Smart Net Total Care ポータル ユーザ ガイド

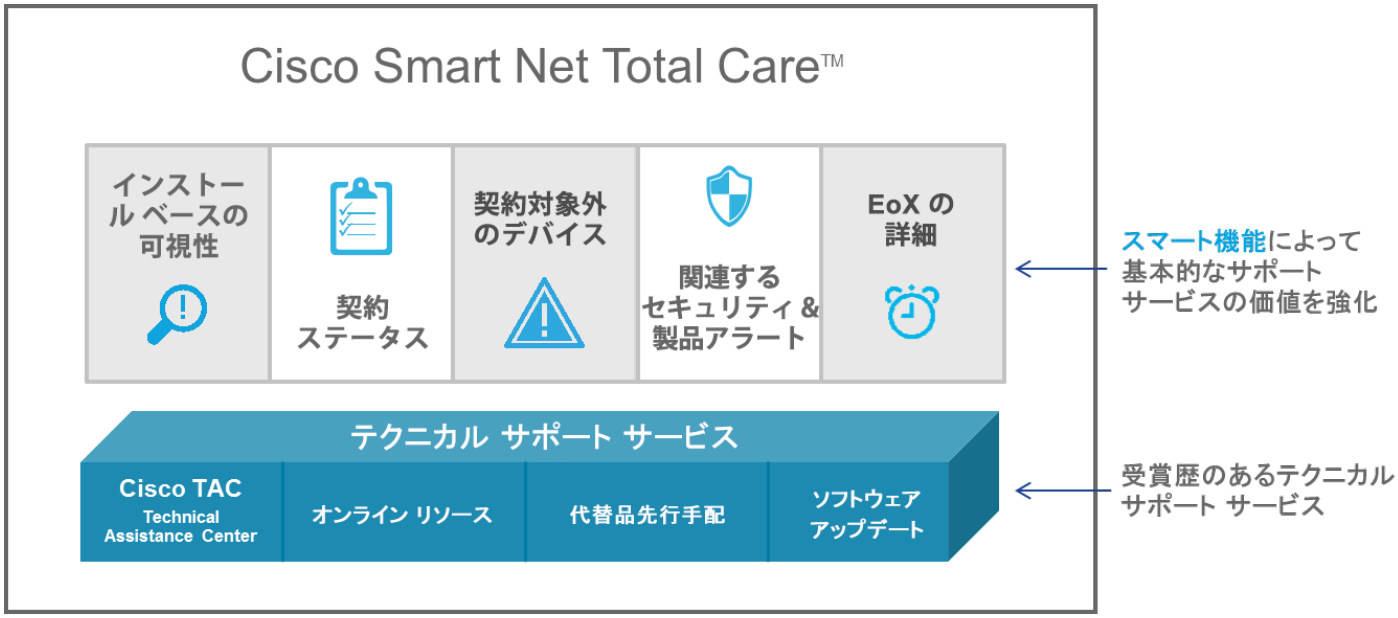
初版:2015 年 8 月 1 日
最終更新日:2016 年 6 月 6 日

目次

はじめに

Cisco Smart Net Total Care™ は、シスコのスマート サービス ポートフォリオの一部です。業界をリードする、受賞歴のある基本的なテクニカル サービスと、Software as a Service(Saas)モデルで提供される、実用性の高いビジネス インテリジェンスを組み合わせたサービスです。Smart Net Total Care の Web ベースのポータルとレポートにより、シスコ製品のインベントリを管理する際に必要となるすべての情報が提供されます。この統合型スマート機能では、インストール ベース、契約、セキュリティのアラートに関する最新情報が提供されるため、サポート ワークフローの効率が向上します。Smart Net Total Care の特長は次のとおりです。

- **迅速な問題解決**:問題を迅速に特定し、インシデント管理プロセスを効率化することで、問題をすばやく解決でき、IT のサービス レベルを向上できます。スマート機能(プロアクティブなアラート、自動診断、および契約対象と製品に関する最新情報など)により、ダウンタイムを最小限に抑え、ビジネスの継続性を確保します。
- **リスクの軽減**:シスコのテクニカル エキスパート(Cisco Technical Assistance Center)や、IT インフラストラクチャの状態を可視化するスマート ツールを 24 時間 365 日いつでも利用できます。Smart Net Total Care ポータルでインストール ベースを確認できるため、重要なシスコ製品が適切なサービス契約の対象であるかどうかを確認できます。また、ポータルでは製品販売の終了(EoS)または製品サポートの終了(EoL)が近づいているシスコ製品について、更新の計画と予算策定を前もって実施することが容易になります。
- **業務の効率化**:プロアクティブな管理ツールと、ネットワーク運用者や管理者の生産性を高める自動化プロセスによって、業務効率を向上できます。自動インベントリおよび契約管理では、変更点が強調表示されるため、ネットワークのビューを最新に維持する労力を最小限に留めることができ、予算と計画の予測に役立ちます。



対象読者

このドキュメントは、Smart Net Total Care(以下「ポータル」)を使用するユーザを対象としています。

このドキュメントの指示内容は、ネットワークから取得したデバイス データが(サポートされている方法の 1 つで)Smart Net Total Care システムに 1 回以上アップロードされていることを前提としています。

ポータルの [便利なリンク(Userful Links)] ページからこのユーザ ガイドにアクセスできます。

参考資料

Smart Net Total Care の詳細については、サポート コミュニティにアクセスするか、またはビデオ リポジトリを閲覧してください。

Smart Net Total Care のシスコ サポート コミュニティ

https://supportforums.cisco.com/community/4891/smart-net-total-care.

このコミュニティでは、ソフトウェア バージョン 3.x のスマート機能（ポータル、レポート、コレクションなど）に関するヘルプ、リソース、サポートを参照できます。

ハウツー ビデオ リポジトリ

http://www.cisco.com/E-Learning/bulk/subscribed/SNTC_vods_EN/index.html

ビデオを観るには、次の手順に従います。

1. リポジトリに移動します。
2. [<***希望する言語***>（<Preferred Language>）] > [インストール ベースのレポート（Installed Base Reporting）] を選択します。
3. 表示するビデオを選択します。

このリポジトリで利用できるビデオ チュートリアルを観ることで、このガイドで説明する概念やプロセスの一部に関する知識を深めることができます。

このユーザ ガイドでは、当該トピックに直接関連するビデオへのリンクを「**ハウツー ビデオ**」に記載しています。

ロールとアクセス

Delegated Administrator（DA）

Delegated Administrator は上級管理者であり、契約先企業には 1 名以上の DA が必要です。Delegated Administrator は、組織で追加されるユーザと管理者の登録とアクセス権限の管理を担当します。DA は、組織の従業員である必要があります。

DA は、Cisco Access Management Tool を使用して Smart Net Total Care の管理者とユーザの登録、アクセス権限の付与と取り消しを実行できます。.DA は同じツールを使用して、各種 Smart Net Total Care ロールの既存の権限を変更することもできます。Smart Net Total Care ユーザ ロールを作成および登録できるのは DA だけです。

Cisco Access Management Tool を使用したユーザの追加と削除については、このビデオを参照してください。

ハウツー ビデオ

- ユーザと会社の関連付け

Smart Net Total Care のユーザ ロール

ポータルのユーザ ロールは、個々のユーザに付与されるロールです。各ロールはシステムに標準装備されており、ユーザがポータルで表示および実行できる内容を決定する特定の権限と制限が含まれています。組織に応じて、1 名以上の従業員に次のロールを 1 つ以上割り当てることができます。

- 顧客管理者
- 顧客ユーザ

- シスコ ブランドのリセラー(CBR)ユーザ
- シスコ ブランドのリセラー(CBR)管理者

注 1:CBR 管理者と CBR ユーザは、顧客の契約先企業の Delegated Administrator になることはできません。

注 2:複数のロールが割り当てられているユーザに対しては、アクセスできるすべてのデータが表示されます。

顧客管理者

顧客管理者は、契約先企業の従業員である必要があります。顧客管理者は次の操作を実行できます。

- レポートを表示する。
- 企業に登録されているその他のユーザ、管理者、CBR 管理者、および CBR ユーザのポータルの権限を作成、保守する。
- コレクタを登録する。
- ファイルのインポートを実行する。
- アラートを管理する。
- サービス適用範囲を管理する。
- セグメント作成のためのユーザのアクセス権限を付与または制限する。
- Cisco Branded 再販業者へ認可証を提供する。
- IPv6 などのプロトコルについてネットワーク アーキテクチャを評価する。

顧客ユーザ

顧客ユーザは、契約対象企業の従業員である必要があります。顧客管理者からアクセス権限を付与された顧客ユーザは、次の操作を実行できます。

- 各自に関連付けられている企業のレポートを表示する。
- アクセス権限を持つ特定のセグメントとインベントリにアクセスする。
- インストール ベース、アラート、デバイス構成、アラート管理、およびサービス適用範囲に関連する情報にアクセスする。

シスコ ブランドのリセラー(CBR)管理者

顧客管理者は、企業に関連付けられている CBR 管理者に、顧客管理者の代理として特定の管理タスクを実行するためのアクセス権と権限を付与できます。適切な権限を付与されている CBR 管理者は、次の操作を実行できます。

- コレクタを登録する。
- ファイルのインポートを実行する。
- アラートを管理する。
- サービス適用範囲を管理する。
- ユーザ アクセスを管理する。
- 認可書(LOA)がある場合は、その他のパートナーによって再販された契約に関する一部の情報にアクセスする。

シスコ ブランドのリセラー（CBR）ユーザ

CBR ユーザは、契約先企業の顧客管理者からアクセス権が付与されている場合には次の操作を実行できます。

- 契約先企業のレポートを表示する。
- 認可証がある場合は、その他のパートナーによって再販された契約に関する一部の情報にアクセスする。

ハウツー ビデオ

- ロールとアクセス

導入までのステップ

Smart Net Total Care ポータルでは、デバイス情報を、シスコのナレッジ ベースのセキュリティおよびサポート データと照合して解析します。その結果得られる実用的な情報により、問題解決にかかる時間が短縮され、業務効率が向上し、サポート リスクの管理が強化されます。

セルフサービス オンボーディング：Smart Net Total Care ポータルへのアクセス

Cisco SMART 契約対象ユーザ（顧客とパートナー）は、SNTC 3.x ポータルにアクセスするためにセルフサービスで自身を登録できます。

セルフサービス オンボーディング プロセスでは、提供されている契約とシリアル番号を確認することで、ユーザのデータ アクセス権限を確認します。

組織内で最初にセルフサービス オンボーディング プロセスを実施するユーザが Delegated Administrator になります。オンボーディング プロセスでは、DA を選任するためのガイドラインが提供されます。できれば、組織内のユーザ アクセスとアカウントをすでに管理しているユーザを DA として指名してください。ネットワーク管理者はこのロールに適しています。

組織ですでに DA が選任されている場合、DA に対して新規ユーザ セルフサービス リクエストが通知されます。これにより、DA は Smart Net Total Care ポータルへの新規ユーザのアクセスを承認できます。

注：新規登録情報がアクティブになるまでに最大 24 時間かかります。

セルフサービス オンボーディングの前提条件

- 有効なシスコ アカウント プロファイルを所有している必要があります。
- 1 つ以上のスマート サービス対象契約がプロファイルに関連付けられている必要があります。スマート サービス対象契約の例として、SMARTnet（現行名称：Smart Net Total Care）、SP Base、TelePresence、Essential Operate、Solution Support などがあります。
- プロファイルに有効な業務用電子メール アドレスが指定されている必要があります。@yahoo、@gmail、@hotmail などの個人的な電子メール ドメインは受け入れられません。

セルフサービス オンボーディング プロセス

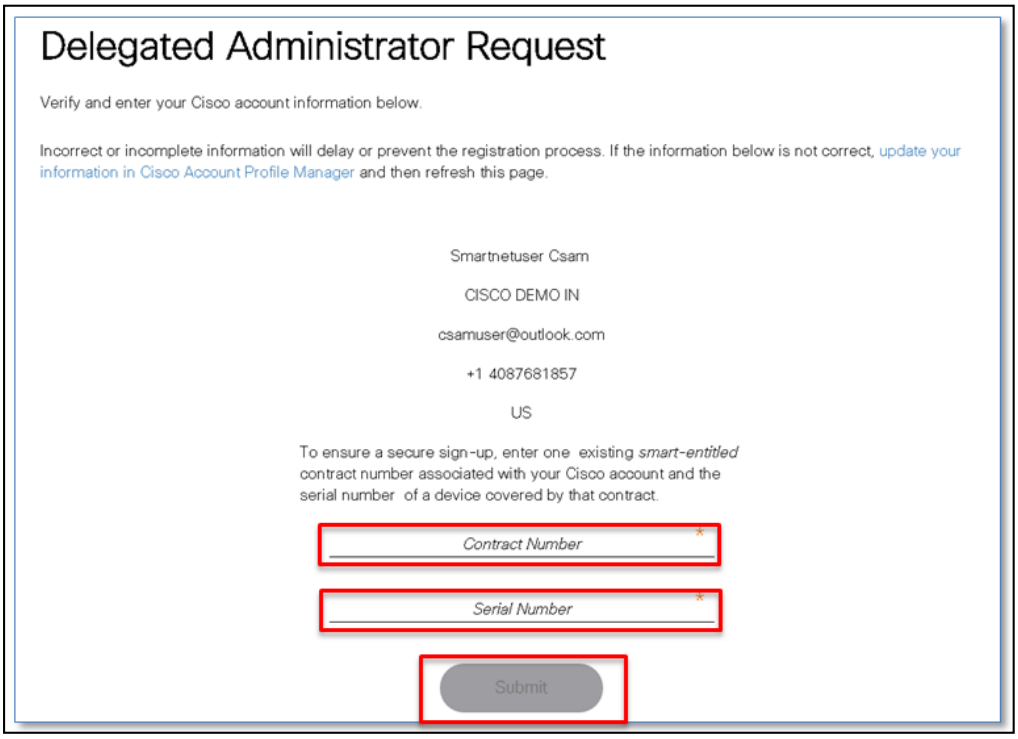
セルフサービス オンボーディングを完了するには、次のタスクを実行します。

1. [Smart Net Total Care] > [登録(Registration)] を開きます。

2. [プロアクティブ対応(Go Proactive)] で [登録(Register)] をクリックします。[シスコ ログイン(Cisco Login)] ページが開きます。
3. 有効なシスコ ユーザ ID とパスワードを使用してログインします。[セルフサービス登録概要(Self-Service Registration Overview)] ページが開きます。このページには、登録手順と、Delegated Administrator の役割と責任が表示されます。
4. [ユーザ自身を Delegated Administrator として設定する(Become a Delegated Administrator)] をクリックします。[Delegated Administrator リクエストフォーム(Delegated Administrator Request Form)] が開きます。

