# レポート



## Cisco ISE 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リングを行います。

Cisco ISE はネットワーク全体からログおよび設定データを収集します。その後、表示と分析のために、データが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する情報の論理カテゴリにグループ化されます。

**関連トピック**


レポートの実行および表示 （4 ページ）

レポートのエクスポート （4 ページ）

使用可能なレポート （9 ページ）

# レポート フィルタ

レポートには、シングルセクション レポートとマルチセクション レポートの 2 種類があります。シングルセクション レポートには 1 つのグリッドが含まれており（RADIUS 認証レポート）、マルチセクション レポートには複数のグリッドが含まれており（認証概要レポート）、データがグラフと表の形式で示されます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

マルチセクション レポートには、入力が必要な必須拡張フィルタが 1 つ以上含まれていることがあります。たとえば、健全性の概要レポート（[操作（Operations）] > [レポート（Reports）] >[診断（Diagnostics）]ページ）をクリックすると、2 つの必須拡張フィルタ（[サーバ（Server）] と [時間範囲（Time Range）]）が表示されます。レポートを生成するには、この両方のフィルタで演算子コマンド、サーバ名、必要な値を指定し、[実行（Go）]をクリックする必要があります。プラス記号（+）をクリックして新しい拡張フィルタを追加できます。マルチセクション レポートは PDF 形式でのみエクスポートできます。特定の時刻または時間間隔で Cisco ISE マルチセクション レポートを実行または再実行するようにスケジュールすることはできません。

（注） レポートをクリックすると、デフォルトでは最新のデータが生成されます。ただし一部のマルチセクション レポートでは、時間範囲以外にもユーザが入力する必要のある項目があります。

シングルセクション レポートでは、デフォルトでクイック フィルタが 1 番目の行として表示されます。フィールドには、検索基準を選択できるドロップダウン リストまたはテキスト ボックスが含まれています。

拡張フィルタには、1 つ以上の内部条件を含む外部条件が含まれています。外部条件では、検索で指定された内部条件すべてに一致する必要があるか、またはいずれかに一致する必要があるかを指定します。内部条件には、カテゴリ（[エンドポイント ID（Endpoint ID）]、[ID グループ（Identity Group）]）、メソッド（Contains、Does Not Contain などの演算子コマンド）、および時間範囲を条件として指定するために使用される 1 つ以上の条件が含まれています。

[クイック フィルタ（Quick Filter）] を使用すると、[記録日時（Logged At）] ドロップダウン リストから日付または時刻を選択し、過去 30 日以内にログインしたデータ セットのレポートを生成できます。30 日より前の日付または時刻のレポートを生成する場合は、[高度なフィルタ（Advanced Filters）] を使用して、ドロップダウン リストの [カスタム（Custom）] オプションの [開始日（From）] と [終了日（To）] のフィールドに必要な時間枠を設定します。

# クイック フィルタ条件の作成

ここでは、クイック フィルタ条件の作成方法を説明します。クイック フィルタ条件はシングルセクション レポートでのみ作成できます。

**ステップ 1** **[操作（Operations）] > [レポート（Reports）]** を選択し、必要なレポートをクリックします。

**ステップ 2** [設定（Settings）] ドロップダウンリストから必須フィールドを選択します。

**ステップ 3** データをフィルタリングするため、必須フィールドでドロップダウンリストから選択するか、または特定の文字を入力できます。検索では Contains 演算子コマンドが使用されます。たとえば、「K」で始まるテキストをフィルタリングするには K と入力し、テキスト内の任意の位置に「geo」が含まれているテキストをフィルタリングするにはgeoと入力します。また、アスタリスク（*）を使用することもできます。たとえば、*abc で始まり *def で終わる正規表現などです。

クイック フィルタで使用される条件には、contains、starts with、ends with、starts with or ends with、および OR 演算子で結合する複数の値があります。

**ステップ 4** Enter キーを押します。

# 拡張フィルタ条件の作成

ここでは、拡張フィルタ条件の作成方法を説明します。拡張フィルタは、シングルセクション レポートとマルチセクション レポートで作成できます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

