ロールベースの CLI アクセス

ロールベースの CLI アクセス機能を使用すれば、ネットワーク管理者はビューを定義できます。ビューは、Cisco IOS EXEC コマンドおよびコンフィギュレーション（config）モード コマンドへのアクセスを精選したり部分的に制限する、操作コマンドと設定機能のセットです。ビューで、ユーザの Cisco IOS コマンドライン インターフェイス（CLI）や設定情報へのアクセスを制限します。つまり、ビューで、使用するコマンドや表示する設定情報を定義できます。したがって、ネットワーク管理者はシスコ ネットワーキング デバイスへのアクセスを柔軟に管理できます。

ロールベースの CLI アクセスの前提条件

イメージで CLI ビューをサポートする必要があります。

ロールベースの CLI アクセスの制約事項

合法的傍受イメージの制限

CLI ビューは Cisco IOS パーサーの一部であるため、すべてのプラットフォームおよび Cisco IOS イメージの一部です。ただし、合法的傍受ビューは、合法的傍受サブシステムが組み込まれたイメージ内でしか使用できません。

許可されたビューの最大数

1 つの合法的傍受ビューを含むCLI ビューとスーパービューの設定可能な最大数は 15 です（これには、ルート ビューは含まれません）。

解析ビューのプロファイル

解析ビューのプロファイルを設定する場合、「no」コマンドまたは「default」コマンドと任意の設定コマンドの組み合わせは、スタートアップ コンフィギュレーション ファイルに保存されません。設定は受け入れられ、デバイスがリロードされるまで保持されます。スタートアップ コンフィギュレーションに保存されないコマンドの例：

- **command configure include all no**
- **command interface include all no**
- **command configure include all default**

ロールベースの CLI アクセスに関する情報

CLI ビューを使用するメリット

ユーザは特権レベルとイネーブル モード パスワードの両方を介して CLI アクセスを制御できますが、これらの機能では、ネットワーク管理者に Cisco IOS デバイスを操作するのに必要な詳細レベルが提供されません。CLI ビューは、より詳細なアクセス コントロール機能をネットワーク管理者に提供するため、Cisco IOS ソフトウェア全体のセキュリティとアカウンタビリティが向上します。

Cisco IOS Release 12.3(11)T 以降では、ネットワーク管理者が、ビューへのインターフェイスまたはインターフェイス グループを指定することもできます。そのため、指定されたインターフェイスに基づくアクセスが可能になります。

ルート ビュー

システムがルート ビューになっている場合は、レベル 15 の権限を持つユーザとして、すべてのアクセス権限が付与されます。管理者がシステムのビュー（CLI ビュー、スーパービュー、合法的傍受ビューなど）を設定する場合は、システムをルート ビューにする必要があります。

レベル 15 権限を持つユーザとルート ビュー ユーザの違いは、ルート ビュー ユーザは、新しいビューを設定したり、ビューに対してコマンドを追加または削除したりできることです。また、CLI ビューでは、ルート ビュー ユーザがそのビューに追加したコマンドにしかアクセスできません。

合法的傍受ビュー

CLI ビューと同様に、合法的傍受ビューは、特定のコマンドと設定情報へのアクセスを制限します。具体的には、合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

合法的傍受ビュー内で使用可能なコマンドは、次のカテゴリのいずれかに属します。

- 他のビューまたは権限レベルでは使用不可にすべき合法的傍受コマンド
- 合法的傍受ユーザにとっては有効であるが、他のビューまたは権限レベルから除外する必要のない CLI ビュー

スーパービュー

スーパービューは、1 つ以上の CLI ビューで構成されています。このビューでは、受け入れるコマンドと表示する設定情報を定義できます。スーパービューを使用すれば、ネットワーク管理者は、複数の CLI ビューをユーザ グループに割り当てなくても、設定された CLI ビュー内のすべてのユーザをスーパービューに割り当てることができます。

スーパービューには次の特性があります。

- CLI ビューを複数のスーパービュー間で共有できます。
- スーパービューにはコマンドを設定できません。つまり、CLI ビューにコマンドを追加してから、その CLI ビューをスーパービューに追加する必要があります。
- スーパービューにログインしたユーザは、そのスーパービューに属している CLI ビューに設定されたすべてのコマンドにアクセスできます。
- スーパービューごとにパスワードが設定されます。このパスワードは、スーパービューを切り替えたり、CLI ビューからスーパービューに切り替えたりするために使用されます。
- スーパービューが削除されても、関連する CLI ビューは削除されません。