   注:ユーザ自身を Delegated Administrator にしない場合は、登録プロセスを中止し、組織内で Delegated Administrator として適切なユーザを決定してください。 ユーザ自身を Delegated Administrator として設定することを要求したが、組織内ですでに別の Delegated Administrator がいる場合、承認のために要求がその Delegated Administrator に転送されます。
5. [Delegated Administrator リクエスト フォーム(Delegated Administrator Request Form)] で次の操作を実行します。
   a. スマート サービス対象契約番号を入力します。
   b. 契約対象となるデバイスのシリアル番号を入力します。
   c. [送信(Submit)] をクリックします。デバイスのシリアル番号または契約番号が無効な場合は、このボタンはアクティブになりません。

      フォームの送信後に、指定した電子メール ID に確認のための電子メールが送信されます。



6. 電子メールの確認のためのリンクをクリックします。「要求が送信されました（Your Request is submitted）」と通知されます。確認のための電子メールが受信トレイにない場合は、迷惑メールのフォルダを調べます。

要求が正常に送信されると、要求の検証と処理に最大で 24 時間かかります。処理が完了すると、次の電子メールを受信します。

- *Delegated Administrator の契約条件に同意する（Accept Delegated Administrator Terms & Conditions）*：この最初の電子メールには、Cisco Services Access Management ツールへのリンクが含まれています。このツールを使用して、所属組織の Delegated Administrator になるための契約条件を読んで同意することができます。ツールにログインし、[法的契約を参照する（Review Legal Agreement）] をクリックします。
- Smart Net Total Care ポータルへのアクセス（Access to Smart Net Total Care Portal）：この 2 番目の電子メールには Smart Net Total Care ポータルへのリンクが記載されています。このメールでは、ユーザのアクセス権限とロールが確認されます。ポータルでは、デフォルトで Delegated Administrator には顧客管理者ロールが割り当てられています。顧客管理者ロールでは、ポータル内でファイルのアップロードやその他の管理アクティビティを実行できます。

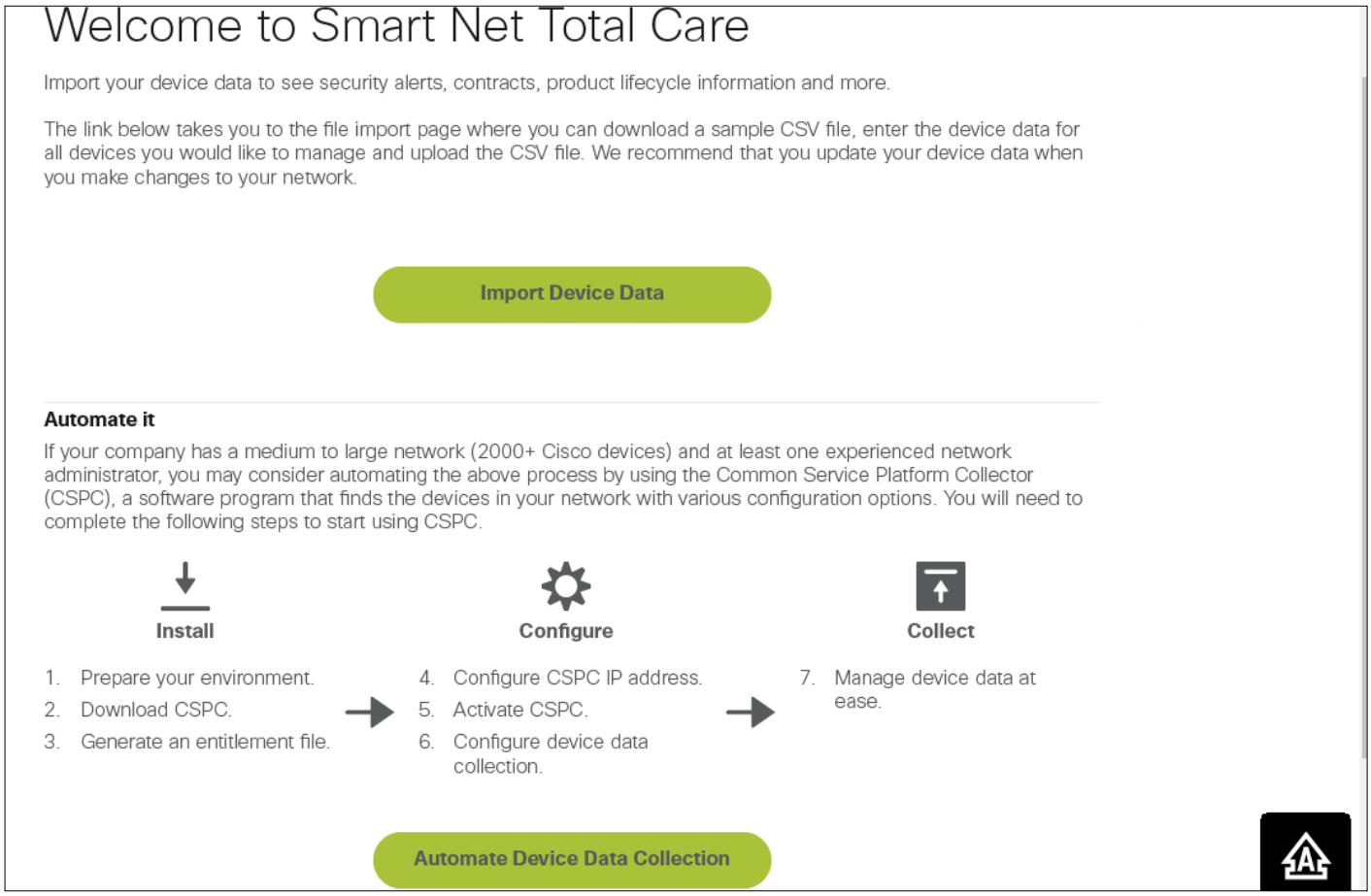
  CCO ユーザ ID とパスワードを使用してポータルにログインできます。

最初のインベントリの作成

インベントリとは、サポートされているいずれかの方法で Smart Net Total Care システムにアップロードされたデバイスの集合です。シスコ製品のインストール ベースの情報を Smart Net Total Care ポータルに取り込むときに使用できる方法は、次のとおりです。

- Cisco Common Service Platform Collector（CSP-C）を使用する。
- サードパーティのコレクタを使用する。
- CSV ファイル インポートを実行する。

インベントリがまだ作成されていない場合に、新しいセルフサービス顧客管理者としてログインすると［はじめに（Get Started）］ページが表示されます。このページには、CSV ファイル インポートまたはコレクタによる自動デバイス収集によってインベントリをインポートするための手順が表示されます。



新規ユーザとしてログインしたときに［レコードが見つかりませんでした（No records found）］が表示される場合は、顧客管理者に連絡し、最初のインベントリを作成するよう依頼してください。

ポータルでユーザに複数の顧客のアカウントが関連付けられており（マルチロール ユーザ）、ログイン時にレポートに［レコードが見つかりませんでした（No records found）］と表示される場合、組織のデバイス データが適切にアップロードされていません。当該顧客の顧客管理者に連絡し、インベントリのアップロードを依頼してください。

注：インベントリのアップロード時にデバイスの IP アドレスを受信しなかった場合、レポートの［IPアドレス（IP Address）］フィールドは［--］になります。

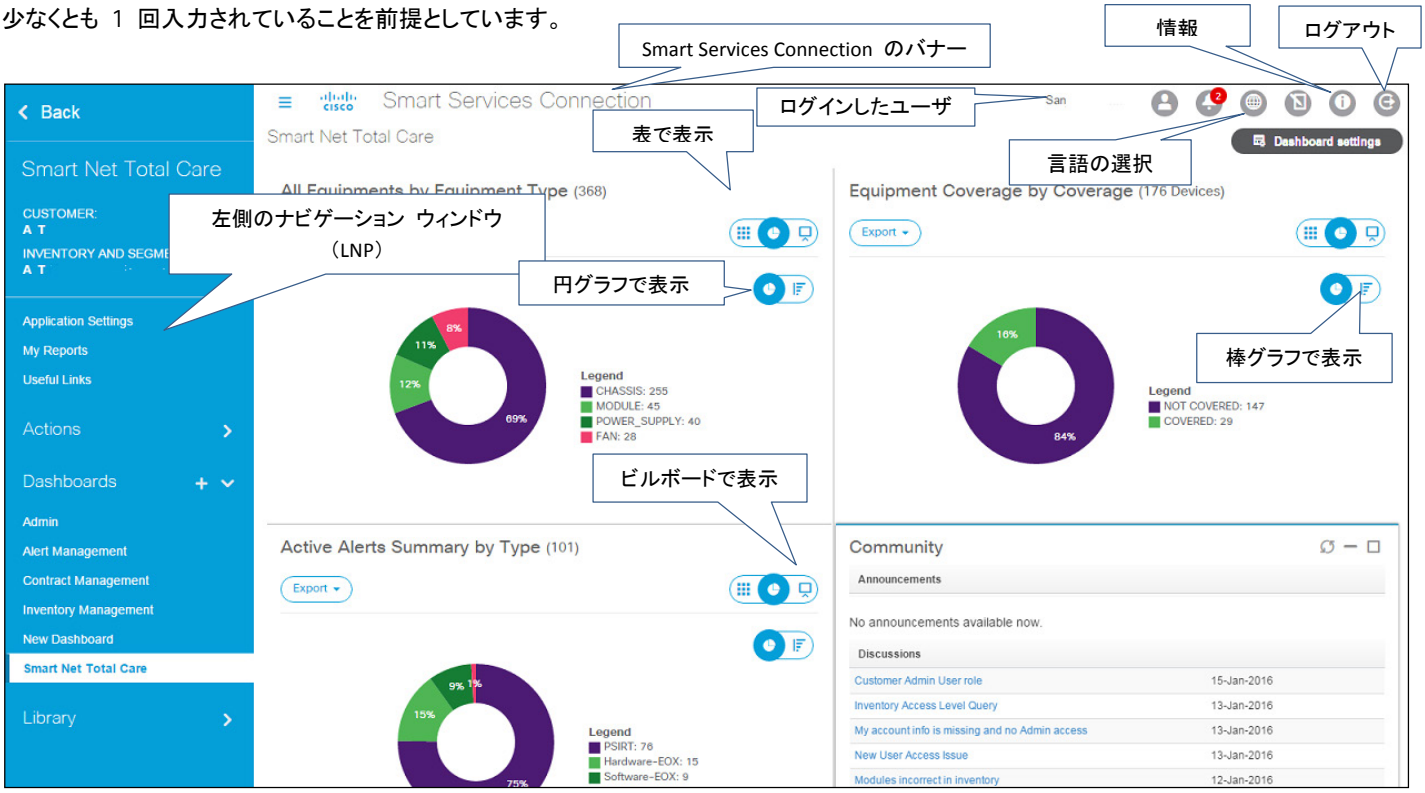
ハウツー ビデオ

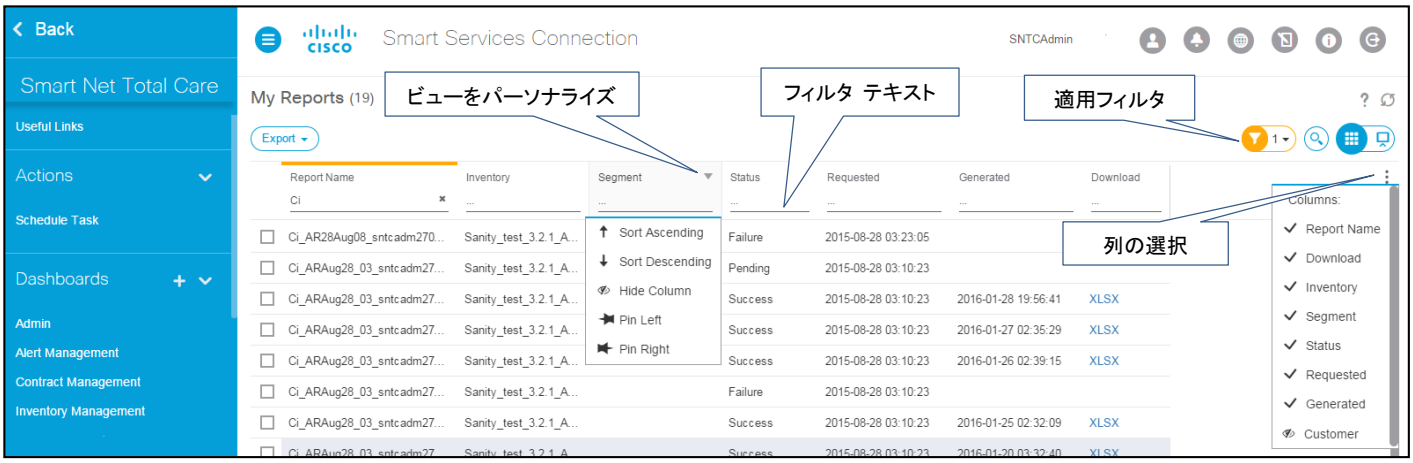
- 最初のインベントリの作成

基本的なポータル ナビゲーション

Smart Net Total Care は、直感的で使いやすいレポートを生成する Smart Services Connection プラットフォームを採用しています。これらのレポートは、フィルタ処理、さまざまな形式での表示、およびデータ表示方法のカスタマイズが可能です。

