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。

以下の項では、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」（P.56-1）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」（P.56-11）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、Protectionライセンスを持つ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」（P.44-1）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

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 個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、アプライアンスはデータベースから最も古いデータをプルーニングし、その数を 100,000 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」（P.56-2）
- 「監査レコードの抑制」（P.56-4）
- 「監査ログ テーブルについて」（P.56-7）
- 「監査ログを使って変更を調査する」（P.56-8）
- 「監査レコードの検索」（P.56-9）

監査レコードの表示

ライセンス：任意

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。このほか、特定の要件に一致する情報のみ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については、「カスタム ワークフローの作成」（P.47-45）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 56-1　監査ログの操作

目的	操作
テーブル内のカラムの内容について理解する	「監査ログ テーブルについて」（P.56-7）にある詳細情報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	「イベント時間の制約の設定」（P.47-27）の詳細情報を参照してください。 イベント ビューを時間で制約した場合、イベント ビューには（グローバルかイベント固有かにかかわらず）アプライアンスで設定されている時間枠の外で生成されたイベントが表示される場合があることに注意してください。アプライアンスでスライド時間枠を設定した場合でも、これが発生する可能性があります。
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」（P.47-39）にある詳細情報を参照してください。
現在のワークフロー ページ内を移動する	「ワークフロー内の他のページへのナビゲート」（P.47-40）にある詳細情報を参照してください。
現在の制約を保持しながら、現在のワークフローのページ間を移動する	ワークフロー ページの左上にある、該当するページの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」（P.47-21）を参照してください。

表 56-1　監査ログの操作（続き）

目的	操作
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 1 つの値で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、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 ページに表示させるイベントの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制約を保持しながら、次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューのページ名には必ず「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
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 ビューが制約されることに注意してください（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 ビューのページ名には、必ず「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
監査レコードの削除	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、[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、[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。
一時的に別のワークフローを使用する	[(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」（P.47-19）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	[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」（P.47-42）を参照してください。
ブックマークの管理ページに移動する	[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」（P.47-42）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	[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」（P.44-2）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	[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」（P.56-8）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

ステップ 1　[System] > [Monitoring] > [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、[(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については、「イベント ビュー設定の設定」（P.58-3）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」（P.47-27）を参照してください。

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

監査イベントの操作

ライセンス：任意

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 [閉じる] 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 [Apply] をクリックします。カラムを無効にすると、あとで再び追加した場合を除き、そのカラムはセッション有効期間にわたって無効になります。最初のカラムを無効にした場合、[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 [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 ビューが制約されます（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 ビューのページ名には必ず「Table View」が含まれます。

詳細については、次のトピックを参照してください。

- 「イベントの制約」（P.47-36）
- 「複合的な制約の使用」（P.47-38）
- 「ドリルダウン ワークフロー ページのソート」（P.47-39）
- 「監査ログ テーブルについて」（P.56-7）

監査レコードの抑制

ライセンス：任意

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、ユーザーがオンライン 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 ユーザー 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　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ことを確認してください。

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、もはやそれらを抑制しないことを決定した場合、AuditBlock.*type* ファイルの内容を削除する必要がありますが、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/小文字を必ず正しく表記してください。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 56-2　監査ブロック タイプ

タイプ	説明
アドレス	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。部分的な IP アドレスを使用できます（ただしアドレスの先頭から照合されます）。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	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	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	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。部分的な文字列の照合を使用できます（ただしユーザ名の先頭から照合されます）。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、サブシステム Audit およびメッセージ Audit Filter *type* Changed 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 56-3　サブシステム名

名前	どの機能のユーザ インタラクションを含んでいるか
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
Alerting	アラート機能：電子メール、SNMP、syslog アラートなど
Audit Log	監査イベントの表示
Audit Log Search	監査イベントの検索
Command Line	コマンドライン インターフェイス
Configuration	電子メール アラート機能
COOP	継続的な運用機能
Date	イベント ビューの日時範囲
Default Subsystem	サブシステムが割り当てられていないオプション
Detection & Prevention Policy	侵入ポリシーのメニュー オプション
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表示
Event	侵入およびディスカバリ イベント ビュー
Events Clipboard	侵入イベント クリップボード
Events Reviewed	レビューされた侵入イベント
Events Search	イベント検索
Failed to install rule update *rule_update_id*	ルール更新のインストール
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
Health	ヘルス モニタリング
Health Events	ヘルス モニタリング イベントの表示
Help	オンライン ヘルプ
High Availability	高可用性（ハイ アベイラビリティ）機能
IDS Impact Flag	影響フラグの設定
IDS Policy	侵入ポリシー
IDSPolicy > *policy_name* > 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
Incidents	侵入インシデント
Insert Policy Apply Job	ポリシーの適用
Install	更新のインストール
Intrusion Events	侵入イベント
Login	Web インターフェイスのログイン/ログアウト機能

