システムの監査

システム上のアクティビティを 2 つの方法で監査できます。FireSIGHT システムに含まれるアプライアンスは、Web インターフェイスとのユーザ インタラクションごとに監査レコードを生成し、システム ログ内にシステム ステータス メッセージも記録します。

次の各項では、システムに備わっているモニタリング機能について詳しく説明します。

- 監査レコードの管理（69-1 ページ）では、システムの監査情報を表示および管理する方法について説明します。
- システム ログの表示（69-11 ページ）では、システム ステータス メッセージを含むシステム ログの表示方法について説明します。

ヒント　また、保護ライセンス付きの管理対象デバイスおよび防御センターに備わっているフル レポート機能を使用すると、監査データを含む、イベント ビューからアクセス可能なほぼすべての種類のデータのレポートを作成できます。詳細については、レポートの操作（57-1 ページ）を参照してください。

監査レコードの管理

ライセンス：任意（Any）

防御センターおよび管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準のイベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで減らします。

（注）　シリーズ 3 アプライアンスをリブートした直後にすばやく CLI にログインした場合、そこで実行するコマンドは、Web インターフェイスが使用可能になるまでは監査ログに記録されません。

詳細については、次の項を参照してください。

- 監査レコードの表示（69-2 ページ）
- 監査レコードの抑制（69-4 ページ）

監査レコードの表示

ライセンス：任意（Any）

アプライアンスを使用して監査レコードのテーブルを表示できます。その後、探している情報に応じて表示方法を操作できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

次の表では、監査ログ ワークフローのページで実行できる操作をいくつか説明します。

表 69-1　監査ログの操作

目的	操作
テーブルのカラムの内容について詳しく調べる	監査ログ テーブルについて（69-7 ページ）で詳細を参照してください。
監査レコードを表示する際に使われる時間範囲を変更する	詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。
現在のワークフロー ページでイベントをソートおよび制約する	テーブル ビュー ページのソートおよびレイアウトの変更（58-38 ページ）で詳細を参照してください。
現在のワークフロー ページ内で移動する	ワークフロー内の他のページへのナビゲート（58-40 ページ）で詳細を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用（58-21 ページ）を参照してください。
ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウン**されません**）。 • いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するイベントの横のチェックボックスを選択し、[表示（View）] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示（View All）] をクリックします。 **ヒント** テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。

表 69-1　監査ログの操作（続き）

目的	操作
特定の 1 つの値で制約する	行内の値をクリックします。 ドリルダウン ページで値をクリックすると、次のページに移動し、その値だけに制約されます。 テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページにドリルダウン**されない**ことに注意してください。 **ヒント** テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
監査レコードを削除する	次のいずれかの方法を使用します。 • いくつかの項目を削除するには、削除するイベントの横にあるチェックボックスを選択し、[削除（Delete）] をクリックします。 • 現在の制限付きビューにあるすべての項目を削除するには、[すべて削除（Delete All）] をクリックした後、すべてのイベントを削除することを確認します。
一時的に他のワークフローを使用する	[ワークフロー切り替え（switch workflow）] をクリックします。詳細については、ワークフローの選択（58-18 ページ）を参照してください。
すぐに戻ることができるように現在のページをブックマークする	[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
ブックマークの管理ページへ移動する	[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
現在のビューのデータに基づいてレポートを生成する	[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。
監査ログに記録されている変更の概要を表示する	[メッセージ（Message）] カラムの該当するイベントの横にある比較アイコン（）をクリックします。詳細については、監査ログを使って変更を調査する（69-8 ページ）を参照してください。

監査レコードを表示するには、次のようにします。

アクセス：Admin

手順 1　[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）] を選択します。

デフォルト監査ログ ワークフローの最初のページ（唯一のページ）が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約の設定（58-26 ページ）を参照してください。

ヒント　監査イベントのテーブル ビューを含まないカスタム ワークフローを使用している場合は、[ワークフロー切り替え（switch workflow）] をクリックし、[監査ログ（Audit Log）] を選択します。

監査イベントの操作

ライセンス：任意（Any）

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しのクローズ アイコン（ ✖ ）をクリックした後、表示されるポップアップ ウィンドウで [適用（Apply）] をクリックします。カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェック ボックスを選択またはクリアしてから [適用（Apply）] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約され、次のページにはドリルダウンされません。

ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

詳細は、次のトピックを参照してください。

- イベントの制約（58-35 ページ）。
- 複合的な制約の使用（58-37 ページ）
- ドリルダウン ワークフロー ページのソート（58-39 ページ）
- 監査ログ テーブルについて（69-7 ページ）

監査レコードの抑制

ライセンス：任意（Any）

監査ポリシーで、FireSIGHT システム/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザがオンライン ヘルプを表示するたびに、FireSIGHT システムは監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの `admin` ユーザ アカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュア シェルを開くことができる）必要があります。

注意　必ず、許可された担当者だけがアプライアンスとその `admin` アカウントにアクセスできるようにしてください。

監査レコードを抑制するには、次の形式の 1 つ以上のファイルを `/etc/sf` ディレクトリに作成する必要があります。

```
AuditBlock.type
```

ここで、*type* は `address`、`message`、`subsystem`、または `user` です。

(注)　特定のタイプの監査メッセージに関する AuditBlock.*type* ファイルを作成した後、それらの抑制を解除することにした場合は、AuditBlock.*type* ファイルの内容を削除する必要があります。ただし、ファイル自体は FireSIGHT システムに残してください。

それぞれの監査ブロック タイプの内容は、次の表に示すような特定の形式でなければなりません。ファイル名の大文字/小文字が正しいことを確認します。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

表 69-2　監査ブロック タイプ

タイプ	説明
アドレス（Address）	AuditBlock.address という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。アドレスの先頭からマッピングされる場合に限り、部分的な IP アドレスを使用できます。たとえば、部分的なアドレス 10.1.1 は、10.1.1.0 から 10.1.1.255 までのアドレスと一致します。
メッセージ (Message)	AuditBlock.message という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば backup をこのファイルに含めた場合、部分文字列の照合により backup という語を含むすべてのメッセージが抑制されることに注意してください。
サブシステム (Subsystem)	AuditBlock.subsystem という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査されるサブシステムのリストについては、サブシステム名の表を参照してください。
ユーザ（User）	AuditBlock.user という名前のファイルを作成し、抑制するユーザ アカウントを 1 行に 1 つずつ含めます。ユーザ名の先頭からマッピングされる場合に限り、部分的な文字列の照合を使用できます。たとえば、部分的なユーザ名 IPSAnalyst は、ユーザ名 IPSAnalyst1 および IPSAnalyst2 と一致します。

AuditBlock ファイルを追加した場合、Audit というサブシステムや Audit Filter *type* Changed というメッセージを含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

次の表に、監査されるサブシステムを示します。

表 69-3　サブシステム名

名前	含まれるユーザ インタラクション
管理(Admin)	管理機能：システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザ アカウントの管理、スケジュール設定など
アラート（Alerting）	アラート機能：電子メール、SNMP、syslog アラートなど
監査ログ（Audit Log）	監査イベントの表示
監査ログ検索（Audit Log Search）	監査イベントの検索
コマンド ライン(Command Line)	コマンドライン インターフェイス

表 69-3　サブシステム名（続き）

名前	含まれるユーザ インタラクション
設定（Configuration）	電子メール アラート機能
COOP	継続的な運用機能
日付（Date）	イベント ビューの日時範囲
デフォルトのサブシステム（Default Subsystem）	サブシステムが割り当てられていないオプション
検出および防御ポリシー（Detection & Prevention Policy）	侵入ポリシーのメニュー オプション
エラー（Error）	システム レベルのエラー
eStreamer	eStreamer の設定
EULA	エンド ユーザ ライセンス契約書の確認
イベント(Events)	侵入およびディスカバリ イベント ビュー
イベント クリップボード（Events Clipboard）	侵入イベント クリップボード
レビューされたイベント（Events Reviewed）	レビューされた侵入イベント
イベント検索（Events Search）	すべてのイベント検索
ルール アップデートのインストール失敗（Failed to install rule update *rule_update_id*）	ルール更新のインストール
ヘッダー(Header)	ユーザ ログイン後のユーザ インターフェイスの最初の表示
状態(Health)	ヘルス モニタリング
ヘルス イベント（Health Events）	ヘルス モニタリング イベントの表示
ヘルプ(Help)	オンライン ヘルプ
高可用性(High Availability)	高可用性機能
IDS インパクト フラグ（IDS Impact Flag）	インパクト フラグの設定
IDS ポリシー（IDS Policy）	侵入ポリシー
IDS ポリシー（IDS Policy）> *policy_name* > アプライアンス（Appliance）> *det_engine_name*	侵入ポリシーの適用
IDSRule sid：*sig_id* rev：*rev_num*	SID による侵入ルール
インシデント(Incidents)	侵入インシデント
ポリシー適用ジョブの挿入（Insert Policy Apply Job）	ポリシーの適用
インストール(Install)	更新のインストール
侵入イベント(Intrusion Events)	侵入イベント