**ステップ 1** **[操作（Operations）] > [レポート（Reports）]** を選択し、必要なレポートをクリックします。

**ステップ 2** [フィルタ（Filters）] セクションで [一致（Match）] 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。

a) 指定したすべての条件に一致する必要がある場合は、[すべて（All）] を選択します。

b) 指定したいずれか 1 つの条件に一致すればよい場合は、[いずれか（Any）] を選択します。

**ステップ 3** [時間範囲（Time Range）] ドロップダウンリストから必要なカテゴリを選択します。

**ステップ 4** [演算子コマンド（Operator Commands）] ドロップダウンリストから、必要なコマンドを選択します。たとえば、特定の文字で始まるテキストや（[次の文字で始まる（Begin With）] を使用）、テキスト内の任意の位置に特定の文字が含まれているテキスト（[次の文字を含む（Contains）] を使用）をフィルタリングできます。あるいは、[ログに記録された時刻（Logged Time）] と対応する [カスタム（Custom）] オプションを選択し、カレンダーからデータをフィルタリングする期間の開始日時と終了日時を指定します。

**ステップ 5** [時間範囲（Time Range）] ドロップダウンリストから必要なオプションを選択します。

**ステップ 6** [移動（Go）] をクリックします。

今後の参照のために、フィルタリングされたレポートを保存し、[フィルタ（Filter）] ドロップダウンリストから取得することができます。

# 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。デフォルトでは、レポートをクリックすると過去7日間のデータが生成されます。各レポートでは、ページごとに500行のデータが表示されます。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。

また、各ワークセンターの[レポート（Reports）]リンクに移動して、ワークセンター固有の一連のレポートを確認することもできます。

**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、異なるフィルタを使用できます。フィルタの一部は必須で一部は任意選択です。

**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** [移動（Go）]をクリックします。

**関連トピック**

レポートのエクスポート （4 ページ）
使用可能なレポート （9 ページ）

# 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ヵ月の期間に1つのレポートを生成した場合、グラフと表には月単位の目盛りでレポートの集約データが表示されます。

表内の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、その特定の失敗したカウントについての認証概要レポートが開きます。

# レポートのエクスポート

次のファイル形式でレポートデータをエクスポートできます。

- カンマ区切り値（.csv）ファイルとしての Excel スプレッドシート。データをエクスポートすると、レポートの場所を詳細に示した電子メールを受信します。
- ローカルディスクに保存できる Microsoft Excel のカンマ区切り値（.csv）ファイル。
- ローカルディスクに保存できる Adobe Acrobat Document（.pdf）ファイル。

（注） Microsoft Excel 形式の場合、エクスポートできるのは 5000 レコードです。PDF ファイル形式の場合、エクスポートできるのは 1000 レコードです。

次のレポートは PDF ファイル形式でののみエクスポートできます。

- 認証概要（Authentication Summary）
- 健全性の概要
- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- 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

（注） レポートをエクスポートした後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 で直接開いた場合、レポートの英語以外の文字は文字化けした状態で表示されます。

（注） レポート データは、プライマリ PAN からのみ .csv 形式にエクスポートできます。

**ステップ 1** 「レポートの実行と表示」の項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 サマリー ページの右上隅にある [エクスポート（Export）][エクスポート先（Export To）] 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。

# Cisco ISE レポートのスケジュールと保存

レポートをカスタマイズし、変更内容を新しいレポートとして保存するか、またはレポートサマリーページの右上隅にある [マイレポート（My Reports）] でデフォルトのレポート設定を復元できます。

Cisco ISE レポートをカスタマイズおよびスケジュールして、特定の時間または時間間隔で実行および再実行することもできます。生成されたレポートに関する電子メール通知を送受信することもできます。

**時間単位**の頻度でレポートをスケジュールする場合は、レポートを複数の日にわたって実行することはできますが、日をまたぐ時間枠を設定することはできません。

たとえば、時間単位のレポートを 2019 年 5 月 4 日から 5 月 8 日までスケジューリングする場合は、時間間隔を各日の午前 6 時から午後 11 時までに設定することはできますが、ある日の午後 6 時から翌日の午前 11 時までに設定することはできません。後者の場合、Cisco ISE は、時間範囲が無効であることを示すエラー メッセージを表示します。

（注） 外部の管理者（Active Directory の管理者など）が電子メール ID フィールドを指定せずにスケジュール設定されたレポートを作成すると、電子メール通知は送信されません。

次のレポートはスケジュールできません。

- 認証概要（Authentication Summary）
- 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

（注） Cisco ISE レポートの保存またはスケジューリング（カスタマイズ）は、PAN からのみ実行できます。

**ステップ 1** 「レポートの実行と表示」の項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 サマリー ページの右上隅の [マイ レポート（My Reports）] をクリックします。