ビュー認証と新しい AAA 属性

ビュー認証は、新しい属性の **cli-view-name** を介して、外部の認証、許可、およびアカウンティング（AAA）サーバーで実行されます。

AAA 認証は特定のユーザに 1 つのビュー名のみを関連付けます。つまり、認証サーバ内の 1 人のユーザに対して 1 つのビュー名しか設定できません。

ロールベースの CLI アクセスの使用方法

CLI ビューの設定

このタスクを実行して、CLI ビューを作成し、必要に応じて、コマンドまたはインターフェイスをビューに追加します。

始める前に

ビューを作成する前に、次のタスクを実行する必要があります。

- **aaa new-model** コマンドを使用して AAA をイネーブルにします。
- システムが特権レベル 15 ではなく、ルート ビューになっていることを確認します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name* [**inclusive**]
4. **secret** [**0** | **5**] *encrypted-password*
5. **commands** *parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface** *interface-name* | *command*]
6. **end**
7. **enable** [*privilege-level* | **view** *view-name*]
8. **show parser view all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルートパスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *view-name* [**inclusive**] 例：	すべてのコマンドを含むビューがデフォルトで作成されます。**inclusive** キーワードオプションを選択しないと、すべてのコマンドを除くビューがデフォル

	コマンドまたはアクション	目的
	`Device(config)# parser view first inclusive` `Device(config-view)#`	トで作成されます。ビューの設定モードになります。
ステップ 4	**secret** [**0** | **5**] *encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。 （注） CSCts50236 を使用すると、パスワードは削除または上書きできます。設定されたパスワードを削除するには、**no secret** コマンドを使用します。
ステップ 5	**commands** *parser-mode* {**exclude** | **include-exclusive** | **include**} [**all**] [**interface** *interface-name* | *command*] 例： `Device(config-view)# commands exec include show version`	コマンドまたはインターフェイスをビューに追加し、指定されたコマンドがあるモードを指定します。 （注） parser view プロファイルを設定するときは、次の **no** または **default** コマンドはスタートアップ コンフィギュレーションには保存されません。これらのコマンドは、デバイスがリロードされるまで使用中です。デバイスをリロードしたら、必要な結果が得られるように、これらのコマンドを再適用します。 • **commands configure include all no** • **commands interface include all no** • **commands configure include all default**
ステップ 6	**end** 例： `Device(config-view)# end`	ビューのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**enable** [*privilege-level* | **view** *view-name*] 例： `Device# enable view first`	設定済みの CLI ビューにアクセスするためのパスワードを求めるプロンプトが表示され、1つのビューから別のビューへ切り替えられます。 パスワードを入力して CLI ビューにアクセスします。

	コマンドまたはアクション	目的
ステップ 8	**show parser view all** 例： `Device# show parser view all`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。 （注） このコマンドはルートユーザーと合法的傍受ユーザーの両方に使用できますが、**all** キーワードはルートユーザーしか使用できません。ただし、**all** キーワードは、ルートビュー内のユーザーが、合法的傍受ビューやCLI ビュー内のユーザーに使用を許可するように設定できます。

トラブルシューティングのヒント

パスワードとビューを関連付ける必要があります。パスワードを関連付けずに、**commands** コマンド経由でビューにコマンドを追加しようとすると、次のようなシステムメッセージが表示されます。

```
%Password not set for view <viewname>.
```

合法的傍受ビューの設定

このタスクを実行して、ビューを初期化し、合法的傍受固有のコマンドと設定情報用に設定します

始める前に

合法的傍受ビューを初期化する前に、**privilege** コマンド経由で特権レベルが 15 に設定されていることを確認します。

（注） レベル 15 権限を持っている管理者またはユーザだけが合法的傍受ビューを初期化できます。

手順の概要

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルートパスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**li-view** *li-password* **user** *username* **password** *password* 例： `Device(config)# li-view lipass user li_admin password li_adminpass`	合法的傍受ビューを初期化します。 li-view が初期化されたら、**user** *username* **password** *password* オプション経由で少なくとも 1 人のユーザーを指定する必要があります。
ステップ 4	**username lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* 例： `Device(config)# username lawful-intercept li-user1 password li-user1pass`	シスコ デバイス上で合法的傍受ユーザを設定します。
ステップ 5	**parser view** *view-name* 例： `Device(config)# parser view li view name`	（任意）ビュー コンフィギュレーション モードに入ります。このモードでは、合法的傍受ビューのパスワードや名前を変更できます。
ステップ 6	**secret 5** *encrypted-password* 例： `Device(config-view)# secret 5 secret`	（任意）合法的傍受ビューの既存のパスワードを変更します。
ステップ 7	**name** *new-name* 例： `Device(config-view)# name second`	（任意）合法的傍受ビューの名前を変更します。 このコマンドが発行されなかった場合、合法的傍受ビューのデフォルト名は "li-view" になります。

トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザーに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

スーパービューの設定

このタスクを実行して、スーパービューを設定し、スーパービューに少なくとも 1 つの CLI ビューを追加します。

始める前に

CLI ビューをスーパービューに追加する前に、スーパービューに追加する CLI ビューがシステム内で有効なビューであることを確認します。つまり、ビューが、**parser view** コマンド経由で正常に作成されたことを確認します。

（注） スーパービューにビューを追加するには、スーパービューに対してパスワードを設定する必要があります（**secret 5** コマンド経由）。その後で、ビュー コンフィギュレーション モードで **view** コマンドを発行して、少なくとも 1 つの CLI ビューをスーパービューに追加します。

