CHAPTER 14

ロギング

この章では、Cisco Identity Services Engine（ISE）に実装されているロギング メカニズムについて説明します。また、ロギング ターゲットの設定、ロギング カテゴリの編集、ロギング設定を行う手順についても説明します。この章の構成は、次のとおりです。

ロギングについて

Cisco ISE には、Cisco ISE によって提供されるサービスの監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部で収集するには、ターゲットと呼ばれる外部 syslog サーバを設定します。ロギング カテゴリについてで説明するように、ログは事前定義された各種のカテゴリに分類されます。ターゲット、重大度レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。

次のロギング関連タスクを実行するには、ISE 管理インターフェイスで [管理（Administration）] > [システム（System）] > [ロギング（Logging）] を選択します。

- ローカル ログ設定を行うには、「ローカル ログ設定」（P.14-2）を参照してください。
- リモート ロギング ターゲットについて理解し、それを作成するには、「リモート ロギング ターゲットについて」（P.14-2）を参照してください。
- ロギング カテゴリについて理解し、それを編集するには、「ロギング カテゴリについて」（P.14-5）を参照してください。
- メッセージ カタログを表示するには、「メッセージ カタログの表示」（P.14-8）を参照してください。

- デバッグ ログについて理解し、それを設定するには、「デバッグ ログ設定について」（P.14-9）を参照してください。
- ログ収集ステータスを表示するには、「ログ収集ステータスの表示」（P.14-11）を参照してください。

ローカル ログ設定

ローカル ログ格納期間を設定したり、ローカル ログを削除するには、このプロセスを使用します。

ロギング設定を行うには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ローカル ログ設定（Local Log Settings）] を選択します。

ステップ 2　次のフィールドを設定します。

a. [ローカル ログ格納期間（Local Log Storage Period）] : 設定ソースにログ エントリを保存しておく最大日数。

（注）　ディスク領域の浪費を避けるために、指定したローカル ログ格納期間中にログを削除できます。格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除（Delete Logs Now）] をクリックします。

ステップ 3　[保存（Save）] をクリックします。

リモート ロギング ターゲットについて

ロギング ターゲットとは、システム ログが収集される場所のことです。Cisco ISE では、ターゲットはログを収集して格納するサーバの IP アドレスを参照します。ログをローカルで生成して格納することも、外部サーバに FTP で送信することもできます。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector : ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe : プロファイラ Radius プローブのデフォルトの syslog ターゲット。

リモート ロギング ターゲットの設定

ISE のインストールの最後にローカルに設定するデフォルトのロギング ターゲットを使用することも、ログを格納する外部ターゲットを作成することもできます。

この項では、次のトピックを扱います。

- 「リモート ロギング ターゲットの表示」（P.14-3）
- 「リモート ロギング ターゲットの作成」（P.14-4）
- 「リモート ロギング ターゲットの編集」（P.14-4）
- 「リモート ロギング ターゲットの削除」（P.14-5）

リモート ロギング ターゲットの表示

事前定義されたリモート ロギング ターゲットおよびユーザ定義のリモート ロギング ターゲットを表示できます。フィルタを使用して特定のターゲットを検索することもできます。