表 69-3　サブシステム名（続き）

名前	含まれるユーザ インタラクション
ログイン（Login）	Web インターフェイスのログイン/ログアウト機能
メニュー(Menu)	すべてのメニュー オプション
設定のエクスポート（Configuration export）> *config_type* > *config_name*	特定のタイプ/名前の設定のインポート
権限エスカレーション（Permission Escalation）	ユーザ ロールのエスカレーション
初期設定(Preferences)	ユーザ アカウントのタイム ゾーンや個々のイベント設定などのユーザ設定
ポリシー(Policy)	侵入ポリシーを含むすべてのポリシー
登録(Register)	防御センターでのデバイスの登録
リモート ストレージ デバイス(Remote Storage Device)	リモート ストレージ デバイスの設定
レポート(Reports)	レポート リスト機能およびレポート デザイナ機能
ルール（Rule）	侵入ルール（ルール エディタとルールのインポート プロセスを含む）
ルール更新のインポート ログ（Rule Update Import Log）	ルール更新のインポート ログの表示
ルール更新のインストール（Rule Update Install）	ルール更新のインストール
ステータス（Status）	syslog およびホストやパフォーマンスの統計情報
システム(System)	システム全体のさまざまな設定
システム ポリシー（System Policy）> *policy_name* アプライアンス（Appliance）> *appliance_name*	システム ポリシーの適用
タスク キュー(Task Queue)	タスク キューの表示
ユーザ(User)	ユーザ アカウントとロールの作成および変更

監査ログ テーブルについて

ライセンス：任意（Any）

各アプライアンスは、Web インターフェイスとのユーザ インタラクションごとに 1 つの監査イベントを生成します。各イベントには、タイムスタンプ、イベントを発生させたアクションを行ったユーザ名、発信元 IP、およびイベントの説明テキストが含まれます。監査ログ テーブルのフィールドについて、以下の表で説明します。

表 69-4　監査ログのフィールド

フィールド	説明
時刻（Time）	アプライアンスが監査レコードを生成した日時。
ユーザ（User）	監査イベントをトリガーしたユーザのユーザ名。

表 69-4　監査ログのフィールド(続き)

フィールド	説明
サブシステム (Subsystem)	監査レコードが生成されたときにユーザがたどったメニュー パス。たとえば、[システム(System)] > [モニタリング(Monitoring)] > [監査(Audit)] は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[サブシステム(Subsystem)] フィールドにイベント タイプのみが表示されます。たとえば、**Login** はユーザのログイン試行を分類します。
メッセージ (Message)	ユーザが実行した操作。 たとえば `Page View` は、[サブシステム(Subsystem)] で示されたページをユーザが単に表示しただけであることを意味します。一方、`Save` は、ユーザがページの [保存(Save)] ボタンをクリックしたことを意味します。 FireSIGHT システムに対して加えられた変更は比較アイコン( )付きで表示され、これをクリックすると変更の概要を表示できます。詳細については、監査ログを使って変更を調査する(69-8 ページ)を参照してください。
ソースIP (Source IP)	ユーザが使用したホストに関連付けられている IP アドレス。
メンバー数 (Count)	各行に表示された情報と一致するイベントの数。[カウント(Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

監査ログを使って変更を調査する

ライセンス:任意(Any)

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

システムの変更を表す監査ログ イベントの横には比較アイコン( )が表示されます。比較アイコンをクリックして [設定の比較(Compare Configurations)] ページにアクセスし、変更についての詳細レポートを表示できます。

[設定の比較(Compare Configurations)] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑は、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

