コンフィギュレーション コマンドを再度実行して、ホスト名を目的の値に設定します。

hostname コマンドを使用して、現在のホスト名を変更できます。シングルインスタンスタイプのコマンドである **hostname** は、システムの設定時に一度だけ実行します。ホスト名には 1 つの引数を含める必要があります。引数がない場合、エラーが発生します。

このコマンドを使用して Cisco ISE サーバーのホスト名を更新すると、次の警告メッセージが表示されます。

```
% Warning:  Updating the hostname will cause any certificate using the old
%           hostname to become invalid. Therefore, a new self-signed
%           certificate using the new hostname will be generated now for
%           use with HTTPs/EAP.  If CA-signed certs were used on this node,
%           please import them with the correct hostname. If Internal-CA
%           signed certs are being used, please regenerate ISE Root CA certificate.
%           In addition, if this ISE node will be joining a new Active Directory
%           domain, please leave your current Active Directory domain before
%           proceeding. If this ISE node is already joined to
%           an Active Directory domain, then it is strongly advised
%           to rejoin all currently joined join-points in order to
%           avoid possible mismatch between current and previous
%           hostname and joined machine account name.
```

例

```
ise/admin(config)# hostname new-hostname
% Changing the hostname will cause ISE services to restart
Continue with hostname change?  Y/N [N]: y

Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
ISE Database processes already running, PID: 9651
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-1/admin#
```

icmp echo

インターネット制御メッセージプロトコル（ICMP）のエコー応答を設定するには、コンフィギュレーション モードで **icmp echo** コマンドを使用します。

icmp echo {*off* | *on*}

構文の説明

echo	ICMP エコー応答を設定します。
off	ICMP エコー応答をディセーブルにします。
on	ICMP エコー応答をイネーブルにします。

コマンド デフォルト

システムは ICMP エコー応答がオン（イネーブル）の場合と同様に動作します。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ICMP エコー応答をオンまたはオフにするには、この **icmp echo** を使用します。

例

```
ise/admin(config)# icmp echo off
ise/admin(config)#
```

identity-store

CLI 管理者を Active Directory ドメインに参加させるには、コンフィギュレーションモードで **identity-store** コマンドを使用します。Cisco ISE ノードが複数のドメインに参加している場合は、このコマンドを使用して参加できるドメインは 1 つだけです。各 CLI 管理者は個別に参加します。Cisco ISE が操作を完了するまで 5 分間待ってください。

このコマンドを使用して参加するドメインが、ISE ノードに参加していたドメインと同じである場合は、管理者コンソールでドメインに再参加する必要があります。管理 CLI ユーザーはネットワーク管理者である必要があります。

コマンド履歴

リリース	変更内容
2.6.0.156	このコマンドが導入されました。

例

```
identity-store active-directory domain-name <aDomainFQDN> user <adUserNameWithJoinPrivs>
```

（注） Active Directory CLI は、子ドメインユーザを使用した認証をサポートしていません。子ドメインは、認証に使用される対応ユーザーに対し、明示的に参加する必要がある個別のドメインと見なされます。

interface

インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドをコンフィギュレーション モードで使用します。このコマンドには **no** 形式はありません。

（注） VMware 仮想マシンで使用可能なインターフェイスの数は、仮想マシンに追加されるネットワーク インターフェイス（NIC）の数によって異なることがあります。

interface GigabitEthernet {*0* | *1* | *2* | *3*}

構文の説明

GigabitEthernet	ギガビット イーサネット インターフェイスを設定します。
0 ～ *3*	設定するギガビット イーサネット ポートの数。

（注） **interface** コマンドでギガビット イーサネット ポートの数を入力すると、config-GigabitEthernet コンフィギュレーション サブモードが開始されます（次の「構文の説明」を参照）。

構文の説明

backup	NIC ボンディング機能を設定して、物理インターフェイスに冗 提供します。
do	EXEC コマンド。このモードで EXEC コマンドを実行できま
end	config-GigabitEthernet サブモードを終了し、EXEC モードに戻
exit	config-GigabitEthernet コンフィギュレーション サブモードを終
ip	ギガビット イーサネット インターフェイスの IP アドレスとネ クを設定します。
ipv6	DHCPv6 サーバーから IPv6 アドレス自動設定および IPv6 ア 定します。
no	このモードのコマンドを否定します。2つのキーワードを使用 • ip：インターフェイスの IP アドレスとネットマスクを設 • ipv6：インターフェイスの IPv6 アドレスを設定します。 • shutdown：インターフェイスをシャットダウンします。
shutdown	インターフェイスをシャットダウンします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

interface コマンドを使用して、インターフェイスを設定し、さまざまな要件をサポートすることができます。

例

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

ip address

GigabitEthernet インターフェイスの IP アドレスとネットマスクを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。

ip address *ip-address network mask*

IP アドレスを削除するか、IP プロセシングを無効にするには、このコマンドの **no** 形式を使用します。

no ip address

（注） 複数のインターフェイスで、同じ IP アドレスを設定できます。この設定により、2 つのインターフェイス間の切り替えに必要なコンフィギュレーション手順を制限できます。

構文の説明

ip-address	IPv4 アドレス。
network mask	関連付けられた IP サブネットのマスク。

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、IP アドレスを設定する前にディセーブルにしてください。IP アドレスの設定後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

コマンド デフォルト

イネーブル。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

（注） 「ip address」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、IP アドレスを変更する場合、一部のアプリケーション コンポーネントは古い IP アドレスを使用し、他のコンポーネントは新しい IP アドレスを使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の「ip address」コンフィギュレーション CLI を発行して、IP アドレスを目的の値に設定します。

アドレスとネットマスクを必ず 1 つずつ指定する必要があります。指定しない場合、エラーが発生します。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
........
To verify that ISE processes are running, use the
'show application status ise' command.
ise/admin(config-GigabitEthernet)#
```

ip default-gateway

IPアドレスを指定してデフォルトゲートウェイを定義または設定するには、コンフィギュレーション モードで **ip default-gateway** コマンドを使用します。

ip default-gateway *ip-address*

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip default-gateway

構文の説明

default-gateway	IP アドレスを指定してデフォルト ゲートウェイを定義します
ip-address	デフォルト ゲートウェイの IP アドレス。

コマンド デフォルト

ディセーブル。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

複数の引数を指定した場合、または引数を指定していない場合はエラーが発生します。

例

```
ise/admin(config)# ip default-gateway 209.165.202.129
Adding/Changing gateway may cause ise services to restart.
Are you sure you want to proceed? Y/N [N]:
```

（注） ゲートウェイを追加または変更した場合、変更を有効にするためにサービスを再起動する必要があります。

ip domain-name

Cisco ISE サーバーがホスト名を完成させるために使用するデフォルトのドメイン名を定義するには、コンフィギュレーション モードで **ip domain-name** コマンドを使用します。

ip domain-name *domain-name*

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip domain-name

構文の説明

domain-name	デフォルトのドメイン名を定義します。
domain-name	ホスト名を完成させるために使用するデフォルトのドメイン名。文字の英数字で指定します。

コマンド デフォルト

イネーブル。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

（注） 「ip domain-name」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、IP ドメイン名を変更する場合、一部のアプリケーション コンポーネントは古いドメイン名を持ち、他のコンポーネントは新しいドメイン名を使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の「ip domain-name」コンフィギュレーション CLI を発行して、ドメイン名を目的の値に設定します。

入力した引数が多すぎる場合または不足している場合、エラーが発生します。

このコマンドで Cisco ISE サーバーのドメイン名を更新する場合は、次の警告メッセージが表示されます。

```
% Warning:  Updating the domain name will cause any certificate using the old
%           domain name to become invalid. Therefore, a new self-signed
%           certificate using the new domain name will be generated now for
%           use with HTTPs/EAP.  If CA-signed certs were used on this node,
%           please import them with the correct domain name. If Internal-CA
%           signed certs are being used, please regenerate ISE Root CA certificate.
%           In addition, if this ISE node will be joining a new Active Directory
%           domain, please leave your current Active Directory domain before
%           proceeding.
```

例

```
ise/admin(config)# ip domain-name cisco.com
ise/admin(config)#
```

ip host

eth1、eth2、eth3 など eth0 以外のイーサネット インターフェイスにホストエイリアスと完全修飾ドメイン名（FQDN）文字列を関連付けるには、グローバル コンフィギュレーション モードで **ip host** コマンドを使用します。

Cisco ISE は認証プロファイルのリダイレクト URL を処理するときに、その IP アドレスを Cisco ISE ノードの FQDN に置き換えます。

ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

ホストエイリアスと FQDN の関連付けを削除するには、このコマンドの **no** 形式を使用します。

no ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

構文の説明

ipv4-address	ネットワーク インターフェイスの IPv4 アドレス。
ipv6-address	ネットワーク インターフェイスの IPv6 アドレス。
host-alias	ホストのエイリアスは、ネットワーク インターフェイスに割り当前です。
FQDN-string	ネットワーク インターフェイスの完全修飾ドメイン名（FQDN）

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、イーサネット インターフェイスのホスト エイリアスおよび FQDN を変更する前にディセーブルにしてください。ホスト エイリアスおよび FQDN の設定完了後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is
not allowed! Please disable PAN Auto-failover first.
```