手順の概要

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **end**
7. **show parser view all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable view** 例： `Device> enable view`	ルート ビューを有効にします。 • プロンプトが表示されたら、権限レベル 15 パスワード（ルート パスワードなど）を入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parser view** *superview-name* **superview** 例： `Device(config)# parser view su_view1 superview`	スーパービューを作成して、ビュー コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 4	**secret 5** *encrypted-password* 例： `Device(config-view)# secret 5 secret`	CLI ビューまたはスーパービューとパスワードを関連付けます。 （注） このコマンドを発行しなければ、ビューのその他の属性が設定できません。
ステップ 5	**view** *view-name* 例： `Device(config-view)# view view_three`	正常な CLI ビューをスーパービューに追加します。 特定のスーパービューに追加する各 CLI ビューに対して、このコマンドを発行します。

ステップ 6	**end**
	例：
	`Device(config-view)# end`
	`Device#`
		ビューのコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

ステップ 7	**show parser view all** 例： `Device# show parser view`	（任意）デバイス上で設定されるすべてのビューに関する情報を表示します。 （注） このコマンドはルートユーザーと合法的傍受ユーザーの両方に使用できますが、**all** キーワードはルートユーザーしか使用できません。ただし、**all** キーワードは、ルートビュー内のユーザーが、合法的傍受ビューや CLI ビュー内のユーザーに使用を許可するように設定できます。

ビューとビュー ユーザのモニタリング

すべてのビュールート、CLI、合法的傍受、およびスーパービューに関するデバッグメッセージを表示するには、特権 EXEC モードで **debug parser view** コマンドを使用します。

ロールベースの CLI アクセスの設定例

例：CLI ビューの設定

次の例は、2 つの CLI ビュー "first" と "second" の設定方法を示しています。その後、実行コンフィギュレーションの CLI ビューを確認できます。

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
```

```
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit
!
!
Device(config-view)# do show running-config | beg view

parser view first inclusive
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec exclude configure terminal
 commands exec exclude configure
 commands exec exclude all show ip
 commands exec exclude show version
 commands exec exclude show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

例：CLI ビューの確認

CLI ビューの "first" と "second" を設定したら、**enable view** コマンドを発行して、各ビュー内で使用可能なコマンドを確認できます。次の例は、ユーザが CLI ビューの "first" にログイン後に、どのコマンドがこのビュー内で使用可能かを示しています（**show ip** コマンドは all オプションと一緒に設定されているため、second ビュー内で **include-exclusive** キーワードを使用している **show ip interface** コマンドを除く、すべてのサブオプションのセットが表示されます）。

```
Device# enable view first
Password:
Device# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
Device# show ?
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Device# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
```

```
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Device Discovery Protocol
.
.
.
```

例：合法的傍受ビューの設定

次の例は、合法的傍受ビューの設定方法、ビューへのユーザの追加方法、および追加されたユーザの確認方法を示しています。

```
!Initialize the LI-View.
Device(config)# li-view lipass user li_admin password li_adminpass
Device(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Device# enable view li-view
Password:
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parser view li-view

Device(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Device(config-view)#
! NOTE:LI View configurations are never shown as part of 'running-configuration'.
! Configure LI Users.
Device(config)# username lawful-intercept li-user1 password li-user1pass

Device(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
Device# show users lawful-intercept
li_admin
li-user1
li-user2
Device#
```

（注） 合法的傍受ビューは特定のイメージに対してのみ使用でき、表示名オプションは合法的傍受ビューでのみ使用できます。

例：スーパービューの設定

次の **show running-config** コマンドのサンプル出力は、"view_one" と "view_two" がスーパービューの "su_view1" に追加され、"view_three" と "view_four" がスーパービューの "su_view2" に追加されていることを示しています。

```
Device# show running-config
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

ロールベースの CLI アクセスに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
SNMP、MIB、CLI 設定	『*Cisco IOS Network Management Configuration Guide , Release 15.0.*』
権限レベル	「パスワード、特権、およびログインによるセキュリティ設定」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ロールベースの CLI アクセスに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1* : ロールベースの *CLI* アクセスに関する機能情報

機能名	リリース	機能情報
ロールベースの CLI アクセス		ロールベースの CLI アクセス機能は、ネットワーク管理者が、CLI と設定情報に対するユーザ アクセスを制限できるようにします。 CLI ビュー機能は、インターフェイス単位レベルでユーザ アクセスを制限するように拡張されました。新しい CLI ビューは、拡張されたビュー機能をサポートするために導入されました。また、設定された CLI ビューをスーパービューにグループ分けするためのサポートが導入されました。 次のコマンドが導入または変更されました。**commands (view)**、**enable**、**li-view**、**name (view)**、**parser view , parser view superview**、**secret**、**show parser view**、**show users**、**username**、および **view**。
ロールベースの CLI 包含ビュー		ロールベースの CLI 包含ビュー機能によって、すべてのコマンドを含む標準 CLI ビューがデフォルトで有効になっています。 次のコマンドが変更されました。**parser view inclusive**。

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。