CHAPTER 26

レポート

モニタリング機能およびトラブルシューティング機能とともに Cisco Identity Services Engine（ISE）レポートを使用して、集中管理する場所からのトレンドの分析、システム パフォーマンスおよびネットワーク アクティビティのモニタを行います。詳細については、第 25 章「モニタリングおよびトラブルシューティング」を参照してください。

この章では、Cisco ISE で使用可能なレポートの種類について説明します。また、レポート データを使用したり、より効率的に使用するためにデータを整理したりするさまざまな方法についても説明します。

この章では、次のトピックについて取り上げます。

Cisco ISE レポート

Cisco ISE では、ネットワーク全体からログおよび設定データが収集されます。これらのデータが表示および分析できるようにレポートに集約されます。Cisco ISE には、使用可能な事前定義されたレポートが用意されており、必要に応じてカスタマイズできます。

Cisco ISE レポートは事前設定されており、認証、セッション トラフィック、デバイス管理、設定と管理、およびトラブルシューティングに関連する情報の論理的なカテゴリに分類されます。すべての Cisco ISE レポートのリストについては、「使用可能なレポート」（P.26-7）を参照してください。

ここでは、次のトピックについて取り上げます。

レポートの実行および表示

ここでは、Reports View を使用してレポートを実行、表示、およびナビゲートする方法について説明します。レポートにデータを表示する時間の増分を指定できます。

ステップ 1　[操作（Operations）] > [レポート（Reports）] > [ISE レポート（ISE Reports）] を選択します。

ステップ 2　使用可能なレポート カテゴリからレポートをクリックします。

ステップ 3　レポートを実行する 1 つ以上のフィルタを選択します。各レポートには、大文字と小文字が区別される使用可能な異なるフィルタがあり、それらには必須のものと任意のものがあります。

ステップ 4　フィルタに適切な値を入力します。

ステップ 5　レポートを実行します。

関連項目

- 「レポートのエクスポート」（P.26-2）
- 「ISE レポートのスケジューリングおよび保存」（P.26-3）
- 「お気に入りレポートの追加」（P.26-4）
- 「使用可能なレポート」（P.26-7）

レポートのナビゲーション

レポート出力から詳細情報を取得できます。たとえば、5 か月間のレポートを生成した場合、グラフと表に月を基準としたレポートの集計データが示されます。

表で特定の値をクリックすると、この特定のフィールドに関連する別のレポートを表示できます。たとえば、認証概要レポートには、ユーザまたはユーザ グループの失敗したカウントが表示されます。失敗したカウントをクリックすると、認証概要レポートがその特定の失敗したカウント用に開かれます。

レポートのエクスポート

レポート データは、カンマ区切り形式（.csv）ファイルとして Excel スプレッドシートにエクスポートできます。データをエクスポートすると、レポートの場所を詳述した電子メールが受信されます。

（注）　プライマリ PAP ノードを使用することによってのみ、レポート データを .csv 形式にエクスポートできます。

ステップ 1　「レポートの実行および表示」（P.26-2）の説明に従ってレポートを実行します。

ステップ 2　レポートの概要ページの右上隅の [エクスポート（Export）] をクリックします。

ステップ 3　エクスポートするデータ カラムを指定します。

ステップ 4　ドロップダウン リストからリポジトリを選択します。

ステップ 5　[エクスポート（Export）] をクリックします。

（注） レポートをエクスポートしたあとで英語以外の文字を正しく表示するには、UTF-8 文字エンコーディングを有効にして、Microsoft Excel にファイルをインポートする必要があります。UTF-8 文字エンコーディングを有効にしないで、エクスポートした .csv ファイルを Microsoft Excel で直接開くことを選択した場合、レポートの英語以外の文字は文字化けして表示されます。

次のレポートはエクスポートできません。

- 認証概要
- 健全性の概要
- RBACL ドロップ概要
- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

関連項目

「通知をサポートするように SMTP サーバを設定」（P.5-5）

ISE レポートのスケジューリングおよび保存

レポートはカスタマイズして、変更を新規レポートとして保存するか、またはデフォルトのレポート設定を復元できます。

特定の時間または時間間隔で実行および再実行するように ISE レポートをカスタマイズおよびスケジューリングすることもできます。レポートが生成されたら、電子メール通知を送受信することもできます。