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。

- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの 4 つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

ip host コマンドを使用して、IP アドレスマッピング用にホストエイリアスと完全修飾ドメイン名（FQDN）文字列を追加します。eth1、eth2、eth3 などのイーサネット インターフェイスに一致する FQDN を検索する場合に使用します。ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

ホスト エイリアスか FQDN 文字列、またはその両方を指定できます。両方の値を指定する場合は、ホスト エイリアスと FQDN 文字列の最初のコンポーネントが一致している必要があります。FQDN 文字列のみを指定すると、Cisco ISE は URL 内の IP アドレスを FQDN に置き換えます。ホスト エイリアスのみを指定すると、Cisco ISE はホスト エイリアスと設定されている IP ドメイン名を組み合わせて完全な FQDN を形成し、URL 内のネットワーク インターフェイスの IP アドレスを FQDN に置き換えます。

（注） Cisco ISE 3.1 以降のバージョンでは、**ip host** コマンドにホストエイリアスを含めることを推奨します。

例 1

```
ise/admin(config)# ip host 172.21.79.96 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

例 2

```
ise/admin(config)# ipv6 host 2001:db8:cc00:1::1 ise1 ise1.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...

Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
```

```
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

ip mtu

インターフェイスで送受信される IP パケットの最大伝送ユニット（MTU）サイズを設定するには、インターフェイス コンフィギュレーション モードで **ip mtu** コマンドを使用します。デフォルトの MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ip mtu *bytes*

no ip mtu *bytes*

構文の説明

mtu	Cisco ISE インターフェイスの MTU を設定します。

コマンド デフォルト

MTU は 1500 として設定されます。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.4.0.357	このコマンドが導入されました。

使用上のガイドライン

IP パケットがインターフェイスに設定された MTU を超過すると、Cisco ISE はそれをフラグメント化します。物理メディアのすべてのデバイスが動作するには、同じプロトコル MTU を持っている必要があります。

例

次の例は、インターフェイスで MTU を設定する方法を示しています。

```
ise/admin(config)# int GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip mtu ?
<1280-9999>  Recommended range VM:1280-9216;appliance:1280-9999
```

次の例は、MTU の設定後に表示される出力を示しています。

```
ise/admin# show run | in mtu
ip mtu 1350
```

ip name-server

DNS クエリー実行時に使用するドメインネームサーバー（DNS）を設定するには、コンフィギュレーション モードで **ip name-server** コマンドを使用します。1 ～ 3 台の DNS サーバーを設定できます。

ip name-server *ip-address* {*ip-address**}

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip name-server *ip-address* {*ip-address**}

（注） このコマンドの **no** 形式を使用すると、設定からすべてのネームサーバーが削除されます。このコマンドの **no** 形式と IP 名の 1 つを使用すると、そのネームサーバーだけが削除されます。

構文の説明

name-server	ネームサーバーの IP アドレスを設定します。
ip-address	ネーム サーバのアドレス。
*ip-address**	（任意）。追加のネーム サーバーの IP アドレス。 （注） IPv4/IPv6 アドレスの一方または両方を設定できます。アドレスでネームサーバーを追加する場合は、ISE etインターフェイスが IPv6 アドレスで静的に設定されていを確認してください。

展開内でプライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、ip name-server コマンドを実行する前にディセーブルにし、DNS サーバーを設定した後でイネーブルに戻してください。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ip name-server コマンドを使用して追加された最初のネームサーバーは最初の位置に配置されます。システムはそのサーバーを最初に使用して、IP アドレスを解決します。

IPv4 または IPv6 アドレスを使用してシステムにネーム サーバーを追加できます。1 つのコマンドで、1 ～ 3 つの IPv4 または IPv6 アドレスを設定できます。システムにすでに 3 台のネーム サーバーが設定されている場合、少なくとも 1 台を削除するまでネーム サーバーを追加できません。

1 台のネームサーバーを最初の位置に配置して、サブシステムがまずそのサーバーを使用するようにするには、このコマンドの **no** 形式を使用してすべてのネームサーバーを削除してから処理を進める必要があります。

（注） AD 接続のこの設定を変更した場合、変更を有効にするために Cisco ISE を再起動する必要があります。また、Cisco ISE で設定されているすべての DNS サーバーがすべての関連する AD DNS レコードを解決できる必要があります。DNS 設定が変更された後、設定済みの AD 参加ポイントが正しく解決されない場合、脱退処理を手動で実行してから、AD 参加ポイントを再参加させる必要があります。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例 1

```
ise/admin(config)# ip name-server ?
<A.B.C.D>|<valid IPv6 format>  Primary DNS server IP address
<A.B.C.D>|<valid IPv6 format>  DNS server 2 IP address
<A.B.C.D>|<valid IPv6 format>  DNS server 3 IP address

ise/admin(config)# ip name-server
```

例 2

IP ネーム サーバーを設定した後に、次の出力が表示されます。

```
ise/admin# show run | in name-server
ip name-server 10.0.0.1 10.0.1.1
3201:db8:0:20:f41d:eee:7e66:4eba
ise/admin#
```

例 3

```
ise/admin(config)# ip name-server ?
ip name-server 10.126.107.120 10.126.107.107 10.106.230.244
DNS Server was modified. If you modified this setting for AD connectivity, you must
restart ISE for the change to take effect.
Do you want to restart ISE now? (yes/no)
```

ip route

スタティックルートを設定するには、コンフィギュレーション モードで **ip route** コマンドを使用します。スタティックルートを削除するには、このコマンドの **no** 形式を使用します。

ip route *prefix mask* **gateway** *ip-address*

no ip route *prefix mask*

構文の説明

prefix	宛先の IP ルート プレフィックス。
mask	宛先のプレフィクス マスク。
ip-address	ネットワークに到達するために使用可能なネクスト ホップの IP ス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

スタティック ルートは手動で設定されます。これによって、柔軟性が低くなります（ネットワーク トポロジの変更に動的に適応できません）が、安定性は非常に高くなります。スタティック ルートは、ルーティング アップデートを送信することなく維持できるため、帯域幅の使用率を最適化できます。また、ルーティング ポリシーの実施が容易になります。

ip route コマンドは個々の Cisco ISE ノードでのスタティックルートの定義に使用できるだけでなく、各インターフェイスのデフォルトルートを定義して、マルチインターフェイス IP ノードに固有の非対称 IP 転送の影響を軽減するために拡張されます。

単一のデフォルト ルートがマルチインターフェイス ノードに設定されている場合、ノードのいずれかの IP インターフェイスから受信したすべての IP トラフィックは、非対称 IP 転送を生成するデフォルト ゲートウェイのネクストホップにルーティングされます。Cisco ISE ノードに複数のデフォルト ルートを設定すると、非対称転送の影響がなくなります。

次の例に、複数のデフォルト ルートを設定する方法を示します。

Cisco ISE ノード eth0、eth1、eth2、および eth3 インターフェイスの次のインターフェイス設定についてそれぞれ考えてみてください。

```
ISE InterfaceIPNetworkGateway
192.168.114.10 192.168.114.0 192.168.114.1
192.168.115.10 192.168.115.0 192.168.115.1
192.168.116.10 192.168.116.0 192.168.116.1
192.168.117.10 192.168.117.0 192.168.117.1
```

ip route コマンドは、ここでは各インターフェイスのデフォルトルートを定義するために使用されます。

```
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.114.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.115.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.116.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.117.1
ise/admin(config)# ip default-gateway 192.168.118.1
```

（注） 上記の「ip default-gateway」は、すべてのインターフェイスのラスト リゾートのルートです。

show ip route コマンドでは、**ip route** コマンドを使用して作成したスタティックルート（デフォルトルートとデフォルト以外のルート）、および「ip default gateway」コマンドの使用により設定されたルートを含むシステムによって作成されたルートの出力が表示されます。これは、各ルートの発信インターフェイスを表示します。

（注） インターフェイスの IP アドレスを変更した場合、到達不能なゲートウェイのためにいずれかのスタティック ルートが到達不能になると、そのスタティック ルートは実行コンフィギュレーションから削除されます。到達不能になったルートはコンソールに表示されます。

例 2

```
ise/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ise/admin(config)#
```

ipv6 address

IPv6の一般的なプレフィックスに基づいてスタティックIPv6アドレスを設定し、インターフェイスでIPv6処理を有効にするには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。

ipv6 address *ipv6-address/prefix-length*

IPv6アドレスを削除するか、IPv6処理を無効にするには、このコマンドの **no** 形式を使用します。

no ipv6 address *ipv6-address/prefix-length*

構文の説明

ipv6-address	IPv6 アドレス。
prefix-length	IPv6プレフィックスの長さ。プレフィックス（アドレスのネット部分）を構成するアドレスの上位連続ビット数を示す 0 ～ 128 の数値です。10 進値の前にスラッシュ記号を付ける必要があります

