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。

コンフィギュレーション変更通知およびロギング機能が導入されるまでは、シスコ 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の制約事項 （1 ページ）
- 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 （2 ページ）
- コンフィギュレーション変更通知およびロギングの設定方法 （3 ページ）
- コンフィギュレーション変更通知およびロギングの設定例 （11 ページ）
- その他の参考資料 （12 ページ）
- 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 （12 ページ）

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 モードでの完全なコマンド入力のみ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

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、設定ログを保持することで、シスコソフトウェアの実行コンフィギュレーションに加えられた変更を追跡します。この設定ログは、CLIまたはHTTPのみを介して開始される変更を追跡します。アクション ルーチンの呼び出しが発生する完全なコマンドが記録されます。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
- デバイス ヘルプ システムを呼び出す一部のコマンド

実行される各設定コマンドでは次の情報が記録されます。

- 実行されたコマンド
- コマンドが実行されたコンフィギュレーション モード
- コマンドを実行したユーザーの名前
- コマンドが実行された時間
- 設定変更のシーケンス番号
- コマンドへのパーサー返還コード

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、シスコ 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。管理者はこのツールを使用して、ソフトウェアの実行コンフィギュレーションに加えられた設定変更をすべて追跡し、その変更を実行したユーザーを特定できます。

EAL4 + 認証用のコンフィギュレーション ロガーの機能強化

Evaluation Assurance Level 4+（EAL4+）認定のためのコンフィギュレーション ロガー機能拡張により、ロギング プロセスが Conformance to Common Criteria, EAL4+ Firewall Protection Profiles で規定されている要件を満たすことが保証されます。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 パラメータを変更すると、それらの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（**copy** *source* **running-config** など）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がログに記録されます。たとえば、特権 EXEC モード（「イネーブル」モード）へのアクセスの失敗が記録されます。

（注） EALの認定はシスコが要求するものではありません。これらの機能拡張は、将来の認定に備えた土台となるものです。

前述のロギング アクションは、デフォルトでは無効になっています。これらのロギング特性を有効にするには、「コンフィギュレーション変更通知およびロギング」機能モジュールの「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」セクションに記載されているタスクを実行します。

コンフィギュレーション変更通知およびロギングの設定方法

コンフィギュレーション変更通知およびロギングの設定

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
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	**archive** 例： `Device(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： `Device(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： `Device(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。 • コンフィギュレーション変更のロギングは、デフォルトでは無効になっています。
ステップ 6	**logging size** *entries* 例： `Device(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。 • 設定ログがいっぱいになると、新しいエントリが追加され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：	（任意）パスワード情報が設定ログ ファイルに表示されないようにします。

	コマンドまたはアクション	目的
	`Device(config-archive-log-config)# hidekeys`	（注） **hidekeys** コマンドを有効にすると、設定ログ ファイルにパスワード情報が表示されなくなり、セキュリティが向上します。
ステップ 8	**notify syslog** 例： `Device(config-archive-log-config)# notify syslog`	（任意）設定変更の通知をリモート syslog に送信できるようにします。
ステップ 9	**end** 例： `Device(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

設定ログ エントリおよび統計の表示

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。コマンドは任意の順序で入力できます。

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。パスワードを入力します（要求された場合）。次に例を示します。

例：

```
Device> 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* を指定すると、*number* 引数で入力した値から *end-number* 引数で入力した値までの範囲のレコード番号を持つすべてのログ エントリが表示されます。次に例を示します。

```
Device# 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
```

例：

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* 引数の範囲は 1 ～ 2147483647 です。

ステップ 3 show archive log config all provisioning

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での表示形式で表示するには、このコマンドを使用します。次に例を示します。

例：

```
Device# 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

コンフィギュレーションのメモリ使用量の情報を表示するには、このコマンドを使用します。次に例を示します。

例：

```
Device# 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 モードに戻ります。次に例を示します。

例：