次のスクリーンショットでは、アクセスしたときの Smart Net Total Care ポータルを示しています。ここでは、組織のデバイス データが少なくとも 1 回入力されていることを前提としています。





ポータルのコンポーネント

上記の画像を参照して、ポータルの主要コンポーネントを確認してください。

- **左側のナビゲーション ウィンドウ(LNP)**:ページのこの部分には、レポート、ダッシュボード、および設定へのリンクが表示されます。
- **ログインしたユーザ**:現在ログインしているユーザの名前が表示されます。
- **言語の選択**:ローカライズされたレポートとポータルを使用する場合はこのアイコンをクリックします。現在、ポータル画面はフランス語、スペイン語、フランス語(カナダ)、簡体字中国語にローカライズされています。

注:一部のレポートまたはレポートのヘルプは、選択された言語で表示できないことがあります。

- **情報**:ハウツー ビデオを閲覧する場合、このガイドのコピーをダウンロードする場合、および Smart Net Total Care の詳細情報を参照する場合は、このアイコンをクリックします。
- **表で表示**:レポートまたはダッシュレットの内容を表形式で表示するには、このアイコンをクリックします。
- **棒グラフで表示**:レポートまたはダッシュレットの内容を棒グラフで表示するには、このアイコンをクリックします。
- **円グラフで表示**:レポートまたはダッシュレットの内容を円グラフで表示するには、このアイコンをクリックします。
- **ビルボードで表示**:最も重要なデータをビルボードとして迅速に表示するには、このアイコンをクリックします。元のビューに戻すには、ビルボードをクリックします。
- **ログアウト**:ポータルからサインアウトするには、このアイコンをクリックします。
- **ビューをパーソナライズ**:列のデータを設定/ソートするには、その列名の横にある小さな三角形をクリックします。

  注:列を別の位置にドラッグ アンド ドロップするか、[左側に固定(Pin Left)] または [右側に固定(Pin Right)] を選択して列を左端/右端に移動することができます。
- **フィルタ テキスト**:このテキスト ボックスに値を入力し、Enter キーを押します。列のデータにフィルタが適用され、指定した条件に一致する結果が表示されます。1 つ以上の列にフィルタ値を追加できます。
- **適用フィルタ**:レポートの列に適用されているフィルタがある場合は、このアイコンをクリックするとフィルタが表示されます。
- **列の選択**:レポートに使用できる列のリスト全体を表示するには、このアイコンをクリックします。レポートで表示または非表示にする列名をクリックします。

注:リリース 3.4 以降では、レポート設定が自動的にプロファイルに保持されます。選択した列、列の配置順序、列のサイズなどの変更内容は、さらに変更するまでセッション間で維持されます。ただし、フィルタとソート順序の維持は特定のセッションに限られます。

ハウツー ビデオ

ナビゲーションとダッシュボード

設定とカスタマイズ

左側のナビゲーション ウィンドウ(LNP)の上部にある Smart Net Total Care セレクタ パネルを使用して、レポートに表示されるデータをカスタマイズまたは選択します。顧客、インベントリ、セグメントに基づいてデータをカスタマイズまたは選択できます。

LNP 上部には、使用中の Cisco Smart Service の名前が表示されます。この場合は Smart Net Total Care です。

顧客

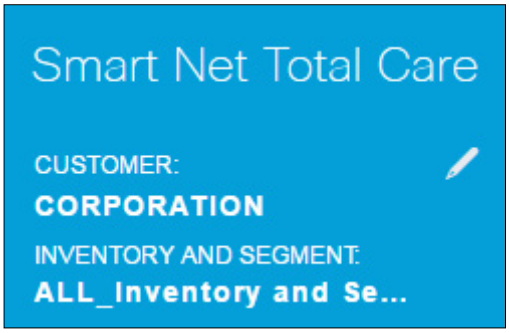
サービス名のすぐ下に、顧客名とインベントリおよびセグメントが表示されていることがわかります。これは、契約先顧客の名前です。レポートにはこの契約先顧客のデバイス データが表示されます。

ほとんどの顧客については、[顧客(Customer)] タブに表示される選択項目は、顧客の組織名だけです。複数の業務組織で構成される顧客については、アクセス権限のある組織ごとに複数の選択項目が表示されます。顧客のデータを表示できる権限があるパートナーまたはマルチロール ユーザについても、複数の顧客が表示されることがあります。

インベントリとセグメント

選択した顧客(契約先企業)に対して使用可能なインベントリとセグメントは、[インベントリおよびセグメント(Inventory and Segment)]の下に表示されます。表示される内容は、各自に割り当てられているユーザ アクセス設定によって異なります。

インベントリとは、1 つのコレクション ソースからアップロードされるデバイス データです。インベントリはセグメントに分割できます。



カスタマイズ手順

1. 鉛筆アイコンをクリックします。[データ フィルタ(Data Filters)] ウィンドウが開きます。
2. [顧客(Customer)] をクリックします。顧客名を選択します。レポートには選択した顧客のデータだけが表示されます。
3. [インベントリとセグメント(Inventory and Segment)] をクリックします。
4. 必要なインベントリとセグメントを選択します。レポートには、選択したインベントリとセグメントのデータだけが表示されます。

   注:複数のインベントリまたはセグメントを選択すると、レポートには選択したすべてのインベントリまたはセグメントのデータが表示されます。

アプリケーションの設定

全般

このタブには、アクセスできるビジネス サービスと顧客のリストと、顧客ごとの各自のロールが表示されます。

[会社通知(Company Notifications)]

管理者ロールが割り当てられている場合、このタブでは、ユーザに送信するメッセージの配信リストを管理します。

マイ通知

このタブでは、ポータルからアラートとシステム メッセージを受信する頻度を管理します。

[レポート設定(Report Preferences)]

このタブでは、レポートに表示するデータのタイプを選択できます。

- [最新のビュー(Latest View)]:サポートされているコレクタまたは CSV ファイルからアップロードされた最新のデータだけが含まれるレポートを表示するには、このビューを選択します。これは、新規ユーザのデフォルト ビューです。

- [包括的なビュー(Comprehensive View)]:すべてのコレクションからのすべてのデータが含まれるレポートを表示するには、このビューを選択します。

選択したオプション/設定は、LNP(オンライン ダッシュボード、オフライン/スケジュール済みレポート、オンライン スマート レポート、およびウィジェット)で表示可能なすべてのデータに反映されます。

注:スケジュールされたレポートには、レポートの生成時点での設定が反映されます。

ハウツー ビデオ

- 柔軟なインベントリ レポート

マイ レポート

[マイ レポート(My Reports)] ページには、次の内容が表示されます。

- ユーザが [エクスポート(Export)] 機能を使用して生成したすべてのレポート。レポート名は、LNP にリストされている名前と同じです。これらのレポートを生成するには、レポートで [エクスポート(Export)] をクリックします。
- [スケジュール済みタスク(Scheduled Task)] 機能を使用してシステムにより生成されたスケジュール済みレポート。デフォルトでは、これらのレポート名にはユーザ名と固有の数値 ID が含まれます。レポートをスケジュールするときにレポート名を変更できます。

保存されているレポートの形式は、レポートの生成時に指定された PDF、XLSX、または CSV です。通常、レポートは生成時点から 72 時間保持されます。

ローカル デバイスにレポートをダウンロードするには、[ダウンロード(Download)] 列でフォーマット リンク(XLSX、PDF など)をクリックします。

注:処理するデータ量に応じて、レポートがダウンロード可能になるまで数分～数時間かかります。

参考リンク

このページには、次の内容に関するリソースへのリンクが表示されます。

- トレーニング
- サポート
- Smart Net Total Care コミュニティへのアクセス
- 契約の管理
- Smart Net Total Care のトラブルシューティング
- アカウント管理
- 返品許可(RMA)手続きの開始
- ユーザ ガイドおよび関連ソフトウェアのダウンロード

アクション

タスクのスケジュール

提供されるワークフローを使用して、指定された時刻または継続ベースで、選択されたレポートの自動生成をスケジュールできます。生成されたレポートは［マイレポート(My Reports)］の下で利用可能になります。デフォルトでは、これらのレポート名にはユーザ名と固有の数値 ID が含まれます。レポートをスケジュールするときにレポート名を変更できます。

ダッシュボード

Smart Net Total Care のダッシュボードには、最も重要なデータの統合ビューが表示されます。ダッシュボードでは、選択された顧客のインストール ベース内の契約、インベントリ、デバイス、およびアラートのステータスの概要が表示されます。

ポータルには次のダッシュボードがあります。

- [管理(Admin)]
- [アラート管理(Alert Management)]
- [契約管理(Contract Management)]
- [インベントリ管理(Inventory Management)]
- [Smart Net Total Care]

ユーザにとって最も関連性が高いレポートとアラートを表示するには、パーソナライズしたダッシュボードを作成してポータルに保存することができます。これらのダッシュボードは、後続のセッションで維持されます。 詳細については、「カスタム ダッシュボードの作成」を参照してください。

[管理(Admin)]

[管理(Admin)] ダッシュボードは、管理者がユーザとデバイス データ収集を管理するために使用します。

ポータルでユーザに対して表示されるデータとレポートは、ユーザのロールによって決まります。管理者は、「ロールベース アクセス コントロール」を適用して、ユーザが把握しておく必要がある情報に基づいてユーザのアクセスを制限できます。たとえば、あるユーザ グループには特定のネットワーク セグメントのデータへのアクセス権限を付与し、別のユーザ グループには特定のレポートのみへのアクセス権限を付与することができます。

[管理(Admin)] ダッシュボードには 4 つのダッシュレットがあります。

[アカウント情報と契約ステータス(Account Information and Contract Status)]

[アカウント情報と契約ステータス(Account Information and Contract Status)] ダッシュレットには、アカウントの契約情報と、特定のインストールでアクティブなサポート契約が表示されます。

[セグメント管理(Segment Management)]

注:このダッシュレットは管理者だけが使用できます。

[セグメント管理(Segment Management)] ダッシュレットには、インベントリ内のセグメントと関連情報が表示されます。セグメントは、ホスト名、IP アドレス、または SysName に基づいて、ポータルに表示するデータを分割するために使用します。管理者がこのセグメント化を行い、その後、各セグメントへのアクセス権限をユーザに付与します。管理者による定義の内容に基づき、ユーザはすべてのセグメントにアクセスできる場合とアクセスできない場合があります。

このダッシュレットでは次の操作を実行できます。

- 複数の条件（ブール条件を含む）に基づいてデータ セグメントを作成する。
- 作成されたセグメントに含まれるデバイスのリストを表示する。
- セグメントのデータへのアクセス権をユーザに付与する。
- 既存のセグメントを表示、変更、コピー、または削除する。

新しいセグメントを作成するには、次の手順に従います。

1. [アクション（Actions）] > [新規セグメントの作成（Create a New Segment）] をクリックします。[新規セグメントの作成（Create a New Segment）] ウィンドウが開きます。
2. [名前（Name）] フィールドに、一意のセグメント名を入力します。この名前には特殊文字やスペースは使用できませんが、数字は使用できます。
3. 条件値（ホスト名、IP アドレスなど）を選択します。
4. ブール演算子（[次を含む（contains）]、[次で始まる（begins with）] など）を選択します。
5. 一致条件を入力します。ワイルドカードを使用できます。
6. プラス記号（+）アイコンをクリックします
7. 必要に応じて手順 1 ～ 6 を繰り返して、別の条件を設定します。
8. 必要に応じてデバイス リストを確認し、ユーザにアクセス権を付与します。セグメントの作成後にこの操作を実行する場合の手順については、以降の項で説明します。
9. [作成（Create）] をクリックします。新しいセグメントが作成されます。

セグメント内のデバイスのリストを表示するには、次の手順に従います。

1. 既存のセグメント名を右クリックし、[表示/変更（View/Modify）] を選択します。
2. [デバイスリストを表示（See Device List）] をクリックします。

セグメント内のデータへのアクセス権をユーザに付与するには、次の手順に従います。

1. 既存のセグメント名を右クリックし、[表示/変更（View/Modify）] を選択します。
2. [ユーザの選択（Select User）] をクリックします。すべてのユーザを選択するか、またはユーザを個別に選択できます。
3. 選択したユーザにアクセス権を付与するため、[追加（Add）] をクリックします。ユーザとその他の顧客管理者は、セグメントへのアクセス権が付与または取り消されると、電子メールによる通知を受信します。
4. [適用（Apply）] をクリックして変更内容を保存します。

既存のセグメントを表示または変更するには、次の手順に従います。

1. 既存のセグメント名を右クリックし、[表示/変更（View/Modify）] を選択します。
2. 必要に応じて既存の設定を変更します。
3. [適用（Apply）] をクリックして変更内容を保存します。