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、IPv6 アドレスを設定する前にディセーブルにしてください。IPv6 アドレスの設定後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切り表記（IPv4 マッピングおよび IPv4 互換の IPv6 アドレス）：::ffff:192.0.2.128 など

fe80 プレフィックスを使用してリンクローカル アドレスを割り当てます。インターフェイスにグローバル アドレスを割り当てると、リンクローカル アドレスが自動的に作成されます。

（注） IPv6 アドレスを変更する場合、**ipv6 address** コマンドでの CLI 設定変更中に Ctrl+C を押すと、システムの一部のアプリケーション コンポーネントは古い IPv6 アドレスを使用し、他のコンポーネントは新しい IPv6 アドレスを使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の **ipv6 address** コマンドを実行して IPv6 アドレスを目的の値に設定します。

例 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address 2001:DB8:0:1::/64
Changing the IPv6 address may result in undesired side effects on any installed
application(s).
Are you sure you want to proceed? Y/N[N]: y
........
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify
all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

例 2

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address fe80::250:56ff:fe87:4763/64
ise/admin(config-GigabitEthernet)#
```

ipv6 address autoconfig

インターフェイスのステートレス自動設定を使用した IPv6 アドレスの自動設定を有効にし、インターフェイスで IPv6 処理を有効にするには、インターフェイス コンフィギュレーション モードで **ipv6 address autoconfig** コマンドを使用します。

IPv6 アドレス自動設定は、Linux ではデフォルトでイネーブルです。Cisco ADE 2.0 は、イネーブルになっている任意のインターフェイスの実行コンフィギュレーションで IPv6 アドレス自動設定を示します。

ipv6 address autoconfig

インターフェイスで IPv6 アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

IPv6 ステートレス自動設定には、予測可能な IP アドレスを持つというセキュリティ面の落とし穴があります。この落とし穴は、プライバシーの拡張によって解決されます。**show interface** コマンドを使用して、プライバシー機能拡張が有効になっていることを確認できます。

例

```
ise/admin(config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)#
```

IPv6 自動設定の設定

IPv6 ステートレス自動設定を有効にするには、インターフェイス コンフィギュレーション モードで **interface GigabitEthernet 0** コマンドを使用します。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config)# (config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)# (config-GigabitEthernet)# end
ise/admin#
```

IPv6 自動設定がイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 0
```

```
  ip address 172.23.90.116 255.255.255.0
  ipv6 address autoconfig
!
```

インターフェイス設定を表示するには、**show interface GigabitEthernet 0** コマンドを使用できます。次の例では、インターフェイスに 3 個の IPv6 アドレスがあることを確認できます。最初のアドレス（3ffe 以降）は、ステートレス自動設定を使用して取得されます。

ステートレス自動設定を実行するには、そのサブネット上で IPv6 ルート アドバタイズメントをイネーブルにする必要があります。次のアドレス（fe80 で始まるアドレス）は、ホストの外部からのスコープを持たないリンク ローカル アドレスです。

IPv6 自動設定か DHCPv6 設定かに関係なく、リンク ローカル アドレスは常に表示されます。最後のアドレス（2001 以降）は、IPv6 DHCP サーバーから取得されます。

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

プライバシー拡張機能の確認

show interface GigabitEthernet 0 コマンドを使用して、プライバシー機能拡張が有効になっていることを確認できます。2 つの自動設定アドレスが表示されます。1 つのアドレスはプライバシー拡張なしで、もう 1 つはプライバシー拡張ありです。

次の例では MAC は 3ffe:302:11:2:20c:29ff:feaf:da05/64 で、非 RFC3041 アドレスには MAC が含まれています。プライバシー拡張アドレスは 302:11:2:9d65:e608:59a9:d4b9/64 です。

出力は次のように表示されます。

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:9d65:e608:59a9:d4b9/64 Scope:Global
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9430102 (8.9 MiB)  TX bytes:466204 (455.2 KiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

ipv6 address dhcp

IPv6（DHCPv6）サーバーの Dynamic Host Configuration Protocol からインターフェイス上に IPv6 アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address dhcp

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

例

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address dhcp
ise/admin(config-GigabitEthernet)# end
ise/admin#
```

IPv6 DHCP がイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 1
  ipv6 address dhcp
  ipv6 enable
!
```

（注） IPv6 ステートレス自動設定および IPv6 アドレス DHCP は相互に排他的ではありません。同じインターフェイスに IPv6 ステートレス自動設定および IPv6 アドレス DHCP の両方を指定できます。

どの IPv6 アドレスが特定のインターフェイスで使用されているかを表示するには、**show interface** コマンドを使用します。

IPv6 ステートレス自動設定および IPv6 アドレス DHCP の両方がイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 1
    ipv6 address dhcp
```

```
    ipv6 address autoconfig
    ipv6 enable
!
```

ipv6 enable

インターフェイス上の IPv6 を有効にするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。

ipv6 enable

インターフェイスで GVRP を無効にするには、このコマンドの **no** 形式を使用します。

no ipv6 enable

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイスで IPv6 を有効化し、インターフェイス MAC アドレスに基づいてリンクローカルアドレスを自動生成する場合に使用します。

例 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 enable
ise/admin(config-GigabitEthernet)#
```

例 2

デフォルトでは、ipv6が、すべてのインターフェイスで有効になっています。これを無効にするには、このコマンドの **no** 形式を使用します。

```
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet6 fe80::20c:29ff:fe83:a610 prefixlen 64 scopeid 0x20 link
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 11766 bytes 1327285 (1.2 MiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 6 bytes 508 (508.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 1
ise/admin(config-GigabitEthernet)# no ipv6 enable
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# end
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163 UP,BROADCAST,RUNNING,MULTICAST mtu 1500
```

```
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 64 bytes 5247 (5.1 KiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 3 bytes 258 (258.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ipv6 route

IPv6 スタティックルートを手動で設定し、2 台のネットワーキングデバイス間の明示的なパスを定義するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。スタティック ルートは自動的に更新されないので、ネットワーク トポロジが変化した場合は手動でスタティック ルートを再設定する必要があります。

ipv6 route *ipv6-address/prefix-length* **gateway** *route-specific gateway*

IPv6 スタティックルートを削除するには、このコマンドの **no** 形式を使用します。

no ipv6 route *ipv6-address/prefix-length* **gateway** *route-specific gateway*

IPv6 アドレスを指定してデフォルト スタティック ルートを設定するには、グローバル コンフィギュレーション モードで **ipv6 route ::/0 gateway** *route-specific gateway* コマンドを使用します。IPv6 アドレスを指定してデフォルト スタティック ルートを無効にするには、このコマンドの **no** 形式を使用します。

構文の説明

ipv6-address	IPv6 アドレス。
prefix-length	IPv6プレフィックスの長さ。プレフィックス（アドレスのネット部分）を構成するアドレスの上位連続ビット数を示す 0 ～ 128 の数値です。10 進値の前にスラッシュ記号を付ける必要があります
route-specific gateway	そのネットワークに到達するために使用できるネクスト ホップアドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切り表記（IPv4 マッピングおよび IPv4 互換の IPv6 アドレス）：::ffff:192.0.2.128 など

show ipv6 route コマンドは、設定済みの IPv6 ルートを表示する場合に使用します。

例 1

```
ise/admin(config)# ipv6 route 2001:DB8:cc00:1::/64 gateway 2001:DB8::cc00:1::1
```

例 2

```
ise/admin(config)# ipv6 route ::/0 gateway 2001:db::5
```

::/0 はデフォルト ルート プレフィックスを示します。

kron occurrence

1 つ以上のコマンド スケジューラ コマンドが特定の日時または一定間隔で実行されるようにスケジューリングするには、コンフィギュレーション モードで **kron occurrence** コマンドを使用します。このスケジュールを削除するには、このコマンドの **no** 形式を使用します。

kron occurrence *occurrence-name*

構文の説明

occurrence	コマンド スケジューラ コマンドをスケジューリングします。
occurrence-name	オカレンスの名前。80 文字までの英数字で指定します。（次の「構文の説明」を参照）。

（注） **kron occurrence** コマンドで *occurrence-name* を入力すると、config-Occurrence コンフィギュレーション サブモードが開始されます（次の「構文の説明」を参照）。