監査ログで変更を調査するには、次のようにします。

アクセス: Admin

手順 1　[システム(System)] > [モニタリング(Monitoring)] > [監査(Audit)] を選択します。

デフォルト監査ログ ワークフローの最初のページが表示されます。

監査イベントのテーブル ビューを含まないカスタム ワークフローを使用している場合は、[ワークフロー切り替え(switch workflow)] をクリックし、[監査ログ(Audit Log)] を選択します。

手順 2　[メッセージ(Message)] カラムの該当する監査ログ イベントの横にある比較アイコン( )をクリックします。

[設定の比較(Compare Configurations)] ページが表示されます。タイトル バーの上の [前へ(Previous)] または [次へ(Next)] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの検索

ライセンス: 任意(Any)

監査レコードを検索して、ユーザ、特定のサブシステム、または監査レコード メッセージに固有の情報を見つけることができます。

実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。次の表で、ユーザが使用できる検索条件について説明します。監査の検索では大文字と小文字を区別しません。たとえば、「Analyst01」で検索しても「analyst01」で検索しても結果は同じになります。

表 69-5　監査レコードの検索条件

検索フィールド	説明	例
ユーザ(User)	対象となる監査イベントをトリガーとして使用したユーザを示すユーザ名を入力します。このフィールドでは、ワイルドカード文字としてアスタリスク(*)を使用できます。	「jsmith」を指定すると、jsmith というユーザに関連したすべての監査レコードが返されます。
サブシステム(Subsystem)	対象となる監査レコードが生成されたときにユーザがたどった完全メニュー パスを入力します。このフィールドでは、ワイルドカード文字としてアスタリスク(*)を使用できます。	たとえば、[システム(System)] > [モニタリング(Monitoring)] > [監査(Audit)] と「*Audit」のどちらを指定した場合も、監査ログの使用に関連した監査レコードが返されます。 「*Audit*」の場合、上記のレコードに加えて、監査レコードの検索に関連したレコードも返されます。
メッセージ(Message)	ユーザが実行したアクション、またはユーザがページでクリックしたボタン。このフィールドでは、ワイルドカード文字としてアスタリスク(*)を使用できます。	「Apply」を指定すると、ユーザが侵入ポリシーを適用した監査レコードが返されます。 「Save Rule」を指定すると、ユーザが相関ルールを保存した監査レコードが返されます。 「Page View」を指定すると、ユーザがページを表示した監査レコードが返されます。
時刻(Time)	監査レコードが生成された日時を指定します。時間入力の構文については、検索での時間制約の指定(60-5 ページ)を参照してください。	「> 2006-01-15 13:30:00」を指定すると、2006 年 1 月 15 日午後 1 時 30 分以降に生成されたすべての監査レコードが返されます。

表 69-5　監査レコードの検索条件（続き）

検索フィールド	説明	例
ソースIP(Souce IP)	対象となる監査レコードに関連するホストの IP アドレスを入力します。 (注)　具体的な IP アドレスを入力する**必要があります**。監査ログを検索するときには、IP 範囲を使用できません。	「172.16.1.37」を指定すると、IP アドレス 172.16.1.37 からユーザによって生成されたすべての監査レコードが返されます。
構成の変更（Configuration Change）	構成の変更に関する監査レコードを表示するかどうかを指定します。	「yes」を指定すると、構成変更の監査レコードが返されます。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

監査レコードを検索するには、次のようにします。

アクセス：Admin

手順 1　[分析（Analysis）] > [検索（Search）] を選択します。

[検索（Search）] ページが表示されます。

手順 2　テーブルのドロップダウン リストから、[監査ログ イベント（Audit Log Events）] を選択します。

監査ログの検索ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　表監査レコードの検索条件に記載されているように、該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

手順 4　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要があります**。

手順 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存(Save As New)] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

手順 6　検索を開始するには、[検索(Search)] ボタンをクリックします。

現在の時刻範囲によって制約されたデフォルト監査ログ ワークフローに、検索結果が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定(71-3 ページ)を参照してください。

システム ログの表示

ライセンス:任意(Any)

システム ログ(syslog)ページには、アプライアンスのシステム ログ情報が表示されます。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ本体

(注)　システム ログ情報はローカルな情報です。たとえば、防御センターを使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

