コンフィギュレーション変更通知およびロギング

この機能が導入されるまでは、Cisco IOS ソフトウェアの設定が変更されたかどうかを判断するための唯一の方法は、実行コンフィギュレーションとスタートアップ コンフィギュレーションのコピーをローカル コンピュータに保存し、行単位で比較することでした。この比較方法では、変更を特定できますが、変更が行われた順序や、変更に責任を持つ人は特定できません。

コンフィギュレーション変更通知およびロギング（コンフィギュレーション ログ アーカイブ）機能を使用すると、アーカイブ機能を実装することにより、設定変更をセッションごとおよびユーザごとに追跡できます。このアーカイブでは、適用された各コンフィギュレーション コマンド、コマンドを適用した人、コマンドの Parser Return Code（PRC）、コマンドを適用した時刻を追跡する「設定ログ」が保存されます。また、この機能により、設定ログが変化したときに非同期通知を登録されたアプリケーションに送信する、通知メカニズムも追加されます。

この章で紹介する機能情報の入手方法

ご使用の Cisco IOS ソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「コンフィギュレーション変更通知およびロギングの機能情報」（P.12）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーション変更通知およびロギングの制約事項

- コンフィギュレーション モードの完全なコマンド入力だけがログに記録されます。
- **copy** コマンドを使用して適用されたコンフィギュレーション ファイルの一部であるコマンドは、ログに記録されません。

コンフィギュレーション変更通知およびロギングについて

コンフィギュレーション変更通知およびロギング機能を設定するには、次の概念について理解する必要があります。

設定ログ

コンフィギュレーション変更通知およびロギング機能は、Cisco IOS ソフトウェアの実行コンフィギュレーションに対する変更を、設定ログを保持することで追跡します。この設定ログは、Command-Line Interface（CLI; コマンドライン インターフェイス）または HTTP を通じて実行された変更だけを追跡します。最終的にアクション ルーチンが呼び出される完全なコマンドだけがログに記録されます。次の種類の入力はログに記録されません。

- 結果的に構文エラー メッセージが表示されるコマンド
- ルータのヘルプ システムを呼び出す部分的なコマンド

実行される各コンフィギュレーション コマンドに対し、次の情報がログに記録されます。

- 実行されたコマンド
- コマンドを実行したユーザの名前
- 設定変更のシーケンス番号
- コマンドに対する Parser Return Code

（注） 一部の環境では、コンフィギュレーション モードとコマンドが実行された時刻もログされます。

設定ログの情報を表示するには、**show archive log config** コマンドを使用します。ただし、Parser Return Code は、Cisco IOS アプリケーションの内部だけで使用されるため、除外されます。

コンフィギュレーション変更通知およびコンフィギュレーション変更ロギング

設定変更の通知を Cisco IOS ソフトウェア システム ロギング（syslog）プロセスに送信するように、コンフィギュレーション変更通知およびロギング機能を設定できます。syslog 通知機能を使用すると、ポーリングや情報収集作業を実行しなくても、設定ログ情報をモニタリングできます。

コンフィギュレーション変更通知およびロギング機能では、セッションごとまたはユーザごとにユーザが入力した設定変更を追跡できます。このツールを使用すると、管理者は、Cisco IOS ソフトウェアの実行コンフィギュレーションに対して行われた変更を追跡し、変更を行ったユーザを特定できます。

EAL4+ 認定のための設定ロガーの機能拡張

Cisco IOS Release 12.3(14)T では、設定変更ロギング プロセスに対してさらなる機能拡張が行われています。これらの機能拡張は、ロギング プロセスが、Conformance to Common Criteria, Evaluation Assurance Level 4+（EAL4+）Firewall Protection Profiles で規定されている要件を満たすようにするための作業を支援します。これらの機能拡張には、次の要件を満たすための変更が含まれています。

- ロギング パラメータを変更した場合、変更がログに記録されます。これは、実行コンフィギュレーションに対する各変更に対し、コピー操作（たとえば、**copy** *source* **running-config** の実行時）から syslog メッセージを送信することで実現されます。
- 管理ユーザ グループに対する変更、特権 EXEC モード（「イネーブル」モード）へのアクセスの失敗がログに記録されます。

（注） シスコでは、Cisco IOS Release 12.3(14)T に対する EAL 認定を要求していません。これは、将来的な認定の基盤となるものです。

上記のロギング アクションは、デフォルトでディセーブルになっています。これらのロギング特性をイネーブルにするには、「コンフィギュレーション変更通知およびロギング機能の設定」（P.4）に示す作業を実行します。