既存のセグメントのコピーを作成するには、次の手順に従います。

1. 既存のセグメントを右クリックし、[新規セグメントへコピー(Copy to a New Segment)] を選択します。
2. このセグメント用の新しい一意の名前を入力します。
3. 必要に応じて既存の設定を変更します。
4. [作成(Create)] をクリックします。

CBR 管理者によって作成されたセグメントは、[セグメント管理(Segment Management)] ダッシュレットで顧客管理者に対してだけ表示されます。顧客管理者はこのダッシュレットで、CBR 管理者により作成されたセグメントに CBR ユーザを割り当てることができます。ただし、CBR 管理者により作成されたセグメントに顧客ユーザを割り当てることはできません。

注意:このレポートで作成、管理されるセグメントは、Smart Net Total Care レポートでのデータの表示方法とアクセス方法だけに影響します。このセグメンテーションは、顧客サイトのネットワーク自体には影響しません。

ハウツー ビデオ

- ネットワーク セグメント管理

[アップロード(Uploads)]

[アップロード(Uploads)] ダッシュレットには、次の方法で契約先企業に対して実行された最新の収集のレコードが表示されます。

- CSP Collector
- CSV ファイルのインポート
- サポートされているサード パーティ コレクタからのコレクタ ファイルのアップロード

このダッシュレットでは、ポータルでのネットワーク データの更新頻度を監視できます。

[ユーザ(Users)]

このダッシュレットには、特定のアカウントのデータにアクセスできるユーザのリストが表示されます。

顧客管理者は、このダッシュレットで次の操作を実行できます。

- ユーザに対し、ポータルの特定機能へのアクセス権を付与または取り消す。
- ユーザのアカウントに対して行われた変更のログを確認する。
- CBR ユーザと CBR 管理者の認可書(LOA)を再検証する。

注:ユーザのアクセス設定に対して行われた変更は、ユーザが次回にシステムへログインするときに反映されます。

各自が管理できるユーザを確認するには、次の手順に従います。

注:この作業を実行できるのは顧客管理者だけです。

1. 縦に並んだ 3 つのドットのアイコン(⋮)をクリックし、[管理可能(Manageable)] 列を表示します(以前に非表示になっていた場合)。

   ユーザの [管理可能(Can Manage)] の値が [はい(Yes)] である場合、ユーザを管理できます。

ユーザのアクセス権を管理するには、次の手順に従います。

注:この作業を実行できるのは顧客管理者だけです。

1. ユーザ行のオプション ボタンをクリックします。
2. 右クリックしてオプション メニューを開きます。[アクセス権の管理(Manage Access)] を選択します。
3. ダイアログボックスに表示される [アクセシビリティ(Accessibility)] と [実行可能(Capabilities)] へのアクセス権をユーザに付与します。

   [アクセシビリティ(Accessibility)] はユーザに対して表示される機能を指し、[実行可能(Capabilities)] は特定のレポートでユーザがアクションを実行できるかどうかを示します。
4. [確認(Confirm)] をクリックして変更内容を保存します。

CBR ユーザの認可書を更新するには、次の手順に従います。

顧客管理者は、CBR ユーザと CBR 管理者に対してこのアクションを実行できます。

1. オプション ボタンをクリックして、ユーザを選択します。
2. [アクション(Actions)] > [認可書(LOA)へのアクセスの再認証(Revalidate Letter of Authorization (LOA) Access)] をクリックします。今後 30 日間以内に LOA 権限が期限切れとなるユーザのリストが表に示されます。
3. ユーザの LOA 権限を継続するには、[再認証(Revalidate)] をクリックします。

プロファイル更新履歴を表示するには、次の手順に従います。

1. オプション ボタンをクリックして、ユーザを選択します。
2. [アクション(Actions)] > [プロファイル更新履歴(Profile Update History)] をクリックします。選択されているユーザの管理者が実行したアクションのログが表示されます。
   このログから、他の顧客管理者が実行したアクションを確認できます。

注:このログを表示するもう 1 つの方法として、[アクション(Actions)] > [アクセスの管理(Manage Access)] ダイアログボックスの [プロファイル更新履歴(Profile Update History)] をクリックする方法もあります。

ハウツー ビデオ

- ユーザ アクセスの管理

[アラート管理(Alert Management)]

Smart Net Total Care は、シスコが発行する製品アラートとセキュリティ アドバイザリの影響を受ける顧客のデバイスに関する情報を提供します。

アラート管理ワークフローにより、ステータス メッセージを受信アラートに割り当てることができます。アクティブ アラートのステータス オプションは、[無視(Ignore)]、[アクション実行済み(Action Taken)]、または [アクションが必要(Action Required)] です。これらのステータス メッセージに基づいてアラートをフィルタリングできます。これにより、関連するアラートだけを表示できます。

[アラート管理(Alert Management)] ダッシュボードには 2 つのダッシュレットがあります。

注:アラートのテーブル ビューについては、[アラートタイプ(Alert Type)] カテゴリの横にあるリンクをクリックします。

[アクティブ アラート(Active Alerts)]

注:デフォルトのグラフ ビューでは、名前は [タイプ別アクティブアラート(Active Alerts by Type)] です。

[アクティブ アラート(Active Alerts)] ダッシュレットには、選択されているインベントリのアラート タイプ別アラート合計数が表示されます。アクティブ アラートは、ユーザがまだ確認していないアラートです。

このレポートを使用すると、次のことができます。

- カテゴリ別の未確認のアラート数の概要を把握する。
- 参照用にレポート データをエクスポートする。
- 特定のアラート カテゴリの影響を受けるデバイスを参照する。円グラフの適切なセクションをクリックします。

このレポートの目的

このダッシュレットでは、ネットワーク管理者と技術者が最も関連性の高いアラートをすぐに確認できるため、業務効率が向上し、リスク管理が強化されます。

ハウツー ビデオ

- アラートの優先順位設定
- アラート管理

[サポート終了日(Last Day of Support)]

[サポート終了日(Last Day of Support)] ダッシュレットには、デバイス ハードウェアの公開 LDoS が次の条件に該当する(選択されているインベントリ内の)デバイスの数と詳細情報がリストされます。

- 12 ヵ月以内である。
- 12 ヵ月超 24 ヵ月以内である。
- すでに終了している。

ハウツー ビデオ

- サービス契約範囲のギャップ

[契約管理(Contract Management)]

[契約管理(Contract Management)] ダッシュボードには、シスコ サービス契約のステータスと関連デバイスが表示されます。4 つのダッシュレットがあります。

[すべての契約(All Contracts)]

[すべての契約(All Contracts)] ダッシュレットには、ネットワーク検出で検出および検証されたデバイスのサービス契約に関する包括的な詳細情報が表示されます。
この情報は、[ライブラリ(Library)] > [契約(Contracts)] にも表示されます。[ライブラリ(Library)] では、デフォルトでレポートが表形式で表示されます。

詳細については、「[すべての契約(All Contracts)]」の項を参照してください。

[機器のサービス契約対象状況(Equipment Coverage)]

[機器のサービス契約対象状況(Equipment Coverage)] ダッシュレットでは、シスコ サービス契約の対象機器と対象外の機器の数の概要が示されます。このレポートには、サービス対象外のデバイスと、サポート終了日を経過しているデバイスが含まれます。

[30日以内に契約終了となる機器(Equipment with Expiring Coverage in 30 Days)]

[30日以内に契約終了となる機器(Equipment with Expiring Coverage in 30 Days)] ダッシュレットでは、30 日以内にシスコ サービス契約が終了するデバイスがリストされています。ホスト名 URL をクリックすると、詳細情報が表示されます。

[契約期限を経過している機器(Equipment with Overdue Coverage)]

[契約期限を経過している機器(Equipment with Overdue Coverage)] ダッシュレットには、契約期限が経過しているデバイスがリストされます。

[インベントリ管理(Inventory Management)]

このダッシュボードには、デバイスから収集され、シスコの製造および商取引レコードに一致するデータが表示されます。2 つのダッシュレットがあります。

このダッシュボードのダッシュレットから、ネットワーク管理者と技術者はネットワーク内のデバイスについてより詳しく把握できます。これにより、管理者や技術者は業務効率を向上しリスク管理を強化できます。

[機器タイプ(Equipment Type)]

[機器タイプ(Equipment Type)] ダッシュレットには、ネットワーク上のすべてのデバイスをカテゴリ(電源やシャーシなど)別に分類した概要が表示されます。各カテゴリをクリックし、個々のデバイス詳細情報のさまざまなカテゴリ レベルをドリルダウンできます。

ハウツー ビデオ

- インベントリの概要
- インベントリ デバイスの確認
- カスタム レポート
- 収集の詳細
- アップロード履歴の表示

[インベントリ ソース(Inventory Source)]

[インベントリ ソース(Inventory Source)] ダッシュレットには、選択されているインベントリのデバイスごとに、インベントリのアップロード元ソース(コレクタ(CSPC およびサードパーティ)、CSV ファイル インポート、またはコレクタ ファイル アップロード)が表示されます。

ハウツー ビデオ

- インベントリの概要
- インベントリ デバイスの確認
- カスタム レポート
- 収集の詳細
- アップロード履歴の表示

Smart Net Total Care

Smart Net Total Care ポータルに初めてアクセスすると表示されるデフォルトのダッシュボードです。このダッシュボードには、4 つのダッシュレットがあります。

[機器タイプ(Equipment Type)]

「[機器タイプ(Equipment Type)]」を参照してください。

[機器のサービス契約対象状況(Equipment Coverage)]

「[機器のサービス契約対象状況(Equipment Coverage)]」を参照してください。

[アクティブアラート(Active Alerts)]

「[アクティブアラート(Active Alerts)]」を参照してください。

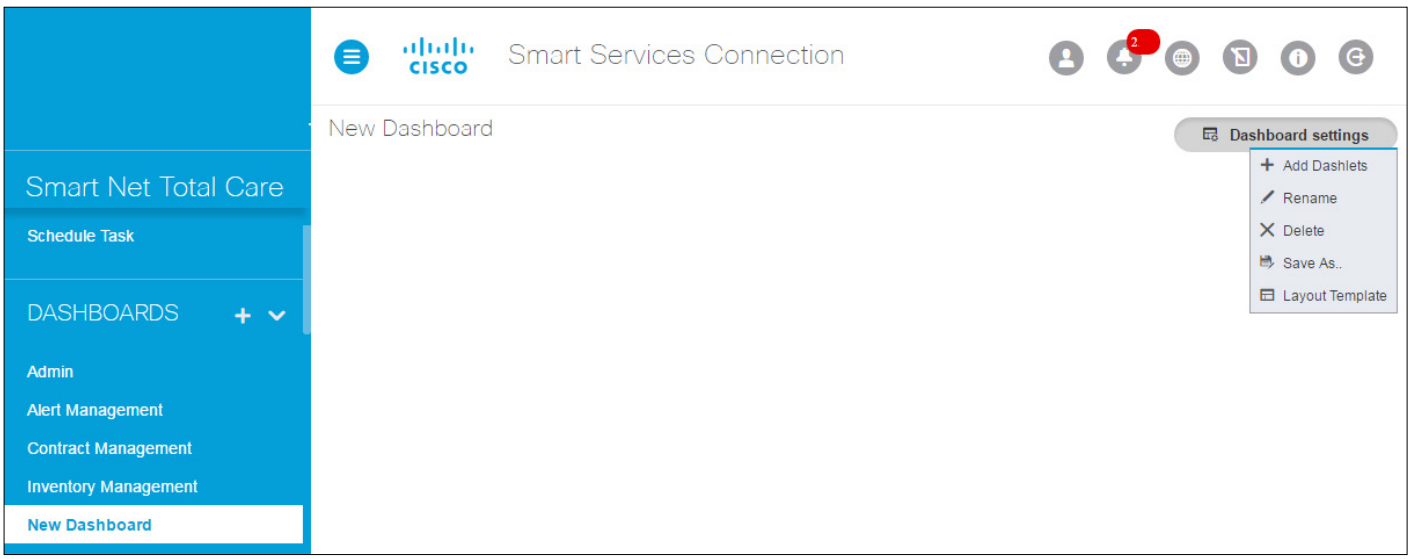
[コミュニティ(Community)]

[コミュニティ(Community)] ダッシュレットには、Smart Net Total Care チームからの最近のアナウンスと、オンライン フォーラムで人気の高いディスカッション トピックへのリンクが表示されます。

カスタム ダッシュボードの作成

各自にとって重要なレポートを表示するカスタム ダッシュボードを作成することができます。これらのダッシュボードはポータルに保存され、LNP からアクセスできます。各自のダッシュボードを作成するには、次の手順を実行します。

1. LNP で [DASHBOARDS] というラベルの横の「+」記号をクリックします。[新規ダッシュボード(New Dashboard)] という空白のペインが開きます。
2. [新規ダッシュボード(New Dashboard)] ペインで [ダッシュボードの設定(Dashboard settings)] > [レイアウトテンプレート(Layout Template)] をクリックします。 ダッシュボードに利用できるすべてのレイアウトが表示されます。
3. レイアウトを選択するには、そのレイアウトの横のオプション ボタンをクリックします。
4. [ダッシュレットの追加(Add Dashlet)] をクリックします。ライブラリのすべてのレポートのリストが表示されます。



5. ダッシュボードに含めるレポートを選択します。表示するレポートをすべて追加するまで操作を続行します。

6. [名前をつけて保存(Save As)] をクリックしてダッシュボードを保存します。ダッシュボードを保存するときに、新しい名前を指定できます。
7. ダッシュボードの名前を変更するには、[名前の変更(Rename)] をクリックします。
8. ダッシュボードを削除するには、[削除(Delete)] をクリックします。