**ステップ 3** 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 4** [新規として保存（Save as New）] をクリックします。

保存済みレポートに戻ると、すべてのフィルタ オプションがデフォルトでオンになります。使用しないフィルタはオフにします。

[マイレポート（My Reports）] カテゴリから、保存したレポートを削除することもできます。

# 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 shutdown）] 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、Session reauthentication 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。

（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。

関連トピック

RADIUS セッションの許可の変更 （8 ページ）

# 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）] > [RADIUSライブログ（RADIUS Livelog）]** の順に選択します。

**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。

- [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。CoA をサポートする ASA デバイスに確立されるセッションにこのオプションを選択すると、セッションポリシープッシュ CoA が呼び出されます。
- [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。

# 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。

ロギングカテゴリの syslog を生成するには、[ログの重大度レベル（Log Severity Level）] を [情報（Info）] に設定します。

- **[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。
- syslog を生成する必要があるロギングカテゴリをクリックします。
- [ログの重大度レベル（Log Severity Level）] フィールドで、ドロップダウンメニューから [情報（Info）] を選択します。
- [保存（Save）] をクリックします。

（注） Cisco ISE リリース 2.6 以降では、IPv6 アドレスを使用するユーザが監査レポートにログインして次のイベントを使用します。ログイン/ログアウト、パスワードの変更、および運用変更など。管理者ログイン、ユーザの変更パスワードの監査、および運用監査レポートでは、IPv4 と IPv6 のレコード別にログをフィルタリングできるようになりました。

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| **Audit** | | |
| 適応型ネットワーク制御の監査 | 適応型ネットワーク制御の監査レポートは、RADIUS アカウンティングに基づきます。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）]** > **[システム（System）]** > **[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。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 管理者ログイン | 管理者ログイン レポートには、GUI ベースの管理者ログイン イベントと成功した CLI ログイン イベントに関する情報が提供されます。 | **[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。 |
| 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）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。 |