表 56-3　サブシステム名 （続き）

名前	どの機能のユーザ インタラクションを含んでいるか
Menu	メニュー オプション
Configuration export > *config_type* > *config_name*	特定のタイプ/名前の設定のインポート
Permission Escalation	ユーザ ロールのエスカレーション
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
Policy	侵入ポリシーを含むポリシー
Register	防御センターでのデバイスの登録
RemoteStorageDevice	リモート ストレージ デバイスの設定
Reports	レポート リスト機能およびレポート デザイナ機能。
Rules	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）
Rule Update Import Log	ルール更新のインポート ログの表示
Rule Update Install	ルール更新のインストール
Status	syslog およびホストやパフォーマンスの統計情報
System	システム全体のさまざまな設定
System Policy > *policy_name* Appliance > *appliance_name*	システム ポリシーの適用
Task Queue	タスク キューの表示
Users	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

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 56-4　監査ログのフィールド

フィールド	説明
Time	アプライアンスが監査レコードを生成した日時。
User	監査イベントをトリガーとして使用したユーザのユーザ名。
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、[System] > [Monitoring] > [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、[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。

表 56-4　監査ログのフィールド（続き）

フィールド	説明
Message	ユーザが実行した操作。 たとえば、`Page View` は [Subsystem] で示されたページをユーザが単に表示したことを意味します。`Save` は、ユーザがページの [Save] ボタンをクリックしたことを意味します。 FireSIGHT システムで行われた変更は比較アイコン（FireSIGHT システム）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。FireSIGHT システム詳細については、「監査ログを使って変更を調査する」（P.56-8）を参照してください。
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。
Count	各行に表示された情報に一致するイベントの数。[Count] フィールドは、制約を適用した後に 2 つ以上の同一行が生じた場合に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

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すると、[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。

[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。
- グリーンは、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

ステップ 1　[System] > [Monitoring] > [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 ビューが含まれないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックし、[Audit Log] を選択します。

ステップ 2　[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。

[Compare Configurations] ページが表示されます。タイトル バーの上の [Previous] または [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

監査レコードを検索して、特定のユーザ、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。使用できる検索条件を次の表に示します。監査の検索では、大文字と小文字が区別されないことに注意してください。たとえば、`Analyst01` と `analyst01` を検索すると同じ結果になります。

表 56-5　監査レコードの検索条件

検索フィールド	説明	例
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、アスタリスク（*）をワイルドカード文字として使用できます。	`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。
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、アスタリスク（*）をワイルドカード文字として使用できます。	たとえば、[System] > [Monitoring] > [Audit] および `*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。
Message	ユーザが実行したアクション、またはユーザーがページでクリックしたボタン。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。	`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。
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」（P.45-5）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。
Source 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。
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。

保存済みの検索をロードしたり削除したりする方法など、検索の詳細については、「イベントの検索」（P.45-1）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

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[Audit Log Events] を選択します。

監査ログ（Audit Log）の検索ページが表示されます。

ヒント　別の種類のイベントをデータベースで検索するには、[Table] ドロップダウン リストからそれを選択します。

ステップ 3　オプションで、検索を保存するには、[Name] フィールドに検索の名前を入力します。

名前を入力しない場合、検索の保存時に自動的に名前が作成されます。

ステップ 4　「監査レコードの検索条件」の表に示すように、該当するフィールドに検索条件を入力します。

複数の条件を入力すると、すべての基準を満たすレコードのみが検索で返されます。

ステップ 5　他のユーザが再使用できるような形式で検索を保存する場合には、[Save As Private] チェックボックスをクリアします。そうでない場合は、このチェック ボックスを選択したままにして、検索をプライベートとして保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[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、[(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については、「イベント ビュー設定の設定」（P.58-3）を参照してください。
- 既存の検索を変更している場合、[Save] をクリックすると変更内容が保存されます。
- [Save as New Search] をクリックすると、検索条件が保存されます。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられて保存され）、あとでそれを使用できます。

システム ログの表示

ライセンス：任意

システム ログ（syslog）ページは、アプライアンスのシステム ログ情報を示します。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」（P.56-11）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

ステップ 1　[System] > [Monitoring] > [Syslog] を選択します。

[System Log] ページが表示されます。防御センターにおけるこのページを以下に示します。

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

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。つまり、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。

注意　[System Log] ページでは、`OR` 式のパイプ文字を使用できません。たとえば、`[word_1|word_2]` を使用した場合、無効なフィルタ エラーを受け取ります。

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 56-6　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. Admin、AdmiN、Admi1、および Admi& と一致します
[[:alpha:]]	任意の英文字と一致します	[[: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式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 つのインスタンスと一致します	ab? 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\? alert? と一致します。

次の表では、[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 56-7　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 日に生成された	Nov[[:space:]]*5
ユーザ名「Admin」が含まれる	Admin
11 月 5 日の認証デバッグ情報が含まれる	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

ステップ 1　[System] > [Monitoring] > [Syslog] を選択します。

[System Log] ページが表示されます。

ステップ 2　[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、「システム ログ フィルタ構文」の表および「システム ログ フィルタの例」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。

ステップ 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、[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。）

ステップ 4　オプションで、[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。

ステップ 5　[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。