コンフィギュレーション変更通知およびロギング機能を設定する方法

ここでは、次の各手順について説明します。

コンフィギュレーション変更通知およびロギング機能の設定

コンフィギュレーション変更通知およびロギング機能をイネーブルにするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging enable**
6. **logging size** *entries*
7. **hidekeys**
8. **notify syslog**
9. **end**

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** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 5	**logging enable** 例： `Router(config-archive-log-config)# logging enable`	設定変更のロギングをイネーブルにします。 • 設定変更のロギングはデフォルトでディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	**logging size** *entries* 例： `Router(config-archive-log-config)# logging size 200`	（任意）設定ログに保持する最大エントリ数を指定します。 • *entries* 引数の有効な値の範囲は、1 ～ 1000 です。デフォルト値は 100 エントリです。 • 設定ログが一杯になると、新しいエントリを追加するたびに最も古いエントリが削除されます。 （注） 現在のログ サイズよりも小さいログ サイズが新たに指定された場合、ログ エントリの経過時間にかかわらず、新しいログ サイズになるまで最も古いログ エントリがすぐに削除されます。
ステップ 7	**hidekeys** 例： `Router(config-archive-log-config)# hidekeys`	（任意）設定ログ ファイル内のパスワード情報の表示を抑止します。 （注） **hidekeys** コマンドをイネーブルにすると、パスワード情報が設定ログ ファイルに表示されなくなるため、セキュリティが高まります。
ステップ 8	**notify syslog** 例： `Router(config-archive-log-config)# notify syslog`	（任意）設定変更の通知のリモート syslog への送信をイネーブルにします。
ステップ 9	**end** 例： `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

設定ログ エントリと統計情報の表示

設定ログのエントリまたは設定ログのメモリ使用量に関する統計情報を表示するには、ここに示す作業を実行します。

設定ログ エントリを表示し、設定ログのメモリ使用量を監視するために、コンフィギュレーション変更通知およびロギング機能に **show archive log config** コマンドが用意されています。

手順の概要

1. **enable**
2. **show archive log config** *number* [*end-number*]
3. **show archive log config all provisioning**
4. **show archive log config statistics**
5. **exit**

手順の詳細

ステップ 1　enable

このコマンドを使用して、特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。たとえば次のコマンドを実行します。

```
Router> enable
```

ステップ 2　show archive log config *number* [*end-number*]

このコマンドを使用して、設定ログ エントリをレコード番号ごとに表示します。オプションの *end-number* 引数でレコード番号を指定すると、レコード番号が *number* 引数と *end-number* 引数で指定した値の間にあるすべてのログ エントリが表示されます。次に例を示します。

```
Router# show archive log config 1 2

idx   sess   user@line        Logged command
 1     1     user1@console    logging enable
 2     1     user1@console    logging size 200
```

この例では、設定ログ エントリ番号 1 と 2 が表示されています。*number* 引数と *end-number* 引数の値の有効範囲は 1 ～ 2147483647 です。

ステップ 3　show archive log config provisioning

このコマンドを使用して、すべての設定ログ ファイルを、表形式ではなく、コンフィギュレーション ファイルに現れるとおりに表示します。次に例を示します。

```
Router# show archive log config all provisioning

archive
 log config
  logging enable
  logging size 200
```

この表示では、ログに記録されたコマンドを正しく適用するために必要な、コンフィギュレーション モードを変更するために使用したコマンドも表示されています。

ステップ 4　show archive log config statistics

このコマンドを使用して、設定のメモリ使用量情報を表示します。次に例を示します。

```
Router# show archive log config statistics

Config Log Session Info:
   Number of sessions being tracked: 1
   Memory being held: 3910 bytes
   Total memory allocated for session tracking: 3910 bytes
   Total memory freed from session tracking: 0 bytes

Config Log log-queue Info:
   Number of entries in the log-queue: 3
   Memory being held in the log-queue: 671 bytes
   Total memory allocated for log entries: 671 bytes
   Total memory freed from log entries:: 0 bytes
```

ステップ 5　exit

このコマンドを使用して、ユーザ EXEC モードを終了します。次に例を示します。

```
Router# exit
Router>
```

設定ログ エントリのクリア

設定ログのエントリは、2 つのうちいずれかの方法でクリアできます。設定ログのサイズを小さくするには、**logging size** コマンドを使用します。また、**logging enable** コマンドで、設定ログをいったんディセーブルにしてから再度イネーブルにします。