| 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。<br>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。<br>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。<br>高いディスク容量使用率がある場合、しきい値の 80% で「ISE モニタ ノードはもうすぐ割り当てられている最大量を超えます（ISE Monitor node(s) is about to exceed the maximum amount allocated）」という警告メッセージが表示されます。その後、しきい値の 90% で「ISE モニタ ノードは割り当てられている最大量を超えました（ISE Monitor node(s) has exceeded the maximum amount allocated）」という警告メッセージが表示されます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| エンドポイントのアクティビティ消去 | エンドポイントのアクティビティ消去レポートを使用すると、エンドポイントのアクティビティ消去の履歴を確認できます。このレポートは、プロファイラ ロギング カテゴリが有効である必要があります。デフォルトでは有効になっています。 | **[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、[プロファイラ（Profiler）] 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。 | — |
| 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）]**>**[システム（System）]**>**[ロギング（Logging）]**>**[ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| pxGrid 管理者の監査 | pxGrid 管理者の監査レポートは、プライマリ PAN でのクライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGrid の管理処理の詳細を提供します。<br>すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。<br>管理者およびメッセージの基準に基づいて、pxGrid 管理者の監査レポートをフィルタできます。 | — |
| セキュアな通信の監査 | セキュアな通信の監査レポートには、認証の失敗、ブレークインの可能性がある試み、SSH ログイン、失敗したパスワード、SSH ログアウト、無効なユーザ アカウントなどが含まれる、Cisco ISE 管理 CLI のセキュリティ関連イベントに関する監査の詳細が提供されます。 | — |
| 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（Administrative and Operational audit） |
| デバイス管理 | | |
| 認証概要（Authentication Summary） | [TACACS 認証概要（TACACS Authentication Summary）] レポートには、最も一般的な認証および認証失敗の理由の詳細が示されています。 | |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| TACACS アカウンティング | TACACS アカウンティング レポートは、デバイス セッションのアカウンティングの詳細を提供します。ユーザおよびデバイスの生成された時刻およびログに記録された時刻に関する情報が表示されます。 | **[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、[TACACSアカウンティング（TACACS Accounting）] を選択します。 |
| 失敗の理由別上位 N の認証（Top N Authentication by Failure Reason） | [失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。 | — |
| ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device） | [ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワーク デバイス名ごとの合格および不合格の認証数が表示されます。 | — |
| ユーザ別上位 N の認証（Top N Authentication by User） | [ユーザ別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザ名ごとの合格および不合格の認証数が表示されます。 | — |
| **診断** | | |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| AAA の診断 | AAA の診断レポートは、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に隔離されているか、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。<br>（注） ISE は、ユーザ認証が進行中のときにエンドポイントのアカウンティング停止要求をサイレントにドロップする場合があります。ただし、ISE はユーザ認証が完了すると、すべてのアカウンティング要求の認識を開始します。 | **[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、次のロギングカテゴリを選択します。[ポリシー診断（Policy Diagnostics）]、[IDストア診断（Identity Stores Diagnostics）]、[認証フロー診断（Authentication Flow Diagnostics）]、および[RADIUS診断（RADIUS Diagnostics）]。 |
| AD コネクタ操作 | ADコネクタ操作レポートは、Cisco ISE サーバのパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、ADコネクタが実行する操作のログを提供します。<br>ADの障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。 | **[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、[ADコネクタ（AD Connector）] を選択します。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| エンドポイント プロファイルの変更 | 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（Passed Authentications, Failed Attempts） |
| 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 時間のデータしか表示しませんが、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。<br><br>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。<br><br>[CPU 使用率（CPU Usage）] テーブルには、各種 Cisco ISE 機能の CPU 使用率（%）が表示されます。**show cpu usage** CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| ISE カウンタ | ISE カウンタ レポートには、さまざまな属性のしきい値が示されます。各種属性の値の収集間隔は異なり、またデータは表形式で表示されます。5 分間隔で収集される属性と 5 分よりも長い間隔で収集される属性があります。<br><br>このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。<br><br>Cisco ISE はデフォルトでこれらの属性の値を収集します。このデータ収集を無効にするには、Cisco ISE CLI で **application configure ise** コマンドを使用します。カウンタ属性の収集を有効または無効にするには、オプション 14 を選択します。 | — |
| 主要パフォーマンス測定指標 | 主要パフォーマンス測定指標レポートには、展開に接続しているエンドポイントの数と、1 時間あたりに各 PAN が処理する RADIUS 要求の数に関する統計情報が表示されます。このレポートには、サーバの平均負荷、要求あたりの平均遅延、および平均トランザクション数/秒が示されます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 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。<br>（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。 | — |
| 設定が誤っているサプリカント | 設定が誤っているサプリカントのレポートは、特定のサプリカントが実行した失敗試行のため、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。<br>（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。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 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。<br><br>Cisco ISE は SNMP クエリ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 デバイスは SNMP v1/v2c を使用して設定されている必要があります。<br><br>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。 | — |
| OCSP Monitoring | 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。適切な/失効したプライマリ/セカンダリ証明書に関連する情報を OCSP サーバから取得します。Cisco ISE は、応答をキャッシュし、後続の OCSP モニタリング レポートの生成に使用します。キャッシュがクリアされる場合は、OCSP サーバから情報を取得します。 | **[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、[システム診断（System Diagnostics）] を選択します。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| RADIUS エラー | RADIUS エラーレポートを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスからの廃棄された認証/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。<br>（注） 過去 5 日間のレポートのみを表示できます。 | **[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、[失敗した試行（Failed Attempts）] 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、このレポートを確認して問題をトラブルシューティングすることができます。<br>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）]** > **[システム（System）]** > **[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（Internal Operations Diagnostics）]、[分散管理（Distributed Management）]、および [管理者の認証と許可（Administrator Authentication and Authorization）]。 |
| **エンドポイントとユーザ** | | |