リモート ロギング ターゲットを表示するには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

[リモート ロギング ターゲット（Remote Logging Targets）] ページに、既存のロギング ターゲットが一覧表示されます。

ステップ 2　[フィルタ（Filter）] をクリックし、次のいずれかのオプションを選択します。

- クイック フィルタ（Quick Filter）
- 拡張フィルタ（Advanced Filter）

クイック フィルタを実行するには、次の 1 つ以上の属性フィールドに検索条件を入力します。

- 名前（Name）
- IP アドレス（IP Address）
- タイプ（Type）
- 説明（Description）

拡張フィルタを実行するには、次の手順を実行して一致ルールを作成します。

- [フィルタ（Filter）] ドロップダウン リストから、次のいずれかのオプションを選択します。
  - 名前（Name）
  - IP アドレス（IP Address）
  - タイプ（Type）
  - 説明（Description）
- 2 番目のドロップダウン リストから、次のいずれかのオプションを選択します。
  - 次を含む（Contains）
  - 次を含まない（Does not contain）
  - 次に等しくない（Does not equal）
  - 次で終わる（Ends with）
  - 空白（Is empty）
  - 次に等しい（Is exactly (or equals)）
  - 空白ではない（Is not empty）
  - 次で始まる（Starts with）
- テキスト ボックスに、検索する値を入力します。
- フィルタ プロセスを起動するには [実行（Go）] をクリックし、検索条件を追加するにはプラス（[+]）をクリックします。
- [フィルタのクリア（Clear Filter）] をクリックすると、フィルタ プロセスがリセットされます。

目的のリモート ロギング ターゲットが表示されます。

リモート ロギング ターゲットの作成

外部ロギング ターゲットを作成するには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

[リモート ロギング ターゲット（Remote Logging Targets）] ページが表示されます。

[追加（Add）] をクリックします。

ステップ 2　[ログ コレクタ（Log Collector）] ページが表示されます。

ステップ 3　次のフィールドを設定します。

a. [名前（Name）] : 新しいターゲットの名前を入力します。

b. [ターゲット タイプ（Target Type）] : デフォルトで [Syslog] に設定されています。このフィールドの値は変更できません。

c. [説明（Description）] : 新しいターゲットの簡単な説明を入力します。

d. [IP アドレス（IP Address）] : ログを格納する宛先マシンの IP アドレスを入力します。

e. [ポート（Port）] : 宛先マシンのポート番号を入力します。

f. [ファシリティ コード（Facility Code）] : ロギングに使用する syslog ファシリティ コードを選択します。有効なオプションは、Local0 ～ Local7 です。

g. [最大長（Maximum Length）] : リモート ログ ターゲットのメッセージの最大長を入力します。有効なオプションは 200 ～ 1024 バイトです。

ステップ 4　[保存（Save）] をクリックします。

ステップ 5　[ロギング ターゲット（Logging Targets）] ページに移動し、新しいターゲットが作成されたことを確認します。

リモート ロギング ターゲットの編集

リモート ロギング ターゲットを編集するには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

[リモート ロギング ターゲット（Remote Logging Target）] ページが表示されます。

編集するロギング ターゲット名の隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

[ログ コレクタ（Log Collector）] ページが表示されます。

ステップ 2　必要に応じて次のフィールドの値を変更します。

- 名前（Name）
- ターゲット タイプ（Target Type）
- 説明（Description）
- IP アドレス（IP Address）
- ポート（Port）
- ファシリティ コード（Facility Code）

- 最大長（Maximum Length）

ステップ 3　[保存（Save）] をクリックします。

選択したログ コレクタの更新が完了しました。

リモート ロギング ターゲットの削除

リモート ロギング ターゲットを編集するには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [リモート ロギング ターゲット（Remote Logging Targets）] を選択します。

[ログ コレクタ（Log Collector）] ページが表示されます。

ステップ 2　削除するロギング ターゲットの隣のオプション ボタンをクリックにして、[削除（Delete）] をクリックします。

ステップ 3　確認ダイアログボックスで [OK] をクリックして、ロギング ターゲットを削除することを確認します。

ロギング カテゴリについて

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。Cisco ISE では、各ログにはログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギング カテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、および重大度レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ（[ポスチャ（Posture）]、[プロファイラ（Profiler）]、[ゲスト（Guest）]、[AAA（認証、許可、アカウンティング）（AAA (authentication, authorization, and accounting)）] など）が提供されており、これらにログ ターゲットを割り当てることができます。