ライブラリ

すべての Smart Net Total Care レポートは、ライブラリで次のカテゴリに分類されます。

- [管理(Administration)]
- [アラート(Alerts)]
- [アーキテクチャ アセスメント(Architecture Assessment)]
- [契約(Contracts)]
- [インシデント(Incidents)]
- [インベントリ(Inventory)]
- [インベントリインサイト(Inventory Insight)]

[管理(Administration)]

管理者は、このカテゴリのレポートでサービス契約範囲/期間を追跡し、新しいデバイスを特定およびモニタし、関連度が最も高いアラートを分類できます。信頼性の高い定期的なレポートにより、懸念事項を事前に把握し、リスクを最小限に抑えることができます。これらのレポートは、リソース プランニングと予算配賦にも役立ちます。

[契約のプロパティ(Contracts Properties)]

[契約のプロパティ(Contracts Properties)] レポートでは、契約を統合レポートに含めるかどうかを設定できます。このレポートには、変更を実行したユーザの名前とコメントも表示されます。

統合レポートに契約を含めるには、次の手順に従います。

1. チェックボックスをクリックして、含める契約を選択します。
2. [アクション(Actions)] > [契約プロパティの編集(Edit Contract Properties)] をクリックします。[契約プロパティの編集(Edit Contract Properties)] ウィンドウが表示されます。
3. [統合レポートの範囲内(In Scope for Aggregated Report)] チェックボックスをクリックします。
4. [名前(Name)] フィールドに名前を入力します。
5. [コメント(Comment)] フィールドにコメントを入力します。この手順は任意です。
6. [OK] をクリックして確定します。

監査履歴を表示するには、次の手順に従います。

1. チェックボックスをクリックして、監査履歴を表示する契約を選択します。
2. [アクション(Actions)] > [監査履歴の表示(View Audit History)] をクリックします。

[アップロード処理状況(Upload Processing)]

[アップロード処理状況(Upload Processing)] レポートには、完了したインベントリのステータス、またはデータ分析が進行中のインベントリのステータスが表示されます。インベントリ アップロード ソースには、CSPC およびサードパーティ コレクタからの収集、CSV ファイルのインポート、およびコレクタ ファイルのアップロードがあります。

[アクティブアラート(Active Alerts)]

注:このレポートは管理者と承認ユーザだけが使用できます。

[アクティブアラート(Active Alerts)] レポートでは、管理者がアラートを確認し、ユーザへのアラート アクセスを提供/管理できます。管理者はこのレポートを使用して次のことができます。

- アラート ステータスを [無視(Ignore)] に設定し、コメントまたは注にその理由を記述する。これは、影響を受けるすべてのデバイスまたは特定のデバイスに対して設定できます。
- アラートへの注意を促すための注を入力する。
- [詳細情報(More Info)] 列でリンクをクリックして、アラートの詳細を表示する。
- 各アラートのステータスと注を確認する。

このレポートの目的

このレポートでは、ネットワーク管理者と技術者が最も重要なアラートに集中して取り組むことができるようにすることで、業務効率が向上し、リスク管理が強化されます。

特定のアラートの影響を受けるすべてのデバイスのアラート ステータスを変更するには、次の手順に従います。

1. 変更する各行のチェックボックスをクリックします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 新しいウィンドウが開きます。
3. アラートのステータスを [アクティブ(Active)] から [無視(Ignore)] に変更するには、[無視(Ignore)] を選択します。
   アラートは [アクティブアラート(Active Alerts)] レポートに表示されなくなります。[アクティブ(Active)] ステータスに戻すには、[すべてのアラート(All Alert)] レポートを使用します。
4. [注(Notes)] フィールドに注を入力します。この手順は任意です。
5. [コメント(Comment)] フィールドにコメントを入力します。この手順は任意です。
6. [OK] をクリックして確定します。

注:アラートのステータスの変更はすべてのインベントリに影響します。

アラート タイプの影響を受けるデバイスのリストを表示するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列の数値リンクをクリックします。この操作により、個々のデバイスのアラート ステータスを管理することもできます。

アラート ステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

ハウツー ビデオ

- 関連アラートの特定
- アラート管理

[すべてのコレクタ(All Collectors)]

[すべてのコレクタ(All Collectors)] レポートには、選択された企業に対して登録されているコレクタがリストされます。

これらのコレクタから収集されたデータは、ポータルによって報告されるデータに含まれます。その他のデータ アップロード方法には、CSV ファイルのインポートとコレクタ ファイルのアップロードがあります。

ファイルのインポート

注:管理者と承認ユーザだけがファイルのインポートを実行できます。

スプレッドシートでデバイス データを手動で管理している場合は、形式設定されたデータを Smart Net Total Care ポータルにアップロードできます。データは、シスコのサポート情報と関連付けて分析され、補強されます。この機能により、デバイス インベントリ データをオンサイト コレクタからアップロードするのではなく、ファイルからアップロードすることができます。

ファイルのインポート機能は、コレクタをインストールしない場合に唯一のデータ アップロード方法として使用するか、または、コレクタと組み合わせて使用することができます。

デバイス データ ファイルは次のいずれかの方法で生成できます。

- 提供されるテンプレート ファイルを使用し、このファイルにデバイス情報を入力する。
- コレクタを使用してデバイス ファイルを生成し、[ファイルのインポート(File Import)] を使用してデバイス データをアップロードする。この場合、コレクタを使用してデバイス データを収集しますが、データのアップロードは手動で行います。

ファイルのアップロードとコレクタを組み合わせて使用すると、コレクタのインベントリを補強できます。これにより、ネットワーク内にあるがコレクタによって収集できないデバイスを追加できます。このようなデバイスはファイアウォールで保護されているか、電源がオフであるか、またはネットワークに接続されていないデバイスである可能性があります。

テンプレートを使用して CSV ファイルをアップロード用に準備するには、次の手順に従います。

1. [インポートタイプ(Import Type)] として [CSVファイルインポート(CSV File Import)] を選択します。
2. リンクをクリックして、サンプル CSV ファイルをダウンロードします。
3. パラメータの情報を入力します。行 2 と列 I を必ず削除してください。
4. ファイルを .csv ファイルとして保存します。

注:ファイルのインポート機能にアクセスするときには、1 つのインベントリだけを選択できます。

コレクタ ファイルをアップロード用に準備するには、次の手順に従います。

1. コレクタからインベントリ ファイルを取得します。このファイルは変更しないでください。
2. ファイルをローカル ハード ドライブに保存します。

CSV ファイルまたはコレクタ ファイルをアップロードするには、次の手順に従います。

1. 適切なインポート タイプ(CSV ファイルのインポートまたはコレクタ ファイルのインポート)を選択します。
2. 既存のインベントリを選択するか、[新規インベントリの作成(Create a New Inventory)] をクリックします。
3. 新規インベントリを作成する場合は、表示されるフィールドに名前を入力します。
4. アップロードするファイルのタイプ(コレクタ生成ファイルまたはテンプレートを使用した CSV ファイル)を選択します。
5. [ファイルの選択(Choose File)] をクリックして、ローカル デスクトップでファイルを特定します。
6. [インポート(Import)] をクリックしてアップロードを実行します。

シリアル番号と製品 ID は、シスコにより有効であると認識される必要があります。つまり、シリアル番号と製品 ID は、シスコ データベース内で「契約先」企業に関連付けられているデータに一致している必要があります。値が有効な値として認識されない場合は、[インベントリ インサイト(Inventory Insight)] レポートに、認識されないアイテムとして表示されます。

注:以降のアップロードで CSV ファイルにデバイスを追加できます。追加されたデバイスは、先にアップロードされたデバイスに追加されます。インポートされたファイルのステータスを確認するには、[管理(Administration)] ライブラリの [アップロード処理状況(Upload Processing)] をクリックします。

ファイルのアップロードの詳細については、Smart Net Total Care サポート コミュニティを参照してください。

ハウツー ビデオ

- ファイルのインポート機能

[サービス契約範囲(Service Coverage)]

[サービス契約範囲(Service Coverage)] レポートでは、デバイスがサービス契約対象外である理由を設定、確認できます。このレポートを使用すると、次のことができます。

- 契約範囲の決定を文書化する。
- 更新のための実用的な情報を入力する。

このレポートの目的

契約管理者はこのレポートを使用して、サービス契約対象にする必要があるデバイスと、レビュー済みであり無視することを選択したデバイスの更新アクションに集中して取り組むことができます。これにより、業務効率が向上しリスク管理を強化できます。

サービス契約更新の準備に入る前に、レポートを確認して次の手順を実行します。

1. 機器タイプ別にサービス契約対象外のデバイスを確認する。
2. 一部のアイテムでサービス契約が不要な理由を記録する。
3. [要レビュー(Review Needed)] とマークされたデバイスをフィルタリングする。
4. PDF、CSV、XLSX 形式でデータをエクスポートする。
5. 計画ミーティングでネットワーク管理者とデータを共有する。

デバイスが契約対象外である理由を設定するには、次の手順に従います。

1. 対象デバイスのチェックボックスをオンにします。
2. [アクション(Actions)] > [サービス契約対象外の理由(Service Not Covered Reason)] を選択します。
3. 理由を選択します。
4. [コメント(Comments)] フィールドにコメントを入力します。この手順は任意です。
5. [OK] をクリックして確定します。システムによって生成された確認メッセージが表示されます。
6. メッセージを読み、ダイアログボックスを閉じます。

デバイスでの理由の設定履歴を表示するには、次の手順に従います。

1. 対象デバイスのチェックボックスをオンにします。

2. [アクション(Actions)] > [表示(View)] > [契約対象外の理由の履歴を表示(View Not Covered Reason History)] を選択します。 選択したデバイスで使用可能な理由とコメントのリストが表示されます。

注:このレポートで選択された理由と入力されたコメントは、[契約対象外(Not Covered)] レポートの [ライブラリ(Library)] > [契約(Contracts)] の下にも表示されます。

ハウツー ビデオ

- サービス適用範囲の管理

アラート

このカタログのレポートは、ポータルに表示されるアラートに関連しています。ネットワーク内のデバイスに影響するアラートを特定して事前に対応することで、ネットワークの中断を事前に防止できます。

- ハードウェア アラートは、ネットワークのデバイスのサポート終了に関する情報を通知します。
- ソフトウェア アラートは、使用しているソフトウェア バージョンのサポート終了に関する情報を通知します。
- セキュリティ アラートは、ネットワーク上の特定デバイスに関連するセキュリティの脆弱性を通知します。
- ハードウェアの Field Notice は、ハードウェア デバイスの重大な問題(セキュリティの脆弱性の問題以外)を通知します。ハードウェアの Field Notice は、顧客のアクション(RMA など)を必要とすることがよくあります。
- ソフトウェアの Field Notice は、使用しているソフトウェア バージョンのその他の重大な問題(セキュリティの脆弱性の問題以外)を通知します。ソフトウェアの Field Notice は、顧客のアクションを必要とすることがよくあります。

これらのレポートの目的

ネットワーク管理者と技術者は、これらのレポートにより、最も重要なアラートと Field Notice を迅速に確認できるため、業務効率が向上し、リスク管理が強化されます。

ハウツー ビデオ

- アラートの優先順位設定
- アラート管理

[すべてのアラート(All Alerts)]

[すべてのアラート(All Alerts)] レポートには、選択されているインベントリの製品アラートがタイプ別にリストされます。このレポートを使用すると、次のことができます。

- アラートのステータスを [無視(Ignore)] から [アクティブ(Active)] に変更する。
- 影響を受けるデバイスの数に基づくアラートを確認する。

最も多くのデバイスに影響するアラートを確認するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列ヘッダーをクリックして矢印の向きを下にします。これにより、情報が降順でソートされます。

シスコが発行したアラートの説明を表示するには、次の手順に従います。

1. [詳細情報(More Info)] 列で、該当するアラート行の URL をクリックします。

アラート ステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

アラート ステータスを [無視(Ignore)] から [アクティブ(Active)] に変更するには、次の手順に従います。

注:この作業を実行できるのは、管理者とアラート管理権限を持つユーザだけです。

1. 変更する各アラートのチェックボックスをオンにします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 デフォルトでは [アクティブ(Active)] ステータスが選択されています。
3. [注(Notes)] フィールドに注を入力します。この手順は任意です。

このレポートの [アクション(Actions)] メニューでは、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更することはできません。管理者レポートにアクセスできる場合は、[ライブラリ(Library)] > [管理(Administration)] > [アクティブアラート(Active Alerts)] に移動し、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更します。それ以外の場合は、組織内の顧客管理者に連絡してください。

注:特定のアラートの影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

[すべてのField Notice(All Field Notices)]

[すべてのField Notice(All Field Notices)] レポートには、選択されているインベントリのハードウェア Field Notice がタイプ別にリストされます。このレポートを使用すると、次のことができます。

- Field Notice のステータスを [無視(Ignore)] から [アクティブ(Active)] に変更する。
- 次の条件に基づいて Field Notice を確認する。
  - 影響を受けるデバイスの数。
  - Field Notice の脆弱性アセスメント。

最も多くのデバイスに影響する Field Notice を確認するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列ヘッダーをクリックして矢印の向きを下にします。これにより、情報が降順でソートされます。