（注） プライマリ PAP ノードを使用することによってのみ、ISE レポートを保存またはスケジューリング（カスタマイズ）できます。

ステップ 1　「レポートの実行および表示」（P.26-2）の説明に従ってレポートを実行します。

ステップ 2　レポートの概要ページの右上隅の [名前を付けて保存（Save As）] をクリックします。

ステップ 3　[レポート（Report）] または [スケジュール設定されたレポート（Scheduled Report）] を選択します。

ステップ 4　ダイアログボックスに必要な詳細を入力します。

ステップ 5　[新規として保存（Save as New）] をクリックします。

次のレポートはスケジューリングできません。

- 認証概要
- 健全性の概要

- RBACL ドロップ概要
- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

お気に入りレポートの追加

事前設定済みシステム レポートおよびカスタマイズしたレポートは、お気に入りリストに追加できます。

ブラウザでお気に入りの Web サイトをブックマークに追加するのと同様に、頻繁に使用するレポートをお気に入りのリストに追加して、見つけやすくすることができます。お気に入りレポートのパラメータを表示および編集した後、再利用のために、カスタマイズしたレポートを保存できます。

（注）　各管理者アカウントには、1 つ以上の管理ロールが割り当てられています。アカウントに割り当てられているロールによっては、この項で説明するタスクを実行できない場合があります。

ステップ 1　「レポートの実行および表示」（P.26-2）の説明に従ってレポートを実行します。

ステップ 2　レポートの概要ページの右上隅の [お気に入り（Favorites）] をクリックします。

お気に入りリストにそのレポートが表示されます。

（注）　プライマリ PAP ノードを使用することによってのみ、事前設定済みシステム レポートをお気に入りリストに追加できます。

Cisco ISE のアクティブな RADIUS セッション

Cisco ISE では、ライブ セッション用の動的な許可変更（CoA）機能が提供されます。この機能を使用すると、アクティブな RADIUS セッションを動的に制御できます。次のタスクを実行するために再認証または接続解除要求をネットワーク アクセス デバイス（NAD）に送信できます。

- 認証に関連する問題のトラブルシューティング：[セッション再認証（Session reauthentication）] オプションを使用して、再認証を試みることができます。ただし、アクセスを制限するためにこのオプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[ポート シャットダウンによるセッション終了（Session termination with port shut down）] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。ただし、RADIUS プロトコルでは、シャットダウンされたポートを再度有効にするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サプリカントまたはクライアントを持たないエンドポイントに対して [ポート バウンスでのセッション終了（Session termination with port bounce）] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。

- エンドポイントへの更新された許可ポリシーのプッシュ：[セッション再認証（Session reauthentication）] オプションを使用して、管理者の裁量に基づいた既存のセッションの許可ポリシーの変更などの、更新されたポリシー設定を適用できます。たとえば、ポスチャ確認が有効である場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントのアイデンティティおよびポスチャが確認された後、セッション再認証コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の許可ポリシーを取得できるようにすることが可能です。

デバイスによって CoA コマンドが認識されるためには、適切にオプションを設定することが重要です。

CoA が適切に動作するには、動的な許可変更を必要とする各デバイスの共有秘密情報を設定する必要があります。Cisco ISE では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行において、共有秘密情報設定が使用されます。詳細については、第 14 章「ユーザおよび外部 ID ソースの管理」を参照してください。

（注） このリリースの Cisco ISE では、表示可能な認証されたエンドポイント セッションの最大数が 100,000 に制限されています。

関連項目

「RADIUS セッションの許可の変更」（P.26-5）

RADIUS セッションの許可の変更

ネットワークの一部のネットワーク アクセス デバイスでは、リロード後にアカウンティング停止パケットまたはアカウンティング オフ パケットが送信されないことがあります。このため、[セッション ディレクトリ（Session Directory）] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。

アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、最新のセッションを選択する必要があります。

ステップ 1　[操作（Operations）] > [認証（Authentications）] を選択します。

ステップ 2　[ライブ セッションの表示（Show Live Session）] にビューを切り替えてください。

ステップ 3　CoA を発行する RADIUS セッションの CoA リンクをクリックし、次のいずれかのオプションを選択します。

（注）　インライン ポスチャ ノードについては、ワイヤレス LAN コントローラ（WLC）が使用されている場合、使用可能なオプションは、[セッション再認証（Session reauthentication）] および [セッション終了（Session termination）] の 2 つのみとなります。