表 14-1 に、Cisco ISE でデフォルトで使用可能な Cisco ISE の事前定義済みカテゴリを示します。

表 14-1　ロギング カテゴリ

親カテゴリ（Parent Category）	カテゴリ（Category）
AAA 監査（AAA Audit）	• AAA 監査（AAA Audit） • 失敗した試行（Failed Attempts） • 成功した認証（Passed Authentication）
AAA 診断（AAA Diagnostics）	• AAA 診断（AAA Diagnostics） • 管理者の認証と許可（Administrator Authentication and Authorization） • 認証フロー診断（Authentication Flow Diagnostics） • ID ストア診断（Identity Store Diagnostics） • ポリシー診断（Policy Diagnostics） • Radius 診断（Radius Diagnostics） • ゲスト（Guest）
アカウンティング（Accounting）	• アカウンティング（Accounting） • Radius アカウンティング（Radius Accounting）
管理および操作の監査（Administrative and Operational Audit）	• 管理および操作の監査（Administrative and Operational Audit）
ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）	• ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
ポスチャおよびクライアント プロビジョニングの診断（Posture and Client Provisioning Diagnostics）	• ポスチャおよびクライアント プロビジョニングの診断（Posture and Client Provisioning Diagnostics）
プロファイラ（Profiler）	• プロファイラ（Profiler）
システム診断（System Diagnostics）	• システム診断（System Diagnostics） • 分散管理（Distributed Management） • 内部操作診断（Internal Operations Diagnostics）
システム統計（System Statistics）	• システム統計（System Statistics）

カテゴリごとに関連するトラブルシューティング レポートの詳細については、「使用可能なレポート」（P.25-44）を参照してください。

この項では、次のトピックを扱います。

- 「ロギング カテゴリの検索」（P.14-6）
- 「ロギング カテゴリの編集」（P.14-8）

ロギング カテゴリの検索

[フィルタ（Filter）] を使用して、特定のカテゴリを検索できます。

カテゴリを検索するには、次の手順を実行します。

ステップ 1　ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択します。

[ロギング カテゴリ（Logging Categories）] ページに、既存のカテゴリが一覧表示されます。

ステップ 2　[フィルタ（Filter）] をクリックし、次のいずれかのオプションを選択します。

- クイック フィルタ（Quick Filter）
- 拡張フィルタ（Advanced Filter）

クイック フィルタを実行するには、次の 1 つ以上の属性フィールドに検索条件を入力します。

- 親カテゴリ（Parent Category）
- カテゴリ（Category）
- ターゲット（Targets）
- 重大度（Severity）
- ローカル ログ レベル（Local Log Level）

拡張フィルタを実行するには、次の手順を実行して一致ルールを作成します。

- [フィルタ（Filter）] ドロップダウン リストから、次のいずれかのオプションを選択します。
  - 親カテゴリ（Parent Category）
  - カテゴリ（Category）
  - ターゲット（Targets）
  - 重大度（Severity）
  - ローカル ログ レベル（Local Log Level）
- 2 番目のドロップダウン リストから、次のいずれかのオプションを選択します。
  - 次を含む（Contains）
  - 次を含まない（Does not contain）
  - 次に等しくない（Does not equal）
  - 次で終わる（Ends with）
  - 空白（Is empty）
  - 次に等しい（Is exactly (or equals)）
  - 空白ではない（Is not empty）
  - 次で始まる（Starts with）
- テキスト ボックスに、検索する値を入力します。
- フィルタ プロセスを起動するには [実行（Go）] をクリックし、検索条件を追加するにはプラス（[+]）をクリックします。
- [フィルタのクリア（Clear Filter）] をクリックすると、フィルタ プロセスがリセットされます。

目的のリモート ロギング カテゴリが表示されます。

ロギング カテゴリの編集

この項では、ログ重大度レベルを設定する方法、および選択したカテゴリのログが格納されるロギング ターゲットを選択する方法について説明します。

特定のロギング カテゴリの設定を編集するには、次の手順を実行します。

ステップ 1　Cisco ISE 管理インターフェイスで、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択します。