構文の説明

at	指定した日時にオカレンスが実行されるように指定します。使用 at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*]
do	EXEC コマンド。このモードで EXEC コマンドを実行できます。
end	kron-occurrence コンフィギュレーション サブモードを終了し、E モードに戻ります。
exit	kron-occurrence コンフィギュレーション モードを終了します。
no	このモードのコマンドを否定します。 3 つのキーワードを使用できます。 • at：使用方法：at [hh:mm] [day-of-week | day-of-month | month day-of-month] • policy-list：オカレンスによって実行されるポリシー リストを ます。80 文字までの英数字で指定します。 • recurring：ポリシー リストの実行を繰り返します。
policy-list	オカレンスによって実行されるコマンド スケジューラ ポリシー を指定します。
recurring	繰り返して実行するオカレンスを指定します。 （注） kron occurrence を繰り返して実行しない場合、スケジ 設定されたバックアップの kron occurrence コンフィギ ションは実行後に削除されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config-Occurance）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

kron occurrence および **policy-list** コマンドを使用して、1 つ以上のポリシーリストが同じ時間または間隔で実行されるようにスケジューリングします。

EXEC CLI コマンドを含むコマンド スケジューラ ポリシーを作成して、指定した時刻に Cisco ISE サーバーで実行されるようにスケジューリングするには、**cli** コマンドとともに **kron policy-list** コマンドを使用します。

（注） **kron** コマンドを実行すると、一意の名前（タイムスタンプの追加により）でバックアップバンドルが作成されるため、ファイルが互いに上書きされることはありません。

（注） **Administration > System > Backup and Restore** ページを使用して、GUI を介して設定またはモニターリングのバックアップをスケジューリングすることを推奨します。

例 1：週次バックアップ

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

例 2：日次バックアップ

```
ise/admin(config)# kron occurrence DailyBackup
ise/admin(config-Occurrence)# at 02:00
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

例 3：週次バックアップ

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# no recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

kron policy-list

コマンド スケジューラ ポリシーの名前を指定し、kron-Policy List コンフィギュレーション サブモードを開始するには、コンフィギュレーション モードで **kron policy-list** コマンドを使用します。コマンド スケジューラ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

kron policy-list *list-name*

構文の説明

policy-list	コマンド スケジューラ ポリシーの名前を指定します。
list-name	ポリシー リストの名前。最大 80 文字の英数字をサポートします

（注） **kron policy-list** コマンドで list-name を入力すると、config-Policy List コンフィギュレーション サブモードが開始されます（次の「構文の説明」を参照）。

構文の説明

cli	スケジューラによって実行されるコマンド。最大 80 文字の英数ポートします。
do	EXEC コマンド。このモードで EXEC コマンドを実行できます。
end	config-Policy List コンフィギュレーション サブモードを終了し、モードに戻ります。
exit	このサブモードを終了します。
no	このモードのコマンドを否定します。次の 1 つのキーワードが使です。 • cli：スケジューラによって実行されるコマンド。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config-Policy List）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

EXEC CLI コマンドを含むコマンド スケジューラ ポリシーを作成して、指定した時刻に ISE サーバーで実行されるようにスケジューリングするには、**cli** コマンドとともに **kron policy-list** コマンドを使用します。**kron occurrence** および **policy list** コマンドを使用して、1 つ以上のポリシーリストが同じ時間または間隔で実行されるようにスケジューリングします。

（注） **kron policy-list** コマンドを使用して、CLI から設定および動作データのバックアップをスケジューリングすることはできません。Cisco ISE 管理者ポータルからこれらのバックアップをスケジューリングできます。

例

```
ise/admin(config)# kron policy-list BackupLogs
ise/admin(config-Policy List)# cli backup-logs ScheduledBackupLogs repository
SchedBackupRepo encryption-key plain xyzabc
ise/admin(config-Policy List)# exit
ise/admin(config)#
```

logging

ログレベルを設定するには、コンフィギュレーション モードで **logging** コマンドを使用します。

logging loglevel {*0* | *1* | *2* | *3* | *4* | *5* | *6* | *7*}

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no logging

構文の説明

loglevel	logging コマンドのログ レベルを設定するコマンド。
0 ～ *7*	ログ メッセージをセットする目的のプライオリティ レベル。プリティ レベルは以下のとおりです（キーワードの番号を入力）。 • 0-emerg（緊急事態）：システムが使用不可。 • 1-alert（アラート）：ただちに処置が必要。 • 2-crit（クリティカル）：クリティカルな状態。 • 3-err（エラー）：エラー状態。 • 4-warn（警告）：警告状態。 • 5-notif（通知）：正常であるが、重要な状態。 • 6-inform：（デフォルト）情報メッセージ。 • 7-debug：デバッグ メッセージ。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

このコマンドには **loglevel** キーワードが必要です。

例

```
ise/admin(config)# logging loglevel 0
ise/admin(config)#
```

max-ssh-sessions

分散展開のノードごとにコマンドライン インターフェイス（CLI）の最大同時セッション数を設定するには、コンフィギュレーション モードで **max-ssh-sessions** コマンドを使用します。

max-ssh-sessions {*0* | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10*}

構文の説明

1 ～ *10*	同時 SSH セッションの数。デフォルトは 5 です。

コマンド デフォルト

許可される最大同時 CLI セッション数のデフォルトは、Cisco ISE 管理者ポータルから 5 に設定されます。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

max-ssh-sessions パラメータはコマンドライン インターフェイスから設定可能ではありません。アクティブ CLI セッションの最大数は、プライマリ管理 ISE 管理者ポータルから複製されます。

CLI セッションの最大数を超えると、このセッションを閉じているコマンドライン インターフェイスに「最大アクティブ SSH セッション数に到達（Maximum active ssh sessions reached）」メッセージが表示され、下部に「未接続：続行するには Enter または Space を押します（Not connected - press Enter or Space to connect）」というメッセージが表示されます。

コンソールから CLI にログインして **forceout username** コマンドを使用すると、ユーザーをログアウトさせてアクティブな SSH セッションの数を削減できます。

コマンドライン インターフェイス（CLI）セッションの最大数を設定するためのナビゲーション パスは、Cisco ISE 管理者ポータルの [セッション（Session）] タブの次の場所にあります。**[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [アクセス（Access）]**。

ntp

NTP 設定を指定するには、**authentication-key**、**maxdistance**、および **server** コマンドと共にコンフィギュレーション モードで **ntp** コマンドを使用します。

ntp authentication-key <*key id*> <*authentication key encryption type*> **hash** | **plain** <*key value*>

ntp maxdistance <*maximum distance*>

ntp reselectdistance <*reselect distance*>

ntp server {*ip-address* | *hostname*} *key* <*peer key number*>

no ntp server

構文の説明

authentication-key	信頼できる時刻源の認証キーを指定します。
maxdistance	拒否されない送信元の最大許容ルート距離です。デフォルトでは ISE に設定されている最大ルート距離は 16 秒です。
reselectdistance	現在選択されていない送信元の固定距離。デフォルトの固定距離 マイクロ秒です。
server	使用する NTP サーバーを指定します。

コマンド デフォルト

なし

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ntp コマンドを使用して NTP 設定を指定します。

デバイスの NTP サービスを終了するには、**authentication-key**、**maxdistance** 、**server** などのキーワードや引数を指定して **no ntp** コマンドを入力する必要があります。たとえば、以前に **ntp server** コマンドを実行した場合は、**server** とともに **no ntp** コマンドを使用します。

例

```
ise/admin(config)# ntp ?
  authentication-key  Authentication key for trusted time sources
  maxdistance         Maximum allowed root distance of the sources to not be rejected
  reselectdistance    Fixed distance for sources that are currently not selected
  server              Specify NTP server to use
ise/admin(config)#
ise/admin(config)# no ntp server
ise/admin(config)# do show ntp
% no NTP servers configured
ise/admin(config)#
```

```
ise/admin(config)# ntp reselectdistance ?
  <1-10000000>  Reselect distance in microseconds
ise/admin(config)# ntp reselectdistance 3000
```

ntp authentication-key

時間源の認証キーを指定する場合は、コンフィギュレーション モードで一意の識別子およびキー値を指定して **ntp authentication-key** コマンドを使用します。

ntp authentication-key <*key id*> **md5 hash | plain** *key value*

ntp authentication-key <*key id*> **sha1 hash | plain** *key value*

ntp authentication-key <*key id*> **sha256 hash | plain** *key value*

ntp authentication-key <*key id*> **sha512 hash | plain** *key value*

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ntp authentication-key

構文の説明

authentication-key	信頼できる時刻源の認証キーを設定します。
key id	このキーに割り当てる識別子。1 から 65535 までの数値がサポーます。
md5	認証キーの暗号化タイプ。
sha1	認証キーの暗号化タイプ。
sha256	認証キーの暗号化タイプ。
sha512	認証キーの暗号化タイプ。
hash	認証のハッシュされたキー。暗号化タイプに続けて、暗号化されたシュされた）キーを指定します。4112 までの長さで指定します。
plain	認証用のプレーンテキストのキー。暗号化タイプに続けて、暗号ていないプレーンテキスト キーを指定します。1028 までの長さします。
key value	上記の <*authentication key encryption type*>**plain** | **hash** のいずれかする形式のキー値。 （注） 16 進数のキー値はプレフィックス **HEX:** で追加でき

コマンド デフォルト

なし

コマンド モード

コンフィギュレーション（config）#。

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ntp authentication-keyコマンドを使用して、NTP 認証の認証キーとともに時刻源を設定し、それに関連するキー ID、キー暗号化タイプ、およびキー値設定を指定します。このキーを信頼できるリストに追加してから **ntp server** コマンドに追加します。

信頼リストに追加されている NTP 認証キーのない時刻源は同期されません。

（注） **show running-config** コマンドはセキュリティのためにハッシュ形式に変換される Message Digest 5（MD5）プレーン 形式に入力されたキーを常に示します。たとえば、**ntp authentication-key** 1 **md5 hash** *ee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3* です。

例 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 ?
  md5     MD5 authentication
  sha1    SHA1 authentication
  sha256  SHA256 authentication
  sha512  SHA512 authentication
```