- [SAnet セッション クエリー（SAnet Session Query）] : SAnet でサポートされるデバイスからのセッションに関する情報をクエリーするために使用します。
- [セッション再認証（Session reauthentication）] : セッションを再認証します。
- [最後の方式でのセッション再認証（Session reauthentication with last）] : そのセッションに対して、最後に成功した認証方式を使用します。
- [再実行によるセッション再認証（Session reauthentication with rerun）] : 設定されている認証方式を最初から実行します。

（注）　[最後の方式でのセッション再認証（Session reauthentication with last）] オプションおよび [再実行によるセッション再認証（Session reauthentication with rerun）] オプションは、Cisco IOS ソフトウェアで現在サポートされていません。

- [セッション終了（Session termination）] : 単にセッションを終了します。スイッチは、異なるセッションでクライアントを再認証します。
- [ポート バウンスでのセッション終了（Session termination with port bounce）] : セッションを終了し、ポートを再起動します。
- [ポート シャットダウンによるセッション終了（Session termination with port shut down）] : セッションを終了し、ポートをシャットダウンします。

ステップ 4　[実行（Run）] をクリックして、選択した再認証または終了オプションとともに CoA を発行します。

CoA に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない。
- アイデンティティまたは許可ポリシーに変更があった。
- 共有秘密が一致しない。

ステップ 5　変更を保存する方法については、「ISE レポートのスケジューリングおよび保存」（P.26-3）を参照してください。

関連項目

「予期しない RADIUS 認証の結果のトラブルシューティング」（P.25-18）を参照してください。失敗した動的な CoA は、失敗した RADIUS 認証として表示されます。

CoA、ポリシー、およびプロファイルの詳細については、次を参照してください。

- 「許可ポリシーとサポートされているディクショナリ」（P.20-4）
- 「許可ポリシーの設定」（P.20-8）
- 第 21 章「Cisco ISE エンドポイント プロファイリング ポリシー」
- 第 23 章「クライアント ポスチャ ポリシーの設定」
- 「認証の後に Cisco ISE が CoA を発行しない」（P.G-32）
- 「CoA がクライアント マシンで開始しない」（P.G-3）

- 「Cisco ISE に RADIUS サーバのエラー メッセージ エントリが表示される」（P.G-17）
- 「RADIUS サーバの接続性に関する問題（Cisco ISE にエラー メッセージ エントリが表示されない場合）」（P.G-18）

使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

表 26-1　使用可能なレポート

レポート名	説明	ロギング カテゴリ
認証サービス ステータス		
AAA の診断	AAA 診断レポートは、Cisco ISE とユーザ間のすべてのネットワーク セッションの詳細を提供します。ユーザがネットワークにアクセスできない場合、トレンドを識別し、問題が特定のユーザ隔離されているか、またはより広範囲の問題を示しているかを識別するために、このレポートを確認できます。 このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、次のロギング カテゴリを選択します。ポリシー診断、ID ストア診断、認証フロー診断、および RADIUS 診断。
RADIUS アカウンティング（RADIUS Accounting）	RADIUS アカウンティング レポートは、ユーザがネットワーク上に存在した時間を識別します。ユーザがネットワークにアクセスできない場合、Cisco ISE がネットワーク接続問題の原因であるかどうかを識別するには、このレポートを使用できます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[RADIUS アカウンティング（RADIUS Accounting）] を選択します。
RADIUS エラー	RADIUS エラーを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスから廃棄された認証/アカウンティング要求）、EAP 接続タイムアウトおよび未知の NAD をチェックできます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[失敗した試行（Failed Attempts）] を選択します。
RADIUS 認証	RADIUS 認証レポートを使用すると、認証失敗および成功の履歴を確認できます。ユーザがネットワークにアクセスできない場合、考えられる原因を識別するためにこのレポートの詳細を確認できます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、次のロギング カテゴリを選択します。成功した認証および失敗した試行。