シスコが発行した Field Notice の説明を表示するには、次の手順に従います。

1. [詳細情報(More Info)] 列で、該当する行の URL をクリックします。

Field Notice のステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

Field Notice のステータスを [無視(Ignore)] から [アクティブ(Active)] に変更するには、次の手順に従います。

注:この作業を実行できるのは、管理者とアラート管理権限を持つユーザだけです。

1. 変更する各 Field Notice のチェックボックスをオンにします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 デフォルトでは [アクティブ(Active)] が選択されています。
3. [注(Notes)] フィールドに注を入力します。この手順は任意です。

注:特定の Field Notice の影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

このレポートの [アクション(Actions)] メニューでは、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更することはできません。管理者レポートにアクセスできる場合は、[ライブラリ(Library)] > [管理(Administration)] > [アクティブアラート(Active Alerts)] に移動し、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更します。それ以外の場合は、組織内の Smart Net Total Care 管理者に連絡してください。

[すべてのハードウェアアラート(All Hardware Alerts)]

[すべてのハードウェアアラート(All Hardware Alerts)] レポートには、選択されているインベントリのハードウェア アラートがタイプ別にリストされます。このレポートを使用すると、次のことができます。

- アラートのステータスを [無視(Ignore)] から [アクティブ(Active)] に変更する。
- 次の条件に基づいてアラートを確認する。
  - 影響を受けるデバイスの数。
  - デバイス ハードウェアのサポート終了日(公開されている場合)。

最も多くのデバイスに影響するアラートを確認するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列ヘッダーをクリックして矢印の向きを下にします。これにより、情報が降順でソートされます。

シスコが発行したアラートの説明を表示するには、次の手順に従います。

1. [詳細情報(More Info)] 列で、該当する行の URL をクリックします。

アラート ステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

アラート ステータスを [無視(Ignore)] から [アクティブ(Active)] に変更するには、次の手順に従います。

注:この作業を実行できるのは、管理者とアラート管理権限を持つユーザだけです。

1. 変更する各アラートのチェックボックスをオンにします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 デフォルトでは [アクティブ(Active)] が選択されています。

注:特定のアラートの影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

3. [注(Notes)] フィールドに注を入力します。この手順は任意です。

このレポートの [アクション(Actions)] メニューでは、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更することはできません。管理者レポートにアクセスできる場合は、[ライブラリ(Library)] > [管理(Administration)] > [アクティブアラート(Active Alerts)] に移動し、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更します。それ以外の場合は、組織内の Smart Net Total Care 管理者に連絡してください。

[すべての PSIRT(All PSIRTs)]

[すべての PSIRT(All PSIRTs)] レポートには、選択されているインベントリの Product Security Incident Response Team アドバイザリ(PSIRT)がタイプ別にリストされます。PSIRT は、次のオペレーティング システムを実行しているデバイスでのみ利用できます。

- IOS
- IOS XE
- ASA
- IOS XR
- NX-OS

注:レポートには [高(High)] および [重大(Critical)] の PSIRT アドバイザリのみが表示されます。

このレポートを使用すると、次のことができます。

- PSIRT のステータスを [無視(Ignore)] から [アクティブ(Active)] に変更する。
- 次の条件に基づいてアラートを確認する。
  - 影響を受けるデバイスの数。
  - PSIRT の脆弱性アセスメント。

最も多くのデバイスに影響する PSIRT を確認するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列ヘッダーをクリックして矢印の向きを下にします。これにより、情報が降順でソートされます。

シスコが発行した PSIRT の説明を表示するには、次の手順に従います。

1. [詳細情報(More Info)] 列で、該当する行の URL をクリックします。

PSIRT ステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

PSIRT のステータスを [無視(Ignore)] から [アクティブ(Active)] に変更するには、次の手順に従います。

注:この作業を実行できるのは、管理者とアラート管理権限を持つユーザだけです。

1. 変更する各 PSIRT のチェックボックスをオンにします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 デフォルトでは [アクティブ(Active)] が選択されています。

   注:特定のアラートの影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

3. [注(Notes)] フィールドに注を入力します。この手順は任意です。

注:特定のアラートの影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

このレポートの [アクション(Actions)] メニューでは、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更することはできません。管理者レポートにアクセスできる場合は、[ライブラリ(Library)] > [管理(Administration)] > [アクティブアラート(Active Alerts)] に移動し、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更します。それ以外の場合は、組織内の Smart Net Total Care 管理者に連絡してください。

[すべてのソフトウェアアラート(All Software Alerts)]

[すべてのソフトウェアアラート(All Software Alerts)] レポートには、選択されているインベントリのソフトウェア アラートがタイプ別にリストされます。このレポートを使用すると、次のことができます。

- アラートのステータスを [無視(Ignore)] から [アクティブ(Active)] に変更する。
- 次の条件に基づいてアラートを確認する。
  - 影響を受けるデバイスの数。
  - デバイス ソフトウェアのサポート終了日(公開されている場合)。

最も多くのデバイスに影響するアラートを確認するには、次の手順に従います。

1. [影響を受けるデバイス(Affected Devices)] 列ヘッダーをクリックして矢印の向きを下にします。これにより、情報が降順でソートされます。

シスコが発行したアラートの説明を表示するには、次の手順に従います。

1. [詳細情報(More Info)] 列で、該当する行の URL をクリックします。

アラート ステータスと注を表示するには、次の手順に従います。

1. [ステータス(Status)] 列と [注(Notes)] 列がデフォルトで表示されていない場合は、これらの列を表示します。

アラート ステータスを [無視(Ignore)] から [アクティブ(Active)] に変更するには、次の手順に従います。

注:この作業を実行できるのは、管理者とアラート管理権限を持つユーザだけです。

1. 変更する各 Field Notice のチェックボックスをオンにします。
2. [アクション(Actions)] > [アラートステータスの変更(Change Alert Status)] をクリックします。 デフォルトでは [アクティブ(Active)] が選択されています。
3. [注(Notes)] フィールドに注を入力します。この手順は任意です。

注:特定のアラートの影響を受けるすべてのデバイスに対してアクションを実行している場合、ステータスは [確認(Acknowledge)] です。

このレポートの [アクション(Actions)] メニューでは、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更することはできません。管理者レポートにアクセスできる場合は、[ライブラリ(Library)] > [管理(Administration)] > [アクティブアラート(Active Alerts)] に移動し、ステータスを [アクティブ(Active)] から [無視(Ignore)] に変更します。それ以外の場合は、組織内の Smart Net Total Care 管理者に連絡してください。

[アラートが出ているデバイス(Devices with Alerts)]

[アラートが出ているデバイス(Devices with Alerts)] レポートには、選択されているインベントリの各デバイスのアラート タイプ別のアラート数が表示されます。

デバイスの固有のアラートを表示するには、次の手順に従います。

1. 各アラート タイプの列の数値リンクをクリックします。

[サポート終了日(Last Day of Support)]

[サポート終了日(Last Day of Support)] レポートには、(選択されているインベントリで)デバイス ハードウェアの公開されているサポート最終日(LDoS)が今後 2 年以内であるか、または終了日を経過しているすべてのデバイスがリストされます。

このレポートの目的

ネットワーク管理者と契約管理者は、このレポートを使用して、現在または今後に発生するデバイスの可用性の変更について事前に計画できます。これにより業務効率が向上し、リスク管理が強化されます。

[サポート終了日(Last Date of Support)] 列の日付範囲を変更するには、次の手順に従います。

1. [サポート終了日(Last Date of Support)] 列ヘッダーの下の検索フィールドをクリックし、日付検索機能を使用して日付範囲を入力します。

特定のデバイスの LDoS レコードを表示するには、次の手順に従います。

1. [シリアル番号(Serial Number)] 列ヘッダーの下の検索フィールドをクリックし、デバイスのシリアル番号を入力します。
2. Enter を押します。レコードが表示されない場合は、デバイス ハードウェアの LDoS が今後 2 年以内の日付ではありません。

LDoS アラートを表示するには、次の手順に従います。

1. [アラート定義(Alert Definition)] 列で、対応するリンクをクリックします。

デバイスの契約の詳細情報を表示するには、次の手順に従います。

1. [契約番号(Contract No.)] 列が表示されるまで、レポートを左右にスクロールします。
2. 該当するデバイスに対応する URL をクリックします。[契約番号(Contract No.)] の値が [その他(Other)] または [パートナーブランド契約(Partner Branded Contracts)] の場合、詳細にアクセスできる権限がありません。

ハウツー ビデオ

- サービス契約範囲のギャップ

[プロダクト アラート デルタ(Product Alerts Delta)]

[プロダクト アラート デルタ(Product Alerts Delta)] レポートには、指定された期間におけるすべてのアラート カテゴリの追加/変更されたアラートの数が表示されます。

- [追加された数(Added number)] は、開始日から終了日までの間に追加されたアラートの数を示します。
- [変更された数(Changed number)] は、開始日から終了日までの間に変更されたアラートの数を示します。

日付範囲を変更するには、次の手順に従います。

1. [日付の変更(Change Dates)] をクリックします。[カレンダー(Calendar)] ダイアログボックスが開きます。
2. 開始日と終了日を入力します。
3. [OK] をクリックして確定します。

カテゴリ別のデバイスのリストを表示するには、次の手順に従います。

1. 変更または追加された列の番号付きリンクをクリックします。

[アーキテクチャ アセスメント(Architecture Assessment)]

[アーキテクチャ アセスメント(Architecture Assessment)] レポートには、選択されているインベントリ内のデバイスのアーキテクチャ アセスメントが表示されます。

これらのレポートの目的

デバイス アセスメント レポート:

- より効果的なネットワーク アーキテクチャ戦略とソリューション ベースのアーキテクチャを作成できる。
- アップグレードまたは更新する必要があるデバイスを特定し、必要な変更に対応するための計画を準備できる。

クラウド インテリジェント ネットワーク

クラウド インテリジェント ネットワーク(CIN)アセスメント レポートには、インベントリ内のデバイスとその CIN アセスメント ステータスが表示されます。シスコ クラウド インテリジェント ネットワークは、世界中の多くのクラウドの接続を支援するための基盤となります。このネットワークは、データセンター内とクラウド間の両方のコンピューティングを統合するプラットフォームであり、最終的にクラウド エクスペリエンスをエンドユーザに提供します。

このレポートは、シスコ クラウド インテリジェント ネットワークをサポートできるネットワーク内のデバイスを特定するのに役立ちます。レポートには次の情報が表示されます。

- 環境内のデバイスの総数。
- CIN をサポートできる環境内のデバイスの数とパーセンテージ。
- CIN をサポートできない環境内のデバイスの数とパーセンテージ。
- ソフトウェアまたはハードウェアのアップグレードにより CIN をサポートできるデバイスの数とパーセンテージ。

レポートのテーブル ビューには、次の新しい列が追加されています。

- [CIN アセスメント ステータス(CIN Assessment Status)]:デバイスが CIN をサポートできるかどうか。
- [ネットワーク内の場所(Place in Network)]:デバイスが配置されているネットワーク内の場所。
- [アップグレードの理由(Upgrade Reason)]:アップグレードが推奨される理由。
- [推奨されるイメージ バージョン(Recommended Image Version)]:ソフトウェアのアップグレードが必要な場合に表示されます。
- [推奨されるハードウェア(Recommended Hardware)]:ハードウェアのアップグレードが必要な場合に表示されます。
- [推奨されるハードウェアの CIN 機能(CIN Features of Recommended Hardware)]:推奨されるハードウェアに必要な CIN 機能。

デバイスのクラウド インテリジェント ネットワーク アセスメント ステータスを表示するには、次の手順に従います。

1. テーブル ビューをクリックし、インベントリ内の各デバイスの詳細を表示します。

   [CIN アセスメント ステータス(CIN Assessment Status)] 列には、デバイスのステータスが表示されます。アセスメント ステータスは次のとおりです。

   - [未サポート(UNSUPPORTED)]:このデバイスは、アップグレードしても CIN をサポートできません。交換する必要があります。
   - [対応(CAPABLE)]:このデバイスは CIN をサポートできます。
   - [ハードウェア非対応(HARDWARE INCAPABLE)]:このデバイスはハードウェアをアップグレードすれば CIN をサポートできます。
   - [ソフトウェア非対応(SOFTWARE INCAPABLE)]:このデバイスはソフトウェアをアップグレードすれば CIN をサポートできます。

クラウド インテリジェント ネットワーク アセスメント レポートを再生成するには、次の手順に従います。

1. [アクション(Actions)] > [再生成(Regenerate)] をクリックして、最新のインベントリに基づいてレポートを再生成します。

EnergyWise

EnergyWise アセスメント レポートには、インベントリ内のデバイス、その EnergyWise アセスメント ステータス、および推奨事項が表示されます。Cisco Energy Management Suite には、分散オフィスやデータセンター環境で接続されている全デバイスのエネルギー使用量を測定および管理できるソフトウェアとサービスが含まれています。

このレポートは、Cisco Energy Management Suite ソフトウェアをサポートできるネットワーク内のデバイスを特定するのに役立ちます。EnergyWise アセスメント レポートには次の情報が表示されます。

- 環境内のデバイスの総数。
- EnergyWise をサポートできる環境内のデバイスの数とパーセンテージ。
- EnergyWise をサポートできない環境内のデバイスの数とパーセンテージ。
- ソフトウェアまたはハードウェアのアップグレードにより EnergyWise をサポートできるデバイスの数とパーセンテージ。

レポートのテーブル ビューには、次の新しい列が追加されています。

- [EnergyWise アセスメント レポート(EnergyWise Assessment Report)]:デバイスが EnergyWise をサポートできるかどうか。
- [推奨される OS バージョン(Recommended OS Version)]:ソフトウェアのアップグレードが必要な場合に表示されます。