[ロギング カテゴリ（Logging Categories）] ページに、既存のカテゴリが一覧表示されます。

ステップ 2　編集するカテゴリの隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

編集ページが表示され、選択したカテゴリの詳細が示されます。

ステップ 3　次のフィールドの値を変更します。

（注）　[名前（Name）] フィールドは変更できません。

a. [ログ重大度レベル（Log Severity Level）] : 診断ロギング カテゴリでは、このドロップダウン リストを使用して重大度レベルを選択します。有効なオプションは次のとおりです。

- [重大（FATAL）] : 緊急事態。このオプションは、Cisco ISE を使用できないため、すぐに対応する必要があることを意味します。
- [エラー（ERROR）] : このオプションは、クリティカルまたはエラー状況を示します。
- [警告（WARN）] : このオプションは、正常であるが注意を必要とする状況を示します。これがデフォルトの状態です。
- [情報（INFO）] : このオプションは、情報メッセージを示します。
- [デバッグ（DEBUG）] : このオプションは、診断バグ メッセージを示します。

b. [ターゲット（Target）] : このセクションには、[使用可能（Available）] と [選択済み（Selected）] という 2 つのボックスがあります。[使用可能（Available）] ボックスには、論理（事前定義済み）と外部（ユーザ定義）という両方の既存のロギング ターゲットが含まれています。最初は空の [選択済み（Selected）] ボックスには、特定のカテゴリの選択済みターゲットが含まれます。左アイコンと右アイコンを使用して [使用可能（Available）] と [選択済み（Selected）] のボックス間でターゲットを転送することによって、カテゴリのターゲットを変更できます。

ステップ 4　[保存（Save）] をクリックします。

ステップ 5　[ロギング カテゴリ（Logging Categories）] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

メッセージ カタログの表示

[メッセージ カタログ（Message Catalog）] ページを使用して、表示される可能性があるすべてのログ メッセージを表示できます。

メッセージ カタログを表示するには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージ カタログ（Message Catalog）] を選択します。

[ログ メッセージ カタログ（Log Message Catalog）] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。このページで利用可能なデータは表示専用です。

各メッセージには、次のフィールドがあります。

- [カテゴリ名（Category Name）]：メッセージが属しているロギング カテゴリ
- [メッセージ クラス（Message Class）]：メッセージが属しているグループ
- [メッセージ コード（Message Code）]：メッセージに関連付けられている一意のメッセージ コード ID 番号
- [メッセージ テキスト（Message Text）]：メッセージの名前
- [重大度（Severity）]：メッセージに関連付けられている重大度レベル

デバッグ ログ設定について

デバッグ ログにより、ブートストラップ、アプリケーション設定、ランタイム、展開、モニタリングとレポート、および公開キー インフラストラクチャ（PKI）に関する情報が取得されます。

このプロセスを使用して、個別のコンポーネントのログ重大度レベルを設定し、ローカル サーバにデバッグ ログを格納して、評価とトラブルシューティングのためにシスコのテクニカル サポートにエクスポートできます。

（注）　デバッグ ログ設定はバックアップと復元の操作では保存されず、この設定はアップグレードでも保存されません。

デバッグ ログ レベルの設定

Cisco ISE ユーザ インターフェイスからデバッグ ログを設定するには、次の手順を実行します。

ステップ 1　[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログ設定（Debug Log Configuration）] を選択します。[ノード リスト（Node List）] ページに、ノードとそのペルソナが表示されます。

（注）　特にノード リストが大きい場合は、[フィルタ（Filter）] ボタンを使用して特定のノードを検索できます。

ステップ 2　ノードを選択して、[編集（Edit）] をクリックします。

[デバッグ レベル設定（Debug Level Configuration）] ページが表示されます。このページには、選択したノードで実行されているサービス、および個別のコンポーネントに対して設定されている現在のログ レベルに基づいたコンポーネントのリストが含まれています。

各ノードには次のコンポーネントが含まれています。

- Active Directory
- CacheTracker
- NotificationTracker
- ReplicationTracker
- cisco-mnt
- client
- com-cisco-nm
- cpm-clustering
- cpm-mnt
- epm-pap
- epm-pap-api.services
- epm-pdp
- epm-pip
- guest
- guestadmin
- guestauth
- guestportal
- identity-store-AD
- mnt-alert
- mnt-collector
- org-apache
- org-apache-cxf
- org-apache-digester
- org-displaytag
- pep-auth-manager-test
- posture
- profiler
- provisioning
- prrt-JNI
- runtime-AAA
- runtime-config
- runtime-logging
- sponsorportal
- swiss