例 2

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 sha1 plain ?
  <WORD>  Plain text or hexadecimal number with the HEX: prefix key for a (Max Size -
1028)
```

例 3

```
ise/admin(config)# no ntp authentication-key 3
(Removes authentication key 3.)
```

例 4

```
ise/admin(config)# no ntp authentication-key
(Removes all authentication keys.)
```

ntp maxdistance

ntp maxdistance コマンドは、送信元選択アルゴリズムによって拒否されない送信元の最大許容ルート距離を設定します。この距離には、送信元が同期されなくなったときに大きくなる可能性のある累積分散と、プライマリ送信元への総ラウンドトリップ遅延の半分が含まれます。

デフォルトでは、Cisco ISE に設定されている最大ルート距離は 16 秒です。

デフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ntp maxdistance

構文の説明

maxdistance	拒否されない送信元の最大許容ルート距離です。

コマンド デフォルト

なし

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

maxdistance を大きな値に設定すると、送信元への接続が非常にまれであり、クロックの更新の間で大きな分散を蓄積できるサーバーとの同期を可能にするのに役立ちます。

例

```
ise/admin(config)# ntp maxdistance ?
     <1-128>
```

ntp server

NTP サーバーによるシステムのソフトウェアクロックの同期を許可するには、コンフィギュレーション モードで **ntp server** コマンドを使用します。それぞれ別個の行にキーを指定した最大 3 台のサーバーを許可します。キーはオプション パラメータですが、NTP 認証にはキーが必要です。

Cisco ISE には、常に有効で到達可能な NTP サーバーが必要です。

キーはオプション パラメータですが、NTP サーバーを認証する必要がある場合は、キーを設定する必要があります。

この機能を無効にするには、NTPサーバーを削除して別のサーバーを追加する場合のみ、このコマンドの **no** 形式を使用します。

ntp server {*ip-address* | *hostname*} **minpoll** <*minimum poll*> **key**<*peer key number*>

ntp server {*ip-address* | *hostname*} **trust**

構文の説明

server	システムによって、指定されたサーバーと同期されます。
ip-address | *hostname*	クロック同期を提供するサーバーの IPv4 または IPv6 アドレスト名。引数は 255 文字までの英数字で指定します。IPv6 アNTP サーバーを追加する場合は、ISE eth0 インターフェイスがレスで静的に設定されていることを確認してください。
key	（任意）。ピアのキー番号。最大 65535 桁までサポートしま このキーは、 **ntp authentication-key** コマンドを使用して、信キーとして追加する必要があります。 認証を実行するために、キーとキーの値は実際の NTP サーバされているキーと同じ値にする必要があります。
minpoll	2 の累乗秒としてサーバに送信される要求の最小間隔です。**minpoll 5** は、ポーリング間隔が 32 秒未満にならないというします。デフォルトは 6（64 秒）、最小値は -6（1/64 秒）、24（6 ヵ月）です。
trust	この送信元からの時間が常に真であると仮定します。

（注） *key* と **minpoll** オプションは交換可能です。

コマンド デフォルト

デフォルトで設定されているサーバーはありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

show ntp コマンドは同期の状態を表示します。設定されたいずれの NTP サーバーも到達可能ではなく、認証されていない場合（NTP認証が設定されている場合）、このコマンドによって最小のストラタムを持つローカルへの同期が表示されます。

NTPサーバーが到達可能ではないか、適切に認証されていない場合、このコマンド統計についての到達度はゼロになります。

（注） このコマンドは、同期プロセス時に矛盾した情報を表示します。同期プロセスは、完了までに最大 20 分かかることがあります。

例

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# ntp server 209.165.200.225 ?
  key            Peer key number
  minpoll        Minimum interval between requests sent to the server
trust        Assume time from this source is always true


ise/admin# show running-config
interface GigabitEthernet 0
  ip address 209.165.200.225 255.255.255.0
  ipv6 address autoconfig
  ipv6 enable
!
ip name-server 209.165.200.226
!
ip default-gateway 209.165.200.227
!
ip route 2.2.2.0 255.255.255.0 gateway 127.0.0.1
!
!
clock timezone Asia/Kolkata
!
ntp authentication-key nn md5 hash xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

ntp server 209.165.200.228 key nn
ntp server 209.165.200.229
!


ise/admin(config)# ntp server 209.165.200.225 trust
ise/admin(config)# ntp server 209.165.200.225 key 2 trust
ise/admin(config)# ntp server 209.165.200.225 key 2 minpoll 7 trust
ise/admin(config)# ntp server 209.165.200.225 minpoll 7 trust
ise/admin(config)# ntp server 209.165.200.225 minpoll 7 key 2 trust
```

同期化のステータスの確認

同期のステータスを確認するには、**show ntp** コマンドを使用します。

例 1

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.80
Tertiary NTP : 171.68.10.150
synchronised to local net at stratum 11
   time correct to within 448 ms
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.          10 l   46   64   37    0.000    0.000   0.001
 171.68.10.80    .RMOT.          16 u   46   64    0    0.000    0.000   0.000
 171.68.10.150   .INIT.          16 u   47   64    0    0.000    0.000   0.000
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

例 2

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP : 171.68.10.80
synchronised to NTP server (171.68.10.150) at stratum 3
   time correct to within 16 ms
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l   35   64  377    0.000    0.000   0.001
+171.68.10.80    144.254.15.122   2 u   36   64  377    1.474    7.381   2.095
*171.68.10.150   144.254.15.122   2 u   33   64  377    0.922   10.485   2.198
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

rate-limit

送信元IPアドレスからのTCP、UDP、またはICMPパケットの制限を設定するには、コンフィギュレーション モードで **rate-limit** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

rate-limit name 250 ip-address net-mask port

構文の説明

name	設定しているレート制限の名前。
<1-10000>	1 秒あたりの TCP、UDP、または ICMP パケットの平均数。
ip-address ***ip*** または ***ipv6***	パケットレート制限を適用する必要がある送信元 IP アドレス。IP アドレスの場合は **ip**、IPv6 アドレスの場合は **ipv6** と入力します。
net-mask	パケットレート制限を適用する必要がある送信元 IP マスク。
port	パケットレート制限を適用する必要がある宛先ポート番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。
3.2	レート制限CLI応答に、丸められたレート制限値が表示されなくした。ただし、Netfilter では引き続き、実装時にレート制限値をす。

使用上のガイドライン

設定されている実際のレート制限は、Netfilter のハッシュ制限設計により、設定した数と異なる場合があります。以下に、このドキュメントの作成時点での、Netfilter によるレート制限値の丸め方を一覧表示しています。

- 制限値が 5001/s から 10000/s の場合、Netfilter では値が 10000/s に切り上げられます。
- 制限値が 3334/s から 5000/s の場合、Netfilter では値が 5000/s に切り上げられます。
- 制限値が 2501/s から 3333/s の場合、Netfilter では値が 3333/s に切り上げられます。
- 制限値が 2001/s から 2500/s の場合、Netfilter では値が 2500/s に切り上げられます。
- 制限値が 1667/s から 2000/s の場合、Netfilter では値が 2000/s に切り上げられます。

- 制限値が 1429/s から 1666/s の場合、Netfilter では値が 1666/s に切り上げられます。
- 制限値が 1251/s から 1428/s の場合、Netfilter では値が 1428/s に切り上げられます。
- 制限値が 1112/s から 1250/s の場合、Netfilter では値が 1250/s に切り上げられます。
- 制限値が 1001/s から 1111/s の場合、Netfilter では値が 1111/s に切り上げられます。
- 制限値が 910/s から 1000/s の場合、Netfilter では値が 1000/s に切り上げられます。
- 制限値が 834/s から 909/s の場合、Netfilter では値が 909/s に切り上げられます。
- 制限値が 150 未満の場合、丸めは行われません。