ここでは、次の各手順について説明します。

- 「ログ サイズを小さくすることによる設定ログのクリア」（P.7）
- 「設定ログをディセーブルすることによる設定ログのクリア」（P.8）

ログ サイズを小さくすることによる設定ログのクリア

logging size コマンドを使用して設定ログのエントリをクリアするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging size** *entries*
6. **logging size** *entries*
7. **end**

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** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**logging size** *entries* **例：** `Router(config-archive-log-config)# logging size 1`	設定ログに保持する最大エントリ数を指定します。 **（注）** 設定ログのサイズを 1 に設定すると、最新のエントリ以外のエントリが削除されます。
ステップ 6	**logging size** *entries* **例：** `Router(config-archive-log-config)# logging size 200`	設定ログに保持する最大エントリ数を指定します。 **（注）** 設定ログのサイズは、設定ログをクリアした後で目的の値にリセットする必要があります。
ステップ 7	**end** **例：** `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

例

次に、サイズを 1 に減らしてからサイズを目的の値にリセットすることで、設定ログをクリアする例を示します。

```
Router# configure terminal

Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging size 1
Router(config-archive-log-config)# logging size 200
Router(config-archive-log-config)# end
```

設定ログをディセーブルすることによる設定ログのクリア

logging enable コマンドを使用して設定ログのエントリをクリアするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **no logging enable**
6. **logging enable**
7. **end**

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** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# 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	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 5	**no logging enable** 例： `Router(config-archive-log-config)# no logging enable`	設定変更のロギングをディセーブルにします。 **（注）** 設定ログをディセーブルにすると、すべてのレコードが削除されます。
ステップ 6	**logging enable** 例： `Router(config-archive-log-config)# logging enable`	設定変更のロギングをイネーブルにします。
ステップ 7	**end** 例： `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

例

次に、設定ログをディセーブルにしてからイネーブルにすることで設定ログをクリアする例を示します。

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# no logging enable
Router(config-archive-log-config)# logging enable
Router(config-archive-log-config)# end
```

コンフィギュレーション変更通知およびロギング機能の設定例

ここでは、次の設定例について説明します。

- 「コンフィギュレーション変更通知およびロギング機能の設定：例」

コンフィギュレーション変更通知およびロギング機能の設定：例

次に、設定ログの最大エントリ数を 200 にして設定ロギングをイネーブルにする例を示します。この例では、設定ログ レコード内のパスワード情報の表示を抑止することでセキュリティを向上させ、syslog 通知を有効にしています。

```
configure terminal

archive
 log config
 logging enable
 logging size 200
 hidekeys
 notify syslog
```

その他の関連資料

ここでは、コンフィギュレーション変更通知およびロギング機能に関する関連資料について説明します。

関連資料

関連項目	参照先
コンフィギュレーション ファイルの管理についての情報	『Managing Configuration Files』
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **archive**
- **hidekeys**
- **log config**
- **logging enable**（**config-archive-log**）
- **logging size**（**config-archive-log**）
- **notify syslog**
- **show archive log config**

コンフィギュレーション変更通知およびロギングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/cfn にある Cisco Feature Navigator にアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーション変更通知およびロギングの機能情報

機能名	リリース	機能情報
コンフィギュレーション変更通知およびロギング	12.3(4)T 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	コンフィギュレーション変更通知およびロギング（コンフィギュレーション ロギング）機能を使用すると、設定ログを実装することで、セッションごとまたはユーザごとに設定変更を追跡できます。設定ログは、適用された各コンフィギュレーション コマンド、コマンドを適用した人、コマンドに対する Parser Return Code、コマンドを適用した時刻を追跡します。また、この機能により、設定ログが変化したときに非同期通知を登録されたアプリケーションに送信する、通知メカニズムも追加されます。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション変更通知およびコンフィギュレーション変更ロギング」（P.3） • 「コンフィギュレーション変更通知およびロギング機能の設定」（P.4） • 「設定ログ エントリと統計情報の表示」（P.5） この機能により、**archive**、**hidekeys**、**log config**、**logging enable**、**logging size**、**notify syslog**、**show archive log config** の各コマンドが変更されました。
EAL4+ 認定のための設定ロガーの機能拡張	12.3(14)T 12.2(27)SBC	Cisco IOS Release 12.3(14)T および 12.2(27)SBC では、設定変更ロギング プロセスに対してさらなる機能拡張が行われています。これらの機能拡張は、ロギング プロセスが、Conformance to Common Criteria, Evaluation Assurance Level 4+（EAL4+）Firewall Protection Profiles で規定されている要件を満たすようするための作業を支援します。 この機能に関する詳細については、次の項を参照してください。 • 「EAL4+ 認定のための設定ロガーの機能拡張」（P.3）