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
認証概要	認証概要レポートは、RADIUS 認証に基づいています。それにより、最も一般的な認証および認証失敗の原因を特定することができます。たとえば、ある Cisco ISE サーバが他のサーバよりもはるかに多くの認証を処理している場合、負荷を適切に分散するためにユーザを別の Cisco ISE サーバに再割り当てする場合があります。 （注）　認証概要レポートまたはダッシュボードは失敗または成功した認証に対応する最新のデータを収集して表示するため、レポートの内容は数分の遅延の後に表示されます。	—
OCSP モニタリング	OCSP モニタリング レポートは、Online Certificate Status Protocol（OCSP）サービスのステータスを指定します。Cisco ISE が正常に証明書サーバに連絡し、証明書ステータス監査を提供できるかどうかを識別します。Cisco ISE によって実行されたすべての OCSP 証明書検証操作の概要が提供されます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[システム診断（System Diagnostics）] を選択します。
展開ステータス		
管理者ログイン	管理者ログイン レポートは、すべての管理者ログインの監査証跡を提供します。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[管理および操作の監査（Administrative and Operational audit）] を選択します。
内部管理者の概要	内部管理者の概要レポートを使用すると、管理者ユーザのエンタイトルメントを確認できます。このレポートから、管理者ログイン レポートおよび変更設定監査レポートにもアクセスでき、それにより、管理者ごとにこれらの詳細を表示できます。	—
変更設定監査	変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[管理および操作の監査（Administrative and Operational audit）] を選択します。
セキュアな通信の監査	セキュアな通信の監査レポートは、セキュアなチャネルから発生するすべての通信に関する監査詳細を提供します。このレポートは、シスコの共通基準要件に適合します。	—

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
操作監査	操作監査レポートは、次のような操作の変更に関する詳細を提供します。バックアップの実行、Cisco ISE ノードの登録、またはアプリケーションの再起動。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[管理および操作の監査（Administrative and Operational audit）] を選択します。
システム診断	システム診断レポートは Cisco ISE ノードのステータスの詳細を提供します。Cisco ISE ノードが登録できない場合、問題をトラブルシューティングするためにこのレポートを確認できます。 このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、次のロギング カテゴリを選択します。内部操作診断、分散管理、管理者の認証と許可。
健全性の概要	健全性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードは過去 24 時間のデータしが表示しませんが、このレポートを使用するとより多くの履歴データを確認できます。 データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。	—
ネットワーク デバイスのセッション ステータス	ネットワーク デバイスのセッション ステータス概要レポートを使用すると、直接スイッチにログインせずにスイッチ設定を表示することができます。 Cisco ISE は SNMP クエリーを使用してこれらの詳細にアクセスするので、ネットワーク デバイスが SNMP v1/v2c を使用して設定されている必要があります。 ユーザにネットワークの問題が発生している場合に、このレポートは、問題が Cisco ISE ではなくスイッチの設定に関連しているかどうかを識別するのに役立ちます。	—

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
データ消去の監査	データ消去の監査レポートは、ロギング データが消去されている時間を記録します。 このレポートは、データ消去の 2 つのソースを反映します。 毎日午前 4 時に、Cisco ISE は、[管理（Administration）] > [メンテナンス（Maintenance）] > [データ消去（Data Purging）] ページで設定した基準に一致するロギング ファイルがあるかどうかを確認します。あった場合は、ファイルが削除され、このレポートに記録されます。さらに、Cisco ISE は、常にログ ファイルに使用される記憶域を最大 80% に維持します。1 時間ごとに、Cisco ISE はこの割合を確認し、80% のしきい値に再び到達するまで、最も古いデータが削除されます。この情報もこのレポートに記録されます。	—
設定が誤っているサプリカント	特定のサプリカントが失敗試行を行うので、設定が誤っているサプリカントのレポートは、設定が誤っているサプリカントの一覧および統計情報を提供します。修正処置を行い、設定が誤っているサプリカントを修正すると、レポートはレポートに修正済み確認を表示します。 **（注）** レポートを実行するには、RADIUS 抑制を有効にする必要があります。	—
設定が誤っている NAS	設定が誤っている NAS レポートは、通常、アカウンティング情報を頻繁に送信するときに、アカウンティング頻度が不正確な NAD に関する一般情報を提供します。修正処置を行い、設定が誤っている NAD を修正すると、レポートはレポートに修正済み確認を表示します。 **（注）** レポートを実行するには、RADIUS 抑制を有効にする必要があります。	—
エンドポイントとユーザ		
クライアント プロビジョニング	クライアント プロビジョニング レポートは、特定のエンドポイントに適用されるクライアント プロビジョニング エージェントについて示します。各エンドポイントに適用されるポリシーを確認してエンドポイントが正しくプロビジョニングされたことを確認するには、このレポートを使用できます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[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）] および [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）] を選択します。