ハッシュ制限の動作の詳細については、Netfilter のドキュメントを参照してください。

レート制限名に割り当てられた値を更新するには、rate-limit コマンドの no 形式を使用してから、レート制限を再定義します。

例

```
ise242/admin(config)#rate-limit limit1 5500 port 6543
ise242/admin(config)#do show running-config | include rate
rate-limit limit1 5500 port 6543
```

password-policy

（注） Cisco ISE GUI からパスワードポリシーを設定することもできます。Cisco ISE GUI を介して設定されたパスワードポリシーは、Cisco ISE CLI を介して設定されたパスワードポリシーを上書きし、このポリシーより優先されます。

システムに対するパスワードをイネーブル化または設定するには、コンフィギュレーション モードで **password-policy** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

password-policy *options*

（注） **password-policy** コマンドには、ポリシー オプションが必要です（「構文の説明」を参照）。**password-expiration-enabled** コマンドは、他の password-expiration コマンドの前に入力する必要があります。

（注） **password-policy** コマンドを入力すると、config-password-policy コンフィギュレーション サブモードに入ります。

構文の説明

digit-required	ユーザー パスワードに数字を含むことを必須にします。
disable-cisco-password	パスワードに、「Cisco」や「Cisco」を含む語を使用できないよ ます。
disable-repeat-chars	同じ文字が 5 つ以上含まれているパスワードをディセーブルにし
do	EXEC コマンド。
end	コンフィギュレーション モードを終了します。
exit	このサブモードを終了します。
lower-case-required	ユーザー パスワードに小文字が含まれている必要があります。
min-password-length	有効なパスワードの最小文字数。40 文字までで指定します。
No	コマンドを無効にするか、そのデフォルトに設定します。
no-previous-password	前回のパスワードの一部を再使用できないようにします。
no-username	パスワードにユーザ名を含めることを禁止します。

password-delta	文字数が古いパスワードと異なるようにします。
password-expiration-days	パスワードの有効日数。3650 までの整数をサポートします。
password-expiration-enabled	パスワードの有効期限をイネーブルにします。 （注） **password-expiration-enabled** コマンドは、他の password-expiration コマンドの前に入力する必要があ
password-expiration-warning	パスワードの期限が迫っていることを通知する警告を開始す 数。3650 までの整数をサポートします。
password-lock-enabled	指定した回数の試行が失敗したら、パスワードをロックしま
password-lock-retry-count	試行回数を指定します。この回数の試行が失敗するとユーザー ドがロックされます。20 までの整数をサポートします。
password-lock-timeout	アカウント ロックアウトをクリアするまでの時間を設定しま 位）。5 分から 1440 分までの時間値をサポートします。
special-required	ユーザー パスワードに特殊文字が含まれている必要がありま
upper-case-required	ユーザー パスワードに大文字が含まれている必要があります

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config-password-policy）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

なし

例

```
ise/admin(config)# password-policy
ise/admin(config-password-policy)# password-expiration-days 30
ise/admin(config-password-policy)# exit
ise/admin(config)#
```

repository

バックアップを設定するためにリポジトリサブモードを開始するには、コンフィギュレーション モードで **repository** コマンドを使用します。

repository *repository-name*

構文の説明

repository-name	リポジトリの名前。最大 80 文字の英数字をサポートします。

（注） **repository** コマンドでリポジトリの名前を入力すると、config-Repository コンフィギュレーション サブモードが開始されます（「構文の説明」を参照）。

構文の説明

do	EXEC コマンド。このモードですべての EXEC コマンドを実行です。
end	config-Repository サブモードを終了し、EXEC モードに戻ります。
exit	このモードを終了します。
no	このモードのコマンドを否定します。 次の 2 つのキーワードを使用できます。 • url：リポジトリの URL。 • user：リポジトリにアクセスするためのユーザー名とパスワ
url	リポジトリの URL。最大 300 文字の英数字をサポートします（表参照）。
user	アクセスするためのユーザー名とパスワードを設定します。ユーには最大 30 文字の英数字、パスワードには最大 15 文字の英数字できます。 パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|#、$、%、^、&、*、(、)、+、および = です。

（注） server はサーバー名です。path は /subdir/subsubdir を指します。NFS ネットワーク サーバーのサーバー名の後には、コロン（:）が必要です。

表 *5 :* 表 *4-5 URL* キーワード（続き）

キーワード	コピー元またはコピー先
URL	サーバーおよびパス情報を含む、リポジトリの URL を入力し 大 80 文字の英数字をサポートします。
cdrom:	ローカルの CD-ROM ドライブ（読み取り専用）。
disk:	ローカル ストレージ。 ローカルリポジトリ内のすべてのファイルを表示するには、 **repository** を実行します。 （注） すべてのローカル リポジトリは、/localdisk パーテ に作成されます。リポジトリの URL で disk:// を指定 システムは、/localdisk に対する相対パスでディレ 作成します。たとえば、**disk://backup,** と入力する レクトリは /localdisk/backup に作成されます。
ftp:	FTP ネットワーク サーバーのコピー元またはコピー先の URL ftp://server/path という URL を使用します。
http:	HTTP ネットワーク サーバーのコピー元またはコピー先の UR り専用）。
https:	HTTPS ネットワーク サーバーのコピー元またはコピー先の U 取り専用）。
nfs:	NFS ネットワーク サーバーのコピー元またはコピー先の URL nfs://server:/path という URL を使用します。
sftp:	SFTP ネットワーク サーバーのコピー元またはコピー先の UR sftp://server/path という URL を使用します。
tftp:	TFTP ネットワーク サーバーのコピー元またはコピー先の UR tftp://server/path という URL を使用します。 （注） Cisco ISE アップグレードの実行に、TFTP リポジト できません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config-Repository）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

サブモードで **url sftp:** を設定する場合は、最初に RSA フィンガープリント（AKA host-key）をターゲット SFTP ホストから ISE にロードする必要があります。これを行うには、CLI で **crypto host_key add** コマンドを使用します。詳細については、crypto コマンドを参照してください。

この機能を無効にするには、EXEC モードで **crypto host_key delete** コマンドを使用します。

Cisco ISE 管理者ポータルの [管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [リポジトリ（Repository）] > [リポジトリの追加（Add Repository）] でセキュアな FTP リポジトリを設定すると Cisco ISE は常に次の警告を表示します。

このリポジトリを使用できるようにするには、SFTP サーバーのホスト キーをホスト キー オプションを使用して CLI を介して追加する必要があります。

ホスト キーを設定せずに、セキュアな FTP リポジトリにバックアップしようとすると、対応するエラーが Cisco ADE のログにスローされます。

（注） Cisco ISE は、FIPS モードが ISE で有効になっていない場合でも、FIPS モードで発信 SSH または SFTP 接続を開始します。ISE と通信するリモート SSH または SFTP サーバーが FIPS 140-2 承認暗号化アルゴリズムを許可していることを確認します。

Cisco ISE では、組み込みの FIPS 140-2 の検証済み暗号化モジュールが使用されています。FIPS コンプライアンスの要求の詳細については、『FIPS Compliance Letter』を参照してください。

service

管理するサービスを指定するには、コンフィギュレーション モードで **service** コマンドを使用します。

service sshd

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no service

構文の説明

sshd	Secure Shell Daemon。SSH のデーモン プログラムです。
enable	sshd サービスをイネーブルにします。
encryption-algorithm	SSH暗号化アルゴリズムを設定します。サポートされている ムは、a、aes128-cbc、aes128-ctr、aes256-cbc、および aes256-
encryption-mode	システムで SSH 暗号化モードを設定します。サポートされて ドは、cbc と ctr です。
key-exchange-algorithm	sshd サービスで許可するキー交換アルゴリズムを指定します
diffie-hellman-group14-sha1	キー交換アルゴリズムを diffie-hellman-group14-sha1 に制限し
Loglevel	sshd からセキュア システム ログに対するメッセージのログ 定します。 • 1：抑止 • 2：致命的 • 3：エラー • 4：情報（デフォルト） • 5：冗長 • 6：デバッグ • 7：デバッグ 1 • 8：デバッグ 2 • 9：デバッグ 3

PubkeyAuthentication	ユーザーの秘密キーを使用してユーザー認証を行うように指定し （注） インストール前に ZTP 構成イメージファイルに公開キ 含めていない場合は、**service sshd PubkeyAuthenticat** マンドを実行しないでください。このコマンドを実行 と、パスワードベースの認証が無効になり、Cisco ISE 密キーを使用してログインすると想定します。この問 発生した場合は、コンソールポートを使用して Cisco ログインし、設定を元に戻す必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。
3.2	**PubkeyAuthentication** キーワードが追加されました。

使用上のガイドライン

なし

例

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd encryption-algorithm
 Configure aes128-cbc algo
 Configure aes128-ctr algo
 Configure aes256-cbc algo
 Configure aes256-ctr algo
ise/admin(config)# service sshd encryption-mode
 Configure cbc cipher suites
 Configure ctr cipher suites
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd encryption-algorithm
 Configure aes128-cbc algo
 Configure aes128-ctr algo
 Configure aes256-cbc algo
 Configure aes256-ctr algo
ise/admin(config)# service sshd encryption-mode
 Configure cbc cipher suites
 Configure ctr cipher suites
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