| 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。<br>（注） 認証概要レポートまたはダッシュボードが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。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 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。このレポートを使用すると、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ことができます。<br>（注） エンドポイントがISE に接続されない（セッションが確立されない）場合、またはネットワーク アドレス変換（NAT）アドレスがセッションで使用される場合、エンドポイントの MAC アドレスは [エンドポイントID（Endpoint ID）] 列に表示されません。 | **[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、[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（Audit and Posture and Client Provisioning Diagnostics）] を選択します。 |
| 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。<br>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。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 外部モバイル デバイス管理 | 外部モバイル 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。<br>このレポートを使用すると、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ことができます。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。 | **[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、[MDM] を選択します。 |
| パッシブ ID | パッシブ ID レポートでは、ドメイン コントローラへの WMI 接続の状態をモニタし、関連する統計情報（受信した通知の数、1 秒あたりのユーザ ログイン/ログアウト回数など）を収集することができます。<br>（注） この方法で認証されたセッションには、レポートの認証の詳細がありません。 | **[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、[IDマッピング（Identity Mapping）] を選択します。 |
| 手動証明書プロビジョニング | 手動証明書プロビジョニング レポートには、証明書プロビジョニング ポータル経由で手動でプロビジョニングされたすべての証明書がリストされます。 | — |
| 条件によるポスチャ アセスメント | 条件によるポスチャ アセスメント レポートでは、ISE に設定されたポスチャ ポリシー条件に基づいてレコードを表示し、最新のセキュリティ設定またはアプリケーションがクライアント マシンで利用可能かどうかを確認できます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| エンドポイントによるポスチャ アセスメント | [エンドポイントによるポスチャ アセスメント（Posture Assessment by Endpoint）] レポートには、エンドポイントの時間、ステータス、PRA アクションなどの詳細な情報が提供されます。[詳細（Details）] をクリックして、エンドポイントの詳細情報を表示することができます。<br>（注） [エンドポイントによるポスチャアセスメント（Posture Assessment by Endpoint）] レポートでは、エンドポイントのアプリケーションおよびハードウェア属性のポスチャ ポリシーの詳細は提供されません。[コンテキストの可視性（Context Visibility）] ページでのみこの情報を確認できます。 | — |
| 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。<br>（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）]** > **[システム（System）]** > **[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。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 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、このレポートを使用して識別できます。<br>（注） 暫定アップデートに、指定されたセッションの IPv4 または IPv6 アドレスの変更に関する情報が含まれている場合、Radius アカウンティング暫定アップデートは [RADIUS アカウンティング（RADIUS Accounting）] レポートに含まれています。 | **[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、[RADIUSアカウンティング（RADIUS Accounting）] 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、このレポートの詳細を確認して考えられる原因を識別できます。 | **[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、次のロギングカテゴリを選択します。[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）]。 |
| 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。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 拒否エンドポイント | 拒否エンドポイント レポートには、従業員が登録したパーソナル デバイスのうち、拒否されたデバイスまたはリリースされたデバイスがすべて表示されます。このレポートのデータは、Plus ライセンスをインストールしている場合にのみ使用可能です。 | — |
| 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（Posture and Client Provisioning Audit） |
| エンドポイントによる上位承認 | 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（Passed Authentications, Failed Attempts） |
| 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（Passed Authentications, Failed Attempts） |
| アクセス サービス別上位 N の認証（Top N Authentication by Access Service） | [アクセス サービス別上位 N の認証（Top N Authentication by Access Service）] レポートには、選択されたパラメータに基づいて、特定の期間におけるアクセス サービス タイプごとの合格および不合格の認証数が表示されます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 失敗の理由別上位 N の認証（Top N Authentication by Failure Reason） | [失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。 | — |
| ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device） | [ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワーク デバイス名ごとの合格および不合格の認証数が表示されます。 | — |
| ユーザ別上位 N の認証（Top N Authentication by User） | [ユーザ別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザ名ごとの合格および不合格の認証数が表示されます。 | — |
| **ゲスト** | | |
| AUP 受け入れステータス | AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの AUP 承認の詳細が示されます。 | **[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、[ゲスト（Guest）] 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がこのレポートに表示されます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
| --- | --- | --- |
| マスター ゲスト レポート | | **[管理（Administration）]**>**[システム（System）]**>**[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択して、[成功した認証（Passed Authentications）] を選択します。 |