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
現在のアクティブなセッション	現在アクティブなセッション レポートを使用すると、指定の期間内のその時点でネットワーク上に存在していた者に関する詳細を含むレポートをエクスポートできます。 ユーザがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。	—
ゲスト アクティビティ	ゲスト アクティビティ レポートは、ゲスト ユーザがアクセスしている Web サイトに関する詳細を提供します。このレポートは、セキュリティ監査の目的で使用し、ゲスト ユーザがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。 ゲスト トラフィックに使用されるネットワーク アクセス デバイス（NAD）上で HTTP インスペクションも有効にする必要があります。この情報は、NAD によって Cisco ISE に送り返されます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[成功した認証（Passed Authentications）] を選択します。
ゲスト アカウンティング	ゲスト アカウンティング レポートは RADIUS アカウンティング レポートのサブセットです。アクティブなゲストまたはゲスト ID グループに割り当てられたすべてのユーザは、このレポートに表示されます。	—
ゲスト スポンサー概要	ゲスト スポンサー概要レポートには、各スポンサーによって作成されたすべてのゲスト ユーザが表示されます。スポンサー名をクリックして、そのゲスト ユーザの詳細を表示します。	—
エンドポイント セッション履歴	エンドポイント セッション履歴レポートは、RADIUS アカウンティングに基づいています。つまり、エンドポイントごとにすべてのネットワーク セッションの履歴レポートを表示します。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[成功した認証（Passed Authentications）] および [RADIUS アカウンティング（RADIUS Accounting）] を選択します。
モバイル デバイス管理	モバイル デバイス管理レポートは、Cisco ISE と外部モバイル デバイス管理（MDM）サーバ間の統合に関する詳細を提供します。 MDM サーバに直接ログインせずに、MDM サーバによってプロビジョニングされたエンドポイントを確認するには、このレポートを使用できます。また、登録および MDM コンプライアンス ステータスなどの情報が表示されます。	—

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
Posture Detail Assessment	Posture Detail Assessment レポートは、特定のエンドポイントのポスチャ コンプライアンスに関する詳細を提供します。エンドポイントは以前ネットワークにアクセスできていたのに、突然ネットワークにアクセスできなくなった場合、ポスチャの違反が発生したかどうかを決定するためにこのレポートを使用できます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[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）] および [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）] を選択します。
プロファイリングされたエンドポイントの概要	プロファイリングされたエンドポイントの概要レポートは、ネットワークにアクセスしているエンドポイントに関するプロファイリングの詳細を提供します。 **（注）** Cisco IP Phone など、セッション時間を登録しないエンドポイントの場合、[エンドポイント（Endpoint）] セッション時間フィールドに、[該当なし（Not Applicable）] と表示されます。	[管理（Administration）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] を選択し、[プロファイラ（Profiler）] を選択します。
エンドポイント プロファイルの変更	エンドポイント プロファイルの変更レポートは、次の 2 つの目的に使用されます。 • 特定のエンドポイントのプロファイルの変更を比較して、最新のプロファイルが適用されていることを確認します。 • プロファイラ フィード サービス（Cisco ISE の拡張ライセンスで使用可能）によって開始されたプロファイルの変更を表示します。	
エンドポイント（MAC アドレス）別上位認証	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行
ユーザ別上位認証	ユーザ別上位認証レポートは、ネットワークにアクセスするために各ユーザが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行
User Change Password Audit	User Change Password Audit レポートは、従業員のパスワード変更に関する検証を表示します。	管理および操作の監査
サプリカント プロビジョニング	サプリカント プロビジョニング レポートは、従業員のパーソナル デバイスにプロビジョニングされたサプリカントに関する詳細を提供します。	ポスチャおよびクライアント プロビジョニングの監査
登録済みエンドポイント	登録済みエンドポイント レポートは、従業員によって登録されているすべてのパーソナル デバイスを表示します。	—
セキュリティ グループ アクセス		

表 26-1　（続き）使用可能なレポート

レポート名	説明	ロギング カテゴリ
RBACL ドロップ概要	RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスだけで使用できるセキュリティ グループ アクセス（SGA）機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 ユーザが特定のポリシーまたはアクセスに違反した場合、パケットがドロップされ、このレポートに示されます。	—
ユーザ別上位 N 個の RBACL ドロップ	ユーザ別上位 N 個の RBACL ドロップレポートは、拡張 Cisco ISE ライセンスだけで使用できるセキュリティ グループ アクセス（SGA）機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 このレポートは、特定のユーザ別にポリシー違反（パケット ドロップに基づく）を表示します。	—