公開キー認証を有効にする方法：

```
ise/admin(config)# service sshd PubkeyAuthentication
```

公開キー認証を無効にする方法：

```
ise/admin(config)# no service sshd PubkeyAuthentication
```

shutdown

インターフェイスをシャットダウンするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config-GigabitEthernet）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用してインターフェイスをシャットダウンすると、そのインターフェイスを経由した Cisco ISE アプライアンスへの接続性が失われます。これは、アプライアンスの電源が投入されていても変わりません。

ただし、アプライアンス上に別の IP を使用して 2 番目のインターフェイスを設定し、そのインターフェイスがシャットダウンされていなければ、その 2 番目のインターフェイス経由でアプライアンスに接続できます。

インターフェイスをシャットダウンする別の方法として、ONBOOT パラメータを使用して、/etc/sysconfig/network-scripts にある ifcfg-eth[0,1] ファイルを変更することもできます。

- インターフェイスをディセーブルにするには、ONBOOT="no" と設定します。
- インターフェイスをイネーブルにするには、ONBOOT="yes" と設定します。

no shutdown コマンドを使用して、インターフェイスをイネーブルにすることもできます。

例

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# shutdown
```

snmp-server enable

Cisco ISE で SNMP サーバーを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。

snmp-server enable

SNMP サーバーを無効にするには、このコマンドの **no** 形式を使用します。

コマンド デフォルト

SNMP サーバーはイネーブルに設定されています。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

例

```
ise/admin(config)# snmp-server enable
ise/admin(config)#
```

snmp-server user

新しい SNMP ユーザーを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。

snmp-server user *username* **v3 sha1**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha224**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha256**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha384**{**hash** | **plain**} *auth-password priv-password*

snmp-server user *username* **v3 sha512**{**hash** | **plain**} *auth-password priv-password*

（注） このコマンドは、SNMP バージョン 3 のみに対して使用する必要があります。

指定した SNMP ユーザーを削除するには、このコマンドの **no** 形式を使用します。

構文の説明

user	新しいユーザーを設定します。
username	SNMP エージェントに属するホスト上のユーザーの名前。
v3	トラップの送信に使用する SNMP のバージョン。 priv および auth キーワードを有効にするには SNMP バージョン 3 リティ モデルを使用する必要があることを指定します。
auth-password	認証ユーザーパスワードを指定します。パスワードの最小長は 1 すが、セキュリティを確保するために 8 文字以上にすることをお ます。 （注） パスワードを忘れた場合は、回復できないため、ユー を再設定する必要があります。プレーンテキストのパ ドまたはローカライズされたダイジェストを指定でき ローカライズされたダイジェストは、ユーザーに対し 択した認証アルゴリズム（MD5 または SHA にするこ きます）に一致する必要があります。ユーザー設定が ソールに表示される場合、またはファイル（スタート プ コンフィギュレーション ファイルなど）に書き込 場合、ローカライズされた認証ダイジェストとプライ ダイジェストが常にプレーン テキストのパスワードの りに表示されます。

priv-password	暗号ユーザーパスワードを指定します。パスワードの最小長すが、セキュリティを確保するために8文字以上にすること ます。 （注） パスワードを忘れた場合は、回復できないため、 を再設定する必要があります。プレーンテキストの ドまたはローカライズされたダイジェストを指定で ローカライズされたダイジェストは、ユーザーに 択した認証アルゴリズム（MD5またはSHAにする きます）に一致する必要があります。ユーザー設 ソールに表示される場合、またはファイル（スタ プ コンフィギュレーション ファイルなど）に書き 場合、ローカライズされた認証ダイジェストとプラ ダイジェストが常にプレーン テキストのパスワー りに表示されます。
sha1	認証タイプ
sha224	Sha224 認証タイプ。
sha256	Sha256 認証タイプ。
sha384	Sha384 認証タイプ。
sha512	Sha512 認証タイプ。
{**hash** | **plain**}	パスワードは、暗号化形式またはプレーン形式です。暗号化 ワードは、16 進数の形式である必要があります。

コマンド デフォルト

ディセーブル。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ユーザーを設定した後、SNMP バージョン 3 のホストを設定する必要があります。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともにこのホストを設定するには、ユーザー名を設定する必要があります。

例

```
ise/admin(config)# snmp-server user testuser v3 ?
   hash   Hash Passwords
   plain  Plain Passwords
   sha1   Sha1 authentication
   sha224 Sha224 authentication
```

```
   sha256 Sha256 authentication
   sha384 Sha384 authentication
   sha512 Sha512 authentication

ise/admin(config)# snmp-server user testuser v3 hash authpassword privpassword
ise/admin(config)#
```

snmp-server host

SNMP トラップを受信者に送信するには、コンフィギュレーション モードで **snmp-server host** コマンドを使用します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。

（注） `snmp-server host` コマンドを使用する前に、SNMP ユーザーを作成する必要があります。

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha1** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha224** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha256** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha384** {**hash** | **plain**} *auth-password priv-password*}

snmp-server host {*ip-address* | *hostname*} **version** {{*1* | *2c*} *community* | *3 username engine_ID* **sha512** {**hash** | **plain**} *auth-password priv-password*}

トラップ転送を削除するには、このコマンドの **no** 形式を使用します。

（注） SNMP バージョン 3 のホストが Cisco ISE で設定されている場合、トラップは設定されたユーザーだけに送信されるため、ユーザーをそのホストに関連付ける必要があります。**snmp-server host** コマンドを追加した後、トラップを受信するには、Cisco ISE で設定されているクレデンシャルと同じクレデンシャルを使って、NMS でユーザークレデンシャルを設定する必要があります。

構文の説明

host	SNMP 通知を受信するホストを設定します。
ip-address	SNMP 通知ホストの IP アドレス。最大 32 文字の英数字をサポートします。
hostname	SNMP 通知ホストの名前。最大 32 文字の英数字をサポートし

version {*1* | *2c* | *3*}	（任意）。トラップの送信に使用するSNMPのバージョン。デフ は1です。 versionキーワードを使用する場合は、次のキーワードのいずれか します。 • 1：SNMPv1。 • 2c：SNMPv2C。 • 3：SNMP v3。
community	Cisco ISEとNMSとの間での共有秘密キーを指定します。長さが 文字の大文字と小文字が区別された値。スペースは使用できませ フォルト コミュニティ ストリングは「public」です。Cisco ISEに キーを使用して、着信SNMP要求が有効であるかどうかを判断し
username	（オプション。SNMP バージョン 3 を選択した場合にのみ必要） ISE で SNMP バージョン 3 のホストが設定されている場合、ユー ホストを関連付けます。
engine_ID	（オプション。SNMP バージョン 3 を選択した場合にのみ必要） ト エンジンの ID。
auth-password	（オプション。SNMP バージョン 3 を選択した場合にのみ必要） ユーザー パスワードを指定します。
priv-password	（オプション。SNMP バージョン 3 を選択した場合にのみ必要） ユーザー パスワードを指定します。
sha1	認証タイプ
sha224	Sha224 認証タイプ。
sha256	Sha256 認証タイプ。
sha384	Sha384 認証タイプ。
sha512	Sha512 認証タイプ。

コマンド デフォルト

イネーブル。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

SNMP がすでに設定されている場合、Cisco ISE ではアプライアンスの起動（リロード）時に「coldStart(0)」トラップを送信します。Cisco ISE では、最初に起動するときは「coldStart(0)」トラップを送信する Net-SNMP クライアントを使用し、停止するときは企業固有のトラップ「nsNotifyShutdown」を使用します。

snmp-server host コマンドを使用して SNMP を再設定した後は、通常の場合、標準の「coldStart(0)」トラップでも「warmStart(1)」トラップでもなく、企業固有のトラップ「nsNotifyShutdown」を生成します。

（注） SNMP トラップターゲットがホスト名または FQDN によって指定され、DNS によって IPv4 と IPv6 の両方のアドレスに解決される場合、ISE は ipv6 ではなく IPv4 を介して IPv6 デュアルスタックターゲット受信者に SNMP トラップを送信します。IPv6 を介してトラップが送信されるようにするために、ISE 管理者は、DNS によってホスト名または FQDN のみを IPv6 に対して解決するか、または SNMP トラップを設定するときに IPv6 アドレスを直接指定することができます。

例