デバイスの EnergyWise アセスメント ステータスを表示するには、次の手順に従います。

1. テーブル ビューをクリックし、インベントリ内の各デバイスの詳細を表示します。

   [EnergyWise アセスメント ステータス(EnergyWise Assessment Status)] 列には、デバイスのステータスが表示されます。アセスメント ステータスは次のとおりです。

   - [未サポート(UNSUPPORTED)]:このデバイスは、アップグレードしても EnergyWise をサポートできません。交換する必要があります。
   - [対応(CAPABLE)]:このデバイスは EnergyWise をサポートできます。
   - [ハードウェア非対応(HARDWARE INCAPABLE)]:このデバイスはハードウェアをアップグレードすれば EnergyWise をサポートできます。
   - [ソフトウェア非対応(SOFTWARE INCAPABLE)]:このデバイスはソフトウェアをアップグレードすれば EnergyWise をサポートできます。[推奨される OS バージョン(Recommended OS Version)] 列には、オペレーティング システムのバージョンに関する推奨事項が表示されます。

EnergyWise アセスメント レポートを再生成するには、次の手順に従います。

1. [アクション(Actions)] > [再生成(Regenerate)] をクリックして、最新のインベントリに基づいてレポートを再生成します。

[IPv6]

[IPv6] アセスメント レポートには、インベントリ内のデバイスとその IPv6 アセスメント ステータスが表示されます。テーブル ビューにはインベントリ内の個々のデバイスの詳細情報が表示され、サマリー レポートには次の情報が表示されます。

- 環境内の IPv6 対応デバイスの数とパーセンテージ。
- 環境内の IPv6 非対応デバイスの数とパーセンテージ。
- ソフトウェアまたはハードウェアのアップグレードにより IPv6 対応にできるデバイスの数とパーセンテージ。

- 詳細な分析を必要とするデバイスの数とパーセンテージ。これらのデバイスは、シリアル番号や OS バージョンなどの重要な情報を取得できないデバイスです。

デバイスの IPv6 アセスメント ステータスを表示するには、次の手順に従います。

1. テーブル ビューをクリックし、インベントリ内の各デバイスの詳細を表示します。[IPv6 アセスメント(IPv6 Assessment)] 列に、デバイスの IPv6 ステータスが表示されます。

   [IPv6 アセスメント(IPv6 Assessment)] 列には、デバイスの IPv6 ステータスが表示されます。アセスメント ステータスは次のとおりです。

   - [対応(CAPABLE)]:このデバイスは IPv6 をサポートできます。
   - [より詳細な分析(FURTHER ANALYSIS)]:このデバイスのシリアル番号や OS バージョンなどの情報を取得できませんでした。
   - [非対応(NOT CAPABLE:)]:このデバイスはハードウェアを交換しないと IPv6 をサポートできません。
   - [アップグレードが必要(REQUIRES UPGRADE:)]:このデバイスはソフトウェアかハードウェアをアップグレードすれば IPv6 をサポートできます。

IPv6 アセスメント レポートを再生成するには、次の手順に従います。

1. [アクション(Actions)] > [再生成(Regenerate)] をクリックして、最新のインベントリに基づいてレポートを再生成します。

ハウツー ビデオ

- IPv6 アセスメント レポート

MediaNet

MediaNet アセスメント レポートには、インベントリ内のデバイスとその MediaNet アセスメント ステータスが表示されます。このレポートは、リッチ メディア アプリケーション向けに最適化されたインテリジェント ネットワークをサポートできるネットワーク内のデバイスを特定するのに役立ちます。Cisco MediaNet は、ビデオおよびコラボレーション展開向けにシスコが推奨するアーキテクチャです。

MediaNet アセスメント レポートには次の情報が表示されます。

- 環境内のデバイスの総数。
- MediaNet をサポートできる環境内のデバイスの数とパーセンテージ。
- MediaNet をサポートできない環境内のデバイスの数とパーセンテージ。
- ソフトウェアまたはハードウェアのアップグレードにより MediaNet をサポートできるデバイスの数とパーセンテージ。

レポートのテーブル ビューには、次の新しい列が追加されています。

- [MediaNet アセスメント レポート(MediaNet Assessment Report)]:デバイスが MediaNet をサポートできるかどうか。
- [ネットワーク内の場所(Place in Network)]:デバイスが配置されているネットワーク内の場所。
- [重点分野(Focus Area)]:デバイスが重点を置いている分野。 キャパシティや可視性など。
- [推奨されるハードウェア(Recommended Hardware)]:ハードウェアのアップグレードが必要な場合に表示されます。
- [推奨されるソフトウェア(Recommended Software)]:ソフトウェアのアップグレードが必要な場合に表示されます。
- [推奨される機能構成(Recommended Feature Configuration)]:パフォーマンスの向上に役立つ環境設定の更新。

デバイスの MediaNet アセスメント ステータスを表示するには、次の手順に従います。

1. テーブル ビューをクリックし、インベントリ内の各デバイスの詳細を表示します。

   [MediaNet アセスメント ステータス(MediaNet Assessment Status)] 列には、デバイスのステータスが表示されます。アセスメント ステータスは次のとおりです。

   - [対応(CAPABLE)]:このデバイスは MediaNet をサポートできます。
   - [より詳細な分析(FURTHER ANALYSIS)]:このデバイスのシリアル番号や OS バージョンなどの情報を取得できませんでした。
   - [機能非対応(FEATURE INCAPABLE)]:このデバイスには MediaNet をサポートするために必要な特定の機能がありません。
   - [ハードウェア非対応(HARDWARE INCAPABLE)]:このデバイスはハードウェアをアップグレードすれば MediaNet をサポートできます。
   - [ソフトウェア非対応(SOFTWARE INCAPABLE)]:このデバイスはソフトウェアをアップグレードすれば MediaNet をサポートできます。

MediaNet アセスメント レポートを再生成するには、次の手順に従います。

1. [アクション(Actions)] > [再生成(Regenerate)] をクリックして、最新のインベントリに基づいてレポートを再生成します。

TrustSec

TrustSec アセスメント レポートには、インベントリ内のデバイスとその TrustSec アセスメント ステータスが表示されます。Cisco TrustSec では、ソフトウェア定義型セグメンテーションによって、マルウェア増殖のリスクの軽減、セキュリティ運用の簡素化、コンプライアンス目標達成の支援を行います。このレポートは、Cisco TrustSec をサポートできるネットワーク内のデバイスを特定するのに役立ちます。

レポートには次の情報が表示されます。

- 環境内のデバイスの総数。
- TrustSec をサポートできる環境内のデバイスの数とパーセンテージ。
- TrustSec をサポートできない環境内のデバイスの数とパーセンテージ。
- ソフトウェアまたはハードウェアのアップグレードにより TrustSec をサポートできるデバイスの数とパーセンテージ。

レポートのテーブル ビューには、次の新しい列が追加されています。

- [TrustSec アセスメント ステータス(TrustSec Assessment Status)]:デバイスが TrustSec をサポートできるかどうか。
- [推奨されるイメージ バージョン(Recommended Image Version)]:ソフトウェアのアップグレードが必要な場合に表示されます。
- [推奨されるハードウェア(Recommended Hardware)]:ハードウェアのアップグレードが必要な場合に表示されます。
- [TrustSec 機能(TrustSec Features)]:利用可能な TrustSec 機能。

デバイスの TrustSec アセスメント ステータスを表示するには、次の手順に従います。

1. テーブル ビューをクリックし、インベントリ内の各デバイスの詳細を表示します。

   [TrustSec アセスメント ステータス(TrustSec Assessment Status)] 列には、デバイスのステータスが表示されます。アセスメント ステータスは次のとおりです。

- [未サポート(UNSUPPORTED)]:このデバイスは、アップグレードしても TrustSec をサポートできません。交換する必要があります。
- [対応(CAPABLE)]:このデバイスは TrustSec をサポートできます。
- [ハードウェア非対応(HARDWARE INCAPABLE)]:このデバイスはハードウェアをアップグレードすれば TrustSec をサポートできます。
- [ソフトウェア非対応(SOFTWARE INCAPABLE)]:このデバイスはソフトウェアをアップグレードすれば TrustSec をサポートできます。

TrustSec アセスメント レポートを再生成するには、次の手順に従います。

1. [アクション(Actions)] > [再生成(Regenerate)] をクリックして、最新のインベントリに基づいてレポートを再生成します。

[契約(Contracts)]

このライブラリのレポートには、企業がシスコと締結しているサービス契約に関する情報が表示されます。

[すべての契約(All Contracts)]

[すべての契約(All Contracts)] レポートには、すべてのサービス契約、契約対象のデバイス、および契約のステータスに関する包括的な詳細情報が表示されます。このレポートでは次のことができます。

- サービス契約範囲のギャップとこれに伴うネットワークのリスクを特定する。
- 今後の有効期限を確認する。
- 契約の詳細情報を確認する。
- 各契約に関連付けられているデバイスを確認する。

このレポートの目的

契約管理者はこのレポートを使用して、サポートの観点からネットワークを包括的に把握できます。これにより業務効率が向上し、リスク管理を強化できます。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ
- サービス契約期間の有効期限
- サービス契約へのアクセス

[期限切れの契約(Expiring Contracts)]

[期限切れの契約(Expiring Contracts)] レポートには、選択されているインベントリで、12 カ月以内にサービス契約期間が終了するデバイスがリストされます。このレポートでは次のことができます。

- サービス契約範囲のギャップとこれに伴うネットワークのリスクを特定する
- 今後の有効期限を確認する

- 契約の詳細情報を確認する
- 各契約に関連付けられているデバイスを確認する

このレポートの目的

契約管理者はこのレポートを使用して、サービス契約範囲の観点からネットワークを包括的に把握できます。これにより業務が効率化され、リスク管理が強化されます。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ
- サービス契約期間の有効期限
- サービス契約へのアクセス

[契約対象(Covered)]

[契約対象(Covered)] レポートには、選択されているインベントリで、1 つ以上の有効なシスコ サービス契約の対象であるデバイスがリストされます。このレポートを使用すると、次のことができます。

- デバイスと、デバイスに関連付けられている契約を確認する。
- デバイスのサポート終了日(LDoS)を確認する(公開されている場合)。
- 契約の詳細情報を確認する。

このレポートの目的

契約管理者はこのレポートを使用して、ネットワーク上のさまざまなデバイスに関連付けられている契約を確認できます。これにより業務が効率化され、リスク管理が強化されます。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ
- サービス契約期間の有効期限
- サービス契約へのアクセス

[契約対象外(Not Covered)]

[契約対象外(Not Covered)] レポートには、選択されているインベントリで、現在サービス契約対象外のデバイスがリストされます。

このレポートの目的

契約管理者はこのレポートを使用して、ネットワーク上でサービス契約対象にする必要があるデバイスを確認できます。これにより業務が効率化され、リスク管理が強化されます。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ
- サービス契約期間の有効期限
- サービス契約へのアクセス

[契約終了間近のデバイス(Expiring Device Coverages)]

[契約終了間近のデバイス(Expiring Device Coverages)] レポートでは、契約が間もなく終了するデバイスがリストされます。デフォルトでは、デバイスは契約終了日でソートされます。このレポートを使用すると、次のことができます。

- サービス契約が間もなく終了するデバイスのリストを取得する。
- 契約の詳細情報を確認する。

このレポートの目的

契約管理者はこのレポートにより、デバイスの契約をタイムリーに更新できます。これにより、業務効率が向上し、リスク管理を強化できます。

デバイスを機器タイプまたはサービス契約範囲ステータスでソートするには、次の手順に従います。

1. グラフ アイコンをクリックします。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ
- サービス契約期間の有効期限
- サービス契約へのアクセス

[複数契約(Contract Duplicates)]

[複数契約(Contract Duplicates)] レポートには、選択されているインベントリで、複数のサービス契約の対象となっているデバイスがリストされます。

デバイスを機器タイプまたはサービス契約範囲ステータスでソートするには、次の手順に従います。

1. グラフ アイコンをクリックします。

注:[契約番号(Contract No.)] の値が [その他(Other)] または [パートナーブランド契約(Partner Branded Contracts)] の場合、詳細にアクセスできる権限がありません。

ハウツー ビデオ

- 契約の詳細
- サービス契約範囲に関する情報へのアクセス
- サービス契約範囲のギャップ

- サービス契約期間の有効期限
- サービス契約へのアクセス

[インシデント(Incidents)]

Cisco Technical Assistance Center(TAC)とのインタラクション インスタンスは、[インシデント(Incidents)] レポートで確認できます。

[マイサポートケース:過去90日間(My Support Cases for Past 90 Days)]

[マイサポートケース(My Support Cases)] レポートには、選択されているインベントリと顧客についてユーザ(ログイン ユーザ)が過去 90 日間に Cisco TAC サポートに登録したサービス リクエストがリストされます。

このレポートの目的

このレポートでは、未解決のすべての TAC ケースを 1 つのレポートで確認できます。これによりネットワーク管理者とネットワーク技術者は、リスクをより効率的に管理できます。

[インベントリ(Inventory)]

このライブラリのレポートは、デバイスおよび設定の詳細(シリアル番号、PID、OS バージョン、搭載メモリとファームウェア、IP アドレス、ホスト名など)を含むシスコ インストール ベースの包括的な情報を提供します。これらのレポートでは、次のことができます。

- サポート終了または販売終了が近づいているシスコ製品を特定する。
- ネットワークで移動、追加、または変更された内容を確認する。
- シスコのハードウェアでサポートされている最新のソフトウェア バージョンが実行されていることを確認する。
- サポートが終了しているデバイスのアップグレードを計画する。