```
Device# exit
Device>
```

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。**logging size** コマンドを使用して設定ログのサイズを縮小するか、または **logging enable** コマンドを使用して設定ログを無効にしてから再び有効にすることができます。

ログサイズのリセットによる設定ログの消去

このタスクでは、 **logging size** コマンドを 2 回入力して、ログ サイズを 1 に減らしてから、ログ サイズを目的の値にリセットする方法を示します。

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
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	**archive** 例： `Device(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：	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
	`Device(config-archive)# log config`	
ステップ 5	**logging size** *entries* 例： `Device(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はすべて消去されます。
ステップ 6	**logging size** *entries* 例： `Device(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） 設定ログを消去した後、設定ログのサイズを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： `Device(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

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

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： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
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。

	コマンドまたはアクション	目的
ステップ 3	**archive** 例： `Device(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： `Device(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： `Device(config-archive-log-config)# no logging enable`	コンフィギュレーション変更のロギングを無効にします。 （注） 設定ログを無効にすると、すべてのレコードが消去されます。
ステップ 6	**logging enable** 例： `Device(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： `Device(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

自動ログ削除

この機能を使用すると、設定可能な時間が経過すると、ロギングバッファからエントリを自動的に削除できます。エントリがデバイスから消去されるまでのローカルsyslog保持期間を設定する必要があります。特定の時間が経過した後にロギングデータを自動的に消去するには、**logging purge-log buffer days x time <x:y>** コマンドを使用します。ログエントリの最大保持期間は、1～120日の範囲で日単位で設定できます。この機能では、1日に1回のバッファクリーンアップも許可されます。これにより、24時間ごとに設定された期間に基づいてバッファログがクリーンアップされます。

（注） コマンドで保存期間を日単位でのみ指定した場合、ログの削除は翌日のコマンドの設定と同時に行われます。

自動ログ削除を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **logging purge-log buffer days entries**
4. **logging purge-log buffer days x time <x:y>**
5. **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： `Device > enable`	特権 EXEC モードを有効にします。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： `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	**logging purge-log buffer days entries** 例： `Device(config)#logging purge-log buffer days 90`	ログエントリの最大保持時間を指定します。 （注） 有効な値の範囲は 1 ～ 120 です。
ステップ 4	**logging purge-log buffer days x time <x:y>** 例： `Device(config)#logging purge-log buffer days 90 time 15:45`	（任意）ログを自動削除する特定の時間を指定します。 （注） • ログは削除されます。 • 時刻が現在のシステム時刻よりも小さい場合、削除は翌日の指定された時刻に行われます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ログ自動削除の設定例

次に、自動ログ削除を有効にして、90 日前のデータのみを保持する例を示します。ログの削除は、指定された時刻（15:45）に行われます。

```
Router (config)# logging purge-log buffer days 90 time 15:45
*May 18 20:20:20 UTC: %DMI-5-SYNC_NEEDED: R0/0: dmiauthd: Configuration
change requiring running configuration sync detected - ' logging purgelog
buffer days 90 time 15:45
'. The running configuration will be sy
```

```
nchronized to the NETCONF running data store.
◦ May 18 20:20:21 UTC: %DMI-5-SYNC_START: R0/0: dmiauthd: Synchronization
of the running configuration to the NETCONF running data store has
started.
May 18 20:20:26 UTC: %DMI-5-SYNC_COMPLETE: R0/0: dmiauthd: The running
configuration has been synchronized to the NETCONF running data store.
```

次に、自動ログ削除を有効にして、10 日前のデータのみを保持し、残りのログをバッファから削除する例を示します。

```
Router(config)# logging purge-log buffer days 10
Jul  5 19:48:16.974: %PARSER-5-CFGLOG_LOGGEDCMD: User:test  logged command:logging
purge-log buffer days 10
*Jul  5 19:48:17.330: %DMI-5-SYNC_NEEDED: R0/0: dmiauthd: Configuration change requiring
 running configuration sync detected - '  logging purge-log buffer days 10'.
The running configuration will be synchronized  to the NETCONF running data store.
*Jul  5 19:48:17.451: %DMI-5-SYNC_START: R0/0: dmiauthd: Synchronization of the running
 configuration to the NETCONF running data store has started.
```

no logging purge-log buffer コマンドの出力例。

```
Router(config)# no logging purge-log buffer
Jul  5 19:49:29.601: %PARSER-5-CFGLOG_LOGGEDCMD: User:test  logged command:no logging
purge-log buffer
*Jul  5 19:49:29.980: %DMI-5-SYNC_NEEDED: R0/0: dmiauthd: Configuration change requiring
 running configuration sync detected - '  no logging purge-log buffer '.
The running configuration will be synchronized  to the NETCONF running data store.
*Jul  5 19:49:30.110: %DMI-5-SYNC_START: R0/0: dmiauthd: Synchronization of the running
 configuration to the NETCONF running data store has started.
```

コンフィギュレーション変更通知およびロギングの設定例

例：コンフィギュレーション変更通知およびロギングの設定

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、**hidekeys** コマンドを使用して設定ログ 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、**notify syslog** コマンドで 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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
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	『コンフィギュレーション ファイルの管理コンフィギュレーション ガイド』の「コンフィギュレーション ファイルの管理」モジュール
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

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

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

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:* 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		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。設定ログには、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）、および、コマンドを適用した時刻が記録されます。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。 次のコマンドが導入または変更されました。**archive**、**hidekeys**、**log config**、**logging enable**、**logging size**、**notify syslog**、**show archive log config**
自動ログ削除のサポート	Cisco IOS XE Dublin 17.12.1a	この機能を使用すると、ロギングバッファからエントリを削除できます。エントリがデバイスから自動的に消去されるまでのローカル syslog 保持期間を設定できます。この機能を有効にするには、**logging purge-log buffer days** コマンドを使用します。

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。