フィルタリング機能を使用すると、特定のコンポーネントのシステム ログ メッセージを表示できます。詳細については、システム ログ メッセージのフィルタリング(69-12 ページ)を参照してください。

syslog を表示するには、次のようにします。

アクセス: Admin/Maint

手順 1　[システム(System)] > [モニタリング(Monitoring)] > [Syslog] を選択します。

[システムログ(System Log)] ページが表示されます。

ヒント　3D9900 の場合、ロード バランシング インターフェイス モジュール (LBIM) がメッセージをデバイスの syslog に転送します。`lbim` でフィルタリングすることで、これらのメッセージを見つけることができます。

システム ログ メッセージのフィルタリング

ライセンス：任意（Any）

フィルタリング機能を使用すると、特定のコンポーネントのシステム ログ メッセージを表示できます。フィルタリングにより、メッセージ内容に基づいて特定のメッセージを検索できます。

フィルタリング機能は、UNIX ファイル検索ユーティリティ Grep を使用するため、Grep で使用可能なほとんどの構文を使用できます。たとえば、パターン マッチング用に Grep 互換の正規表現を使用できます。単一の語をフィルタとして使用したり、Grep でサポートされる正規表現を使用したりして内容を検索できます。

次の表に、システムログ フィルタで使用できる正規表現構文を示します。

表 69-6　システム ログ フィルタ構文

構文のコンポーネント	説明	例
.	任意の文字またはスペースと一致します	Admi. は、Admin、AdmiN、Admi1、および Admi& と一致します。
[[:alpha:]]	任意の英文字 1 字と一致します	[[:alpha:]]dmin は、Admin、bdmin、および Cdmin と一致します
[[:upper:]]	任意の大文字の英文字 1 字と一致します	[[:upper:]]dmin は、Admin、Bdmin、および Cdmin と一致します
[[:lower:]]	任意の小文字の英文字 1 字と一致します	[[:lower:]]dmin は、admin、bdmin、および cdmin と一致します
[[:digit:]]	任意の数字 1 字と一致します	[[:digit:]]dmin は、0dmin、1dmin、および 2dmin と一致します
[[:alnum:]]	任意の英数字 1 字と一致します	[[:alnum:]]dmin は、1dmin、admin、2dmin、および bdmin と一致します
[[:space:]]	タブを含む、任意のスペース 1 字と一致します	Feb[[:space:]]29 は 2 月 29 日のログと一致します。
*	その前にある文字または表現のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、および cabb と一致します [ab]* はすべてのものと一致します
?	ゼロ個または 1 個のインスタンスと一致します	ab? は、a または ab と一致します。
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します。

次の表では、[システムログ（System Log）] ページで使用できるフィルタの例をいくつか示します。

表 69-7　システムログ フィルタの例

次の条件を満たすすべてのログ エントリを検索する場合	使用するフィルタ
11 月 5 日に生成	Nov[[:space:]]*5
ユーザ名「Admin」を含む	Admin
11 月 5 日の認証デバッグ情報を含む	Nov[[:space:]]*5.*AUTH.*DEBUG

システム ログ内で特定のメッセージ内容を検索するには、次のようにします。

アクセス：Admin/Maint

手順 1　[システム（System）] > [モニタリング（Monitoring）] > [Syslog] を選択します。

[システムログ（System Log）] ページが表示されます。

手順 2　[フィルタ（filter）] フィールドに単語またはクエリを入力します。

使用できるフィルタ構文の詳細については、上記の表を参照してください。

（注）　Grep 互換の検索構文のみがサポートされます。たとえば、フィルタとして `ntp` を使ってすべての NTP 関連システム ログ メッセージを検索したり、`Nov` をフィルタとして使って 11 月に生成されたすべてのメッセージを検索したりできます。`Nov[[:space:]]*27` または `Nov.*27` を使用すると 11 月 27 日のメッセージを表示できますが、`Nov 27` または `Nov*27` を使ってこれらのメッセージを表示することはできません。

手順 3　オプションで、大文字と小文字が区別されるようにするには、[大文字と小文字を区別する（Case-sensitive）] をチェックします。（デフォルトでは、フィルタで大文字/小文字は区別されません）。

手順 4　オプションで、[除外（Exclusion）] をチェックすると、入力した条件に一致**しない**すべてのシステム ログ メッセージが検索されます。

手順 5　[移動（Go）] をクリックします。

フィルタに一致するメッセージが表示されます。