（注）　[フィルタ（Filter）] ボタンを使用すると、このリストから特定のコンポーネントを検索できます。

ステップ 3　次のいずれかを実行して、ログ重大度レベルを調整します。

- コンポーネントの名前をクリックし、ドロップダウン リストから目的のログ レベルを選択してから、[保存（Save）] をクリックします。

  有効なオプションは次のとおりです。

  - [重大（FATAL）] : 緊急事態。このオプションは、Cisco ISE を使用できないため、すぐに対応する必要があることを意味します。
  - [エラー（ERROR）] : このオプションは、クリティカルまたはエラー状況を示します。
  - [警告（WARN）] : このオプションは、正常であるが注意を必要とする状況を示します。これがデフォルトの状態です。
  - [情報（INFO）] : このオプションは、情報メッセージを示します。
  - [デバッグ（DEBUG）] : このオプションは、診断バグ メッセージを示します。
- デバッグ ログ レベルを設定するコンポーネントの名前を選択してから、[編集（Edit）] をクリックします。このページで、[ログ レベル（Log Level）] ドロップダウン リストから目的のログ レベルを選択し、[保存（Save）] クリックします。

（注）　*runtime-AAA* コンポーネントのログ重大度レベルを変更すると、サブコンポーネント *prrt-JNI* のログ レベルも変更されます。サブコンポーネントのログ レベルを変更しても、その親コンポーネントには影響はありません。

選択したコンポーネントのデバッグ ログの設定が完了しました。

関連項目

- 「サポート バンドルのダウンロード」（P.24-43）
- 「デバッグ ログのダウンロード」（P.24-50）

ログ収集ステータスの表示

すべての Cisco ISE ノードのログ収集ステータスに関するレポートを取得できます。Cisco ISE 管理インターフェイスで、[操作（Operations）] > [システム（System）] > [レポート（Reports）] > [ログ収集ステータス（Log Collection Status）] を選択します。[ログ収集ステータス（Log Collection Status）] ページに、次の情報が表示されます。

- [ISE サーバ（ISE Server）] : ログが収集される Cisco ISE ノードの名前
- [直近の syslog メッセージ（Last Syslog Message）] : 最も新しい syslog メッセージの到着時刻
- [直近のエラー（Last Error）] : 最も新しいエラー メッセージの名前
- [直近のエラーの時刻（Last Error Time）] : 最も新しいエラー メッセージの到着時刻

ログ収集ステータスに関するレポートを生成する方法の詳細については、「システム レポート」（P.25-11）を参照してください。

ログ収集詳細の表示

[ログ収集詳細（Log Collection Details）] ページを使用して、直近の syslog メッセージ、ログ設定の変更内容、サーバのエラーなど、サーバ ログの詳細を表示できます。Cisco ISE 管理インターフェイスで、[操作（Operations）] > [システム（System）] > [レポート（Reports）] > [ログ収集ステータス

（Log Collection Status）] を選択します。[ログ収集ステータス（Log Collection Status）] ページが表示されます。ノードをクリックして [ログ収集詳細（Log Collection Details）] ページを表示します。このページには、選択したノードに関する次の情報が含まれています。

- [ログ名（Log Name）] : ログが収集されるログ カテゴリの名前
- [直近の syslog メッセージ（Last Syslog Message）] : 最も新しい syslog メッセージの到着時刻
- [直近のエラー（Last Error）] : 最も新しいエラー メッセージの名前
- [直近のエラーの時刻（Last Error Time）] : 最も新しいエラー メッセージの到着時刻

ログ収集ステータスに関するレポートを生成する方法の詳細については、「システム レポート」（P.25-11）を参照してください。