| レポート名 | 説明 | ロギング カテゴリ |
| --- | --- | --- |
| | マスター ゲスト レポートは、さまざまなゲスト アクセス レポートからデータを結合し、異なるレポート ソースからデータをエクスポートできるようにします。マスター ゲスト 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も提供します。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。<br><br>また、ゲスト トラフィックに使用するネットワーク アクセス デバイス（NAD）の HTTP インスペクションを有効にする必要もあります。この情報は、NAD によって Cisco ISE に返送されます。<br><br>クライアントが最大同時セッションの制限数に到達した時期を確認するには、管理者ポータルから、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）] の順に選択し、次を実行します。<br><br>**1.** 「認証フロー診断」のロギング カテゴリのログ レベルを [警告（WARN）] から [情報（INFO）] に上げます。<br><br>**2.** AAA 診断の [ロギングカテゴリ（Logging Category）] の下で [LogCollectorターゲット | |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| | （LogCollector Target）] を [使用可能（Available）] から [選択済み（Selected）] に変更します。 | |
| デバイスのログインおよび監査 | デバイスのログインおよび監査レポートは、デバイス ポータルのデバイスでユーザが実行するログイン アクティビティと操作についての詳細を提供します。 | **[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、[デバイス（My Devices）] を選択します。 |
| スポンサーのログインおよび監査 | スポンサーのログインおよび監査レポートは、スポンサー ポータルでのゲスト ユーザのログイン、追加、削除、有効化、一時停止、および更新操作の詳細、ならびにスポンサーのログイン アクティビティの詳細を提供します。<br>ゲスト ユーザを一括で追加すると、[ゲスト ユーザ（Guest Users）] カラムの下に表示されます。このカラムは、デフォルトでは非表示です。エクスポート時に、これらの一括処理されたユーザもエクスポート ファイルに存在します。 | **[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、[ゲスト（Guest）] を選択します。 |
| **SXP** | | |
| SXP バインディング | SXP バインディング レポートは、SXP 接続を介して交換される IP-SGT バインディングに関する情報を提供します。 | — |
| SXP 接続 | このレポートを使用して、SXP 接続のステータスをモニタしたり、ピア IP、SXP ノード IP、VPN 名、SXP モードなど、その接続に関連する情報を収集できます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| **TrustSec** | | |
| RBACL ドロップ概要 | RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。<br>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。<br>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。<br>（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズスイッチでのみ使用できます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| 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 ライセンスのみで使用できる TrustSec 機能に固有です。<br>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。<br>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。<br>（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。 | — |
| TrustSec ACI | このレポートには、IEPG、EEPG、エンドポイント、APIC のサブネット設定と同期された SGT および SXP のマッピングが一覧表示されます。これらの詳細は、TrustSec APIC 統合機能が有効になっている場合にのみ表示されます。 | — |

| レポート名 | 説明 | ロギング カテゴリ |
| --- | --- | --- |
| TrustSec 展開の検証 | | — |

| レポート名 | 説明 | ロギング カテゴリ |
| --- | --- | --- |
| | このレポートを使用すると、最新の TrustSec ポリシーがすべてのネットワーク デバイスで展開されているかどうか、Cisco ISE とネットワーク デバイスで設定されたポリシーに不一致があるかどうかを確認できます。<br><br>検証プロセスの結果を表示するには、[詳細（Details）] アイコンをクリックします。次の詳細情報を表示できます。<br>• 検証プロセスの開始時期と終了時期<br>• 最新の TrustSec ポリシーがネットワーク デバイスで正常に展開されているかどうか。また、最新の TrustSec ポリシーを展開するネットワーク デバイスの名前および IP アドレスを表示することもできます。<br>• Cisco ISE とネットワーク デバイスで設定されたポリシーに不一致があるかどうか。デバイス名、IP アドレス、および各ポリシーの違いの対応するエラー メッセージが表示されます。<br><br>[アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] と [ホーム（Home）] > [サマリー（Summary）]）で、TrustSec 展開の検証アラームを表示できます。 | |

| レポート名 | 説明 | ロギング カテゴリ |
| --- | --- | --- |
| | （注）<br>• レポート作成にかかる時間は、展開内のネットワーク デバイスと TrustSec グループの数に応じて異なります。<br>• TrustSec 展開の検証レポートのエラー メッセージの長さは、現在 480 文字に制限されています。480 文字を超えるエラー メッセージは切り捨てられます。最初から 480 文字のみがレポートに表示されます。 | |
| TrustSec ポリシーのダウンロード | このレポートには、ポリシー（SGT/SGACL）のダウンロードのためにネットワーク デバイスによって送信された要求と、ISE によって送信された詳細が一覧表示されます。ワークフロー モードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。 | このレポートを表示するには、次の手順を実行する必要があります。<br>1. **[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。<br>2. **[AAA診断（AAA Diagnostics）]** > **[RADIUS診断（RADIUS Diagnostics）]** を選択します。<br>3. RADIUS 診断の [ログ重大度レベル（Log Severity Level）] を DEBUG に設定します。 |

| レポート名 | 説明 | ロギング カテゴリ |
|---|---|---|
| **脅威中心型 NAC サービス** | | |
| アダプタのステータス | アダプタのステータス レポートには、脅威および脆弱性のアダプタのステータスが表示されます。 | — |
| COA イベント | 脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。 | — |
| 脅威イベント | 脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。 | — |
| 脆弱性アセスメント | 脆弱性アセスメント レポートには、エンドポイントで行われているアセスメントに関する情報が提供されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。 | — |