```
ise/admin(config)# snmp-server community new ro
ise/admin(config)# snmp-server host 209.165.202.129 version 1 password
ise/admin(config)#


ise/admin(config)# snmp-server host ise1 version 2c public
ise/admin(config)# snmp-server community public ro
2012-09-24T18:37:59.263276+00:00 ise1 snmptrapd[29534]: ise1.cisco.com [UDP:
[192.168.118.108]:44474]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29) 0:00:00.29, SNMPv2-MIB::snmpTrapOID.0
 = OID: SNMPv2-MIB::coldStart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
ise/admin(config)# snmp-server contact admin@cisco.com
2012-09-24T18:43:32.094128+00:00 ise1 snmptrapd[29534]: ise1.cisco.com [UDP:
[192.168.118.108]:53816]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (33311) 0:05:33.11,
SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix


ise/admin(config)# snmp-server host a.b.c.d version 3 testuser 0x12439343 hash authpassword
 privpassword
ise/admin(config)#


ise/admin(config)# snmp-server host a.b.c.d version 3 testuser 0x12439343 ?
   hash   Hash Passwords
   plain  Plain Passwords
   sha1   Sha1 authentication
   sha224 Sha224 authentication
   sha256 Sha256 authentication
   sha384 Sha384 authentication
   sha512 Sha512 authentication
```

snmp-server community

簡易ネットワーク管理プロトコル（SNMP）へのアクセスを許可するコミュニティアクセス ストリングを設定するには、コンフィギュレーション モードで **snmp-server community** コマンドを使用します。

snmp-server community *community-string* **ro**

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no snmp-server

構文の説明

community	SNMP コミュニティ ストリングを設定します。
community-string	パスワードのように機能するアクセス文字列。これによって SNM アクセスが許可されます。空白は使用できません。最大 255 文字 字をサポートします。
ro	読み取り専用アクセスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

snmp-server community コマンドでは、コミュニティストリングと引数 **ro** を指定する必要があります。指定しない場合、エラーが発生します。Cisco ISE の SNMP エージェントは、読み取り専用の SNMP v1 アクセスと SNMP v2c アクセスを次の MIB に提供します。

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- ENTITY-MIB：次の 3 つの MIB 変数のみが ENTITY-MIB でサポートされます。
  - 製品 ID：entPhysicalModelName
  - バージョン ID：entPhysicalHardwareRev
  - シリアル番号：entPhysicalSerialNumber
- DISMAN-EVENT-MIB

- NOTIFICATION-LOG-MIB
- CISCO-CDP-MIB

例

```
ise/admin(config)# snmp-server community new ro
ise/admin(config)#
```

snmp-server contact

SNMP 接続の管理情報ベース（MIB）値をシステムに設定するには、コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。システム連絡先情報を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *contact-name*

構文の説明

contact	この管理対象ノードの担当者を指定します。最大 255 文字の英数 ポートします。
contact-name	ノードのシステム連絡先情報を表す文字列。255 文字までの英数 定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

なし

例

```
ise/admin(config)# snmp-server contact Luke
ise/admin(config)#
```

snmp-server location

SNMP ロケーションの MIB 値をシステムに設定するには、コンフィギュレーション モードで **snmp-server location** コマンドを使用します。システムロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *location*

構文の説明

location	この管理対象ノードの物理的な場所を設定します。最大255文字をサポートします。
location	システムの物理ロケーション情報を表す文字列。255 文字まで指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

word 文字列では、単語の間にアンダスコア（_）またはハイフン（-）を使用することをお勧めします。*word* 文字列で単語の間に空白を使用する場合、文字列を二重引用符（"）で囲む必要があります。

例 1

```
ise/admin(config)# snmp-server location Building_3/Room_214
ise/admin(config)#
```

例 2

```
ise/admin(config)# snmp-server location “Building 3/Room 214”
ise/admin(config)#
```

snmp-server trap dskThresholdLimit

Cisco ISE パーティションのいずれかがディスク使用率のしきい値の限界に達した際に、SNMP サーバーがトラップを受信するよう設定するには、コンフィギュレーションモードで**snmp-server trap dskThresholdLimit** コマンドを使用します。

snmp-server trap dskThresholdLimit *value*

ディスク使用率がしきい値に達した際にトラップの送信を停止するには、このコマンドの **no** 形式を使用します。

構文の説明

value	使用可能なディスク スペースの比率を表す値。値の範囲は 1 ～ す。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.1.0.474	このコマンドが導入されました。

使用上のガイドライン

Cisco ISE のすべてのパーティションに共通する設定です。しきい値の限界を 40 に設定すると、パーティションのディスク領域が 60% を使用され、残り 40% になった時点でトラップを受信します。つまり、空き領域が設定された値に達したときにトラップが送信されます。

Cisco ISE CLI からこのコマンドを設定すると、kron ジョブが 5 分ごとに実行され、Cisco ISE のパーティションを 1 つずつ監視します。いずれかのパーティションがしきい値の上限に達すると、Cisco ISE は設定されている SNMP サーバーにトラップを送信します。ディスクのパスおよびしきい値の上限値も送信します。複数のパーティションがしきい値の上限に達すると、複数のトラップが送信されます。MIB ブラウザのトラップ レシーバを使用して SNMP トラップを表示できます。

例

```
ise/admin(config)# snmp-server trap dskThresholdLimit 40
ise/admin(config)#
```

snmp engineid

既存のエンジンIDを新しい値に変更するには、コンフィギュレーションモードで**snmp engineid command** を使用します。このコマンドは、既存のすべてのユーザーを再作成する必要があるという警告を表示します。

snmp engineid *engine_ID_string*

設定したエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

構文の説明

engineid	既存のエンジン ID を指定した新しい値に変更します。
engine_ID_string	エンジン ID を識別する最大 24 文字の文字列。

コマンド デフォルト

コマンドのデフォルト値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

例

```
ise/admin(config)# snmp engineid Abcdef129084B
% Warning: As a result of engineID change, all SNMP users will need
           to be recreated.
ise/admin(config)#
```

synflood-limit

TCP SYN パケットレート制限を設定します。

synflood-limit ?

構文の説明

synflood-limit	許可される 1 秒あたりの TCP SYN パケットの平均数。
?	1 ～ 2147483647 の範囲の値を指定できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。
3.2	synflood-limit の running-config 応答に、丸められた制限値が表示くなりました。ただし、synflood 制限では、引き続き実装時に丸ます。

使用上のガイドライン

TCP SYN パケットレート制限を設定するには、この **synflood-limit** を使用します。

設定されている実際のレート制限は、synflood 制限の設計により、設定した数と異なる場合があります。以下に、このドキュメントの作成時点での制限値の切り上げ方法を一覧表示しています。

- 制限値が 5001/s から 10000/s の場合、値は 10000/s に切り上げられます。
- 制限値が 3334/s から 5000/s の場合、値は 5000/s に切り上げられます。
- 制限値が 2501/s から 3333/s の場合、値は 3333/s に切り上げられます。
- 制限値が 2001/s から 2500/s の場合、値は 2500/s に切り上げられます。
- 制限値が 1667/s から 2000/s の場合、値は 2000/s に切り上げられます。
- 制限値が 1429/s から 1666/s の場合、値は 1666/s に切り上げられます。
- 制限値が 1251/s から 1428/s の場合、値は 1428/s に切り上げられます。
- 制限値が 1112/s から 1250/s の場合、値は 1250/s に切り上げられます。
- 制限値が 1001/s から 1111/s の場合、値を 1111/s に切り上げられます。
- 制限値が 910/s から 1000/s の場合、値は 1000/s に切り上げられます。
- 制限値が 834/s から 909/s の場合、値は 909/s に切り上げられます。
- 制限値が 150 未満の場合、丸めは行われません。

例

```
ise49/admin(config)# synflood-limit 5099
ise49/admin(config)# do show running-config | include syn
synflood limit 5099
```

username

SSH を使用して Cisco ISE アプライアンスにアクセスできるユーザーを追加するには、コンフィギュレーション モードで **username** コマンドを使用します。ユーザがすでに存在する場合は、このコマンドを使用してパスワード、特権レベル、または両方を変更します。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。

username *username* **password hash** | **plain** {*password*} **role admin** | **user email** {*email-address*}

既存のユーザーに対しては、次のコマンド オプションを使用します。

username *username* **password role admin** | **user** {*password*}

構文の説明

username	引数 username には 1 つの単語のみを指定できます。空白や二重 （"）は使用できません。最大 31 文字の英数字をサポートします
password	パスワードを指定します。
password	パスワード。40 文字までの英数字で指定します。パスワードは、 の新規ユーザに指定する必要があります。
hash | **plain**	パスワードのタイプ。最大 34 文字の英数字をサポートします。
role admin | **user**	ユーザーのユーザー ロールと特権レベルを設定します。
disabled	ユーザーの電子メールアドレスに従って、ユーザーをディセーブ ます。
email	ユーザーの電子メール アドレスを設定します。
email-address	ユーザーの電子メール アドレスを指定します。たとえば、 user1@mydomain.com のように指定します。

コマンド デフォルト

設定時の初期ユーザーです。

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

username コマンドでは、username および password キーワードの後に、hash | plain and the admin | user オプションを指定する必要があります。

例 1

```
ise/admin(config)# username admin password hash ###### role admin
ise/admin(config)#
```

例 2

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin
ise/admin(config)#
```

例 3

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@mydomain.com
ise/admin(config)#
```

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。