これらのレポートの目的

これらのレポートにより、ネットワーク管理者と技術者は、ネットワーク内のすべての機器の詳細情報と製品のサービス契約範囲ステータスを確認できます。これにより、管理者や技術者は業務効率を向上しリスク管理を強化できます。

ハウツー ビデオ

- インベントリの概要
- インベントリ デバイスの確認
- インベントリ収集デルタ

[要約(Summary)]

[要約(Summary)] レポートには、各種カテゴリ(サービス契約範囲、サポート終了日(LDoS)レコードなど)に基づいて、インベントリ内のシャーシ、モジュール、電源、ファン、およびその他のデバイスの総数が表示されます。

定義

- [インベントリのデバイス(すべてのソース)(Devices in Inventory (all sources))]:インベントリ システム内のすべての機器。
- [収集されたデバイス(Devices Collected)]:インベントリ システム内のコレクタ(CSPC など)から取得されたデバイス。
- [インポートされたデバイス(Devices Imported)]:CSV アップロードによりインベントリ システムに手動で入力されたデバイス。

- [認識されたデバイス(Devices Recognized)]:シリアル番号がシスコの製造データベース内に存在するためにインベントリ システムにより認識された機器。
- [サービス契約対象デバイス(Devices Covered)]:サービス契約対象であると認識されたデバイス。
- [サービス契約対象外デバイス(Devices Not Covered)]:サービス契約対象外であると認識されたデバイス。
- [LDoS 経過(Past LDoS)]:サポート終了日が経過しているデバイス。
- [LDoS が 12 ヵ月以内(LDoS within 12 Months)]:今後 12 ヵ月以内にサポート終了日に達するデバイス。
- [LDoS が 13 ヵ月～ 24 ヵ月以内(LDoS over 12 months and within 24 Months)]:今後 13 ～ 24 ヵ月以内にサポート最終日に達するデバイス。

機器の詳細を表示するには、次の手順に従います。

1. 該当するカテゴリと機器タイプの下の数値リンクをクリックします。

[すべての機器(All Equipment)]

[すべての機器(All Equipment)] レポートには、選択されているインベントリで特定の機器タイプ(シャーシ/カードなど)の機器がすべてリストされます。このレポートを使用すると、次のことができます。

- 収集またはファイルのインポートで検出されたデバイスの要約を確認する。

  注:[未分類(Not Categorized)] は列内のヌル値を指します。[その他(Others)] は、データの上位 16 % に入らないすべての値の組み合わせを指します。

- 指定されたデータからカスタム インベントリ レポートを作成する。

デバイスの詳細を表示するには、次の手順に従います。

1. [ホスト名(Hostname)] の下の該当するリンクをクリックします。

サポート ケースを作成するには、次の手順に従います。

1. サポート ケースを作成するデバイスの横にあるチェックボックスをクリックします。
2. [アクション(Actions)] > [サポートケースの作成(Create Support Cases)] をクリックします。

[複数インベントリ(Inventory Duplicates)]

[複数インベントリ(Inventory Duplicates)] レポートには、複数のインベントリに含まれているデバイスの詳細がリストされます。

デバイスの詳細を表示するには、次の手順に従います。

1. [ホスト名(Hostname)] の下の該当するリンクをクリックします。

[製品別インベントリ(Inventory by Product)]

[製品別インベントリ(Inventory by Product)] レポートには、インベントリ レポートが製品 ID に基づいてソート、グループ化されて表示されます。このレポートを使用すると、次のことができます。

- 導入されたデバイスを製品 ID でソートした要約を確認する。
- 製品 ID に基づいて、製品の数、製品のサービス契約範囲ステータスを特定する。
- デバイスのサポート終了日(LDoS)を確認する。LDoS は現行(システム)日付を経過している場合にのみ表示されます。

デバイスの詳細を表示するには、次の手順に従います。

1. [サービス契約対象(Covered)] と [サービス契約対象外(Not Covered)] の下の数値リンクをクリックします。

シスコにより指定されたアラート通知を表示するには、次の手順に従います。

1. [アラート定義URL(Alert Definition URL)] の下の該当する URL をクリックします。

[インベントリ収集デルタ(Inventory Collection Delta)]

[インベントリ収集デルタ(Inventory Collection Delta)] レポートでは、設定された期間内にネットワーク デバイスで行われた変更を確認します。この情報は、[アプリケーション設定(Application Settings)] でレポート設定を [包括的なビュー(Comprehensive view)] として設定している場合に便利です。このレポートを使用すると、次のことができます。

- 初回アップロード(Network Snapshot 1)から 2 回目のアップロード(Network Snapshot 2)までの間に追加、削除、または変更されたデバイスの数を確認する。
- 変更を機器タイプ別にさらに分類する。
- 選択されたデバイスの詳細を表示する。

注:このレポートを使用するには、1 つのインベントリを選択する必要があります。

レポート プロファイルは、各スナップショットのアップロード日時、各インベントリのアップロード元コレクタ、各インベントリでアップロードおよびインポートされたデバイスの合計数を示します。

変更されたデバイスの詳細を表示するには、次の手順に従います。

1. デバイスの合計数の番号付きリンクをクリックします。

ハウツー ビデオ

- インベントリ収集デルタ

[サイト別インベントリ(Inventory by Sites)]

[サイト別インベントリ(Inventory by Sites)] レポートには、インベントリ内のデバイスのインストール場所の詳細情報が表示されます。このレポートには、特定された各サイトの固有インストール先サイト ID、アドレス、および顧客が表示されます。

このレポートでは、各サイトでのシスコ サービス契約の対象デバイスと対象外デバイスの数を確認することができます。

[すべてのホスト(All Hosts)]

[すべてのホスト(All Hosts)] レポートには、インベントリのすべてのデバイスがリストされます。このレポートを使用すると、次のことができます。

- インベントリのすべてのシャーシを確認する。
- 独立したホスト名が設定されているシャーシまたはカードを確認する。
- デバイスのオペレーティング システムのタイプおよびバージョンを識別する。

注:マスター シャーシがスレーブ シャーシを参照することがあります。それぞれのシャーシには個別の ID が設定されています。

デバイスの詳細を表示するには、次の手順に従います。

1. [ホスト名(Hostname)] の下の該当するリンクをクリックします。

ホストのデバイス設定を表示するには、次の手順に従います。

1. [ホスト名（Hostname）] の下の該当するリンクをクリックします。詳細ページが開きます。
2. 設定の詳細を表示するには、[実行コンフィギュレーション（Running Configuration）] リンクまたは [スタートアップコンフィギュレーション（Startup Configuration）] リンクをクリックします。設定の詳細情報が新しいウィンドウに表示されます。

[カスタム インベントリ（Custom Inventory）]

[カスタム インベントリ（Custom Inventory）] レポートには、選択されているインベントリのすべての機器とその詳細がリストされます。このレポートには、契約情報と、インベントリ内のデバイスのサポート最終日（公開されている場合）も表示されます。

デバイスの詳細を表示するには、次の手順に従います。

1. [ホスト名（Hostname）] の下の該当するリンクをクリックします。

[インベントリ インサイト（Inventory Insight）]

[インベントリ インサイト（Inventory Insight）] ライブラリのレポートには、サービスにより識別されるデバイスに関する追加情報が表示されます。

これらのレポートの目的

これらのレポートは、ネットワーク管理者と技術者に対し、ネットワークの最新ビューを提供します。これにより、ビジネスの継続性を維持し、業務効率を向上させ、リスク管理を強化することができます。

[要約（Summary）]

[要約（Summary）] レポートには、選択されているインベントリのアップロード元コレクタに関する情報がリストされます。また、アプライアンス ID、最終アップロード時刻、およびコレクションの概要などの詳細情報が表示されます。

定義

- [管理対象デバイス リストの IP アドレス（IP addresses in the Managed Device List）]：管理対象デバイス リストのすべての IP アドレス。
- [収集されない IP アドレス（IP addresses Not Collected）]：管理対象デバイス リストで、コレクタがアクセスできなかったすべての IP アドレス。考えられる理由としては、クレデンシャルが正しくない、デバイスがオフラインである、またはデバイスが応答しないことなどがあります。
- [報告済み（Reported）]：[Smart Net Total Care インストールベース管理（Smart Net Total Care Installed Base Management）] レポートと [契約管理（Contract Management）] レポートに含まれているコレクション内の機器。
  - [シャーシ（Chassis）]：適切に識別、処理されたシャーシ。
  - [モジュール（Module）]：適切に識別、処理されたモジュール。
  - [電源装置（Power Supply）]：適切に識別、処理された電源装置。
  - [ファン（Fan）]：適切に識別、処理されたファン。
  - [その他（Other）]：適切に識別、処理されたその他のすべてのタイプの機器。
  - [現場交換不可（Not Field Replaceable）]：交換するにはシスコに送付する必要がある機器。 デバイスの詳細を表示するには、番号リンクをクリックします。

- [未認識(Not Recognized)]:シスコのレコードで見つからず、シスコの機器として認識されなかった機器。 デバイスの詳細を表示するには、番号リンクをクリックします。

- [未報告(Not Reported)]:いずれかのシスコ データベースで処理エラーまたはデータ不一致が発生したため、[Smart Net Total Care インストールベース管理(Smart Net Total Care Installed Base management)] レポートと [契約管理(Contract Management)] レポートに*表示されなかった*コレクション内の機器。推奨される対応策がある場合は、その対応策に従ってください。

- [サードパーティ(3rd Party)]:シスコ以外のサード パーティの機器。 デバイスの詳細を表示するには、番号リンクをクリックします。

- [重複(Duplicate)]:インベントリで重複する機器。 デバイスの詳細を表示するには、番号リンクをクリックします。

- [その他(Others):収集された情報に基づいて、現在の Smart Net Total Care ソフトウェア システムによって完全に分類できなかった機器。 デバイスの詳細を表示するには、番号リンクをクリックします。

[未収集(Not Collected)]

[未収集(Not Collected)] レポートには、管理対象デバイス リストに含まれているものの、コレクタに対して応答しないすべてのデバイスがリストされます。このレポートでは、処理されたが(シスコのデータと統合されたが)現在のコレクションに含まれていないシスコ デバイスを確認できます。このレポートには次の情報も含まれています。

- デバイスが収集されなかった理由。最も一般的な理由として、管理対象デバイス リストでクレデンシャルが正しくないことがあります。[管理対象デバイスリスト(Managed Device List)] でエラーがあるかどうかを確認します。

- 実行できる推奨アクション

ハウツー ビデオ

- 管理対象デバイス リストの更新

[サードパーティ(Third Party)]

[サードパーティ(Third Party)] レポートには、シスコ以外のデバイスとして特定されたすべての収集済みデバイスがリストされます。このレポートでは、サードパーティ デバイスがシスコのサポート情報と統合できなくても、サードパーティ デバイスを含めることでインストール ベースの全体像を把握できます。

[重複(Duplicates)]

[重複(Duplicates)] レポートには、収集データで複数回示されるデバイスがリストされます。このレポートでは、重複エントリの考えられる理由も示されます。

[未認識(Not Recognized)]

[未認識(Not Recognized)] レポートには、選択されているインベントリで、シスコ デバイスとして確認できなかったか、またはシステムがデバイス タイプを判別できなかったシスコ デバイスがリストされます。このレポートを使用すると、コレクションにより処理し、シスコ データと統合できる可能性があるシスコ デバイスを特定できます。

このレポートには、特定のデバイスが識別されなかった理由も示されます。

[現場交換不可(Not Field Replaceable)]

[現場交換不可(Not Field Replaceable)] レポートには、選択されているインベントリのデバイス内で、現場チームが交換または保守できないコンポーネントがリストされます。

現場交換できないデバイスはサービス契約の対象ではないため、このようなデバイスのスペア部品は調達できません。

[その他(Others)]

[その他(Others)] レポートには、データ分析の問題が原因で表示されるデバイスがリストされます。これらのデバイスは、他のインベントリ レポートには含まれません。このレポートでは、問題の考えられる理由も示されます。

このレポートを使用して、ポータルでシスコのサポート情報と統合できる可能性のあるデバイスを特定できます。

セキュリティ

Cisco Threat Awareness Service

Cisco Threat Awareness Service(CTAS)は、基本的な大量のセキュリティ情報を常時利用可能にすることで、脅威の可視化を向上させます。Smart Net Total Care ポータルの Threat Awareness サービスからアクセスできる TS と AS の共同イニシアチブにより、セキュリティが侵害されているシステムを迅速に特定できるようになります。このサービスは企業ネットワーク内外からのネットワークトラフィックを分析することで、悪意のある活動をタイムリーに検出するための実用的な情報を提供します。導入と使用が容易なこのサービスは、中小規模の顧客にとってコスト効果の高い理想的な脅威認識ソリューションです。詳細については、Cisco Threat Awareness Service の Web サイトをご覧ください。

ハウツー ビデオ

Cisco Threat Awareness Service

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool の使用法、サービス要求の送信方法、および追加情報の収集方法については、「*What's New in Cisco Product Documentation*(シスコ製品資料の更新情報)」(http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html)を参照してください。

「*What's New in Cisco Product Documentation*(シスコ製品資料の更新情報)」に配信登録すると、新しい(または改訂された)シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。

法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコによる TCP ヘッダー圧縮の実装には、カリフォルニア大学バークレー校(UCB)が UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発したプログラムを使用しています。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理されていないコピーです。最新バージョンについては、オンライン版の原本を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト(www.cisco.com/go/offices/ [英語])をご覧ください。

シスコの商標または登録商標

シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標を示します。シスコの商標の一覧は http://www.cisco.com/web/JP/trademark_statement.html に掲載されています。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

Cisco 著作権