ホワイト ペーパー

# Cisco Smart Net Total Care Service におけるセキュリティ

Cisco® Smart Net Total Care Service は、シスコ製品に対する基本的なテクニカル サービスやデバイス診断、アラートに加え、お客様のインストール ベースとサービス契約の広範な管理手段を提供します。Smart Net Total Care では、スマート サポート サービス機能を通じて、シスコのインストール ベースを特定し、その情報をシスコ データセンターへセキュアに送信します。これらの機器情報はシスコ データセンターにて、製造、契約、テクニカル サポート、セキュリティ情報などで構成されるシスコの膨大なナレッジ ベースと照合され、分析されます。

このサービスは、リスク マネジメントの改善、問題の迅速な解決、運用費の削減に貢献するプロアクティブなメンテナンス パッケージです。Smart Net Total Care サービスは、実用的なインテリジェンス、関連する推奨事項と情報、および予防的なサポート機能を提供することで運用コストを削減し、ダウンタイムを最小化します。

このドキュメントでは、インベントリ収集、シスコのデータセンターとの通信、アップロードされたデータの処理、および Smart Net Total Care ポータル上での報告機能を含む、Smart Net Total Care によって実装されるセキュリティ プロセスに関する情報を提供します。

# 目次

## Cisco Smart Net Total Care サービスの概要

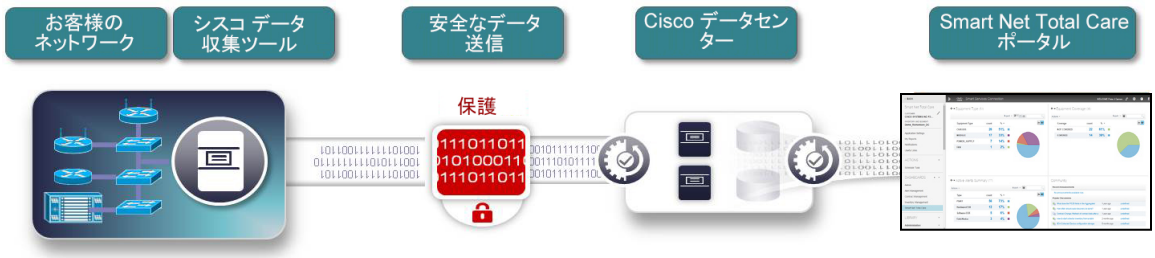
Cisco Smart Net Total Care は、広範なインストール ベースと契約管理機能を提供する、次世代型のスマート サポート サービスです。お客様のネットワークに接続されたシスコ製品よりセキュリティに配慮して取得された情報を使用し、それをシスコの専門知識と関連付けることにより、実用的なインテリジェンスとプロアクティブなサポート機能を提供します。これにより、リスク管理の改善とコスト削減が実現し、迅速な問題解決が可能になります。

Smart Net Total Care データ収集ツールでは、ネットワーク デバイス情報のためのデータ収集メカニズムを利用できます。ネットワークにインストールされたこのデータ収集ツールは、シスコのインストール ベース データを収集し、シスコのファイアウォール内にあるシスコ データセンターにアップロードします。この情報は、シスコの製造、契約、セキュリティ、およびアラートに関するデータの膨大なナレッジ ベースを使用して検証および分析されます。

情報は、Smart Net Total Care ポータルを通じてネットワーク管理者とユーザに送信されます。ポータル レポートでは、ネットワーク内で特定されたデバイスに関する詳細、テクニカル サービス契約範囲、ライフサイクル情報、およびセキュリティと製品のアラートを含む詳細な情報が提供されます。

## Smart Net Total Care のセキュリティ アーキテクチャ

Smart Net Total Care は、インストール ベース データに対してエンドツーエンドのセキュアなアーキテクチャを提供します。セキュリティ機能は、収集、送信、処理、保存、表示などあらゆる側面に対処します。




このドキュメントで紹介する重要なセキュリティ機能には、以下のものがあります。

- データ収集ツールとデータ収集の保護
- シスコのデータセンターへのセキュアな接続とデータ伝送
- シスコのデータセンターにおけるデータ保存
- ポータル データとオフライン レポートへのアクセスの制御

## データ収集ツールとデータ収集の保護

### データ収集ツールのセキュリティ

Smart Net Total Care では、カスタマー ネットワークに導入されたデータ収集ツールを使用して、シスコ デバイスを個別に識別し、製品 ID（PID）、シリアル番号、IOS リリースなど、デバイスの詳細を収集します。お客様は、Smart Net Total Care コレクション用にパッケージ化されたシスコ データ収集ツール ハードウェア アプライアンスを購入するか、お客様が構築した仮想環境に Smart Net Total Care ソフトウェア データ収集ツールを導入できます。シスコは、ハードウェア データ収集ツールとソフトウェア データ収集ツールを同じ手順と方法で保護します。ソフトウェア データ収集ツールについては、お客様は必要に応じて物理ホストのセキュリティを確認する必要があります。

Smart Net Total Care サービスでは、Linux オペレーティング システムの CentOS ディストリビューションが使用されます。またデータ収集ツールの設定の一環として、堅牢化手法が適用されます。堅牢化の手順には、たとえば以下のものが含まれます。

- すべてのアプリケーション コードは、業界標準の推奨事項にそって堅牢化されたオペレーティング システム イメージに組み込まれます。
- セキュアでない、または不要なアカウント、ポート、アプリケーション、サービスは有効化されません。
- ファイアウォールは、データ収集ツール用に調整されたデフォルトのルール セットを使用してインストールおよび設定されます。
- データ収集ツールのトラブルシューティングおよびモニタリングに使用する、データ収集ツール設定の監査とロギングが有効化されます。
- データ収集ツールへの特権（**root**）アクセスは、限定/堅牢化されたシェル環境での管理者による利用に制限されます。
- ユーザ認証はロール ベースのアクセスを通じて行われます。たとえば、一部のユーザにシステムの設定と管理が可能なアクセス権限を与え、他のユーザには表示操作だけが可能なアクセス権限を与えることができます。
- データ収集ツールの管理機能には、セキュアな通信のための業界標準の HTTPS を使用する Web UI を通じて、安全にアクセスできます。

### データ収集ツールのアクセス

データ収集ツールには、ローカル コンソールまたは有効化されたセキュア シェル（SSH）を通じてアクセス可能な管理シェルがあります。このコマンド ライン シェル インターフェイスを使用して、管理者は IP アドレスの割り当てなどの基本タスクのほか、オペレーティング システム関連のタスクを実行できます。ディスカバリ ジョブやデータ収集ジョブの作成と管理を行うユーザ インターフェイスは Web UI です。『Smart Net Total Care Collector Quick Start Guide（Smart Net Total Care Collector クイック スタート ガイド）』[英語] には、Web UI の URL にアクセスする方法が記載されています。セキュリティを確保するため、Web UI には HTTPS プロトコルを通じてアクセス可能です。

データ収集ツールのパスワード ポリシーでは、大文字、小文字、数字、または特殊文字を含む 9 文字以上のパスワードが必要です。わかりやすい英単語やそれに類似する言葉は使用しないでください。これに加えて、データ収集ツールにログインするために使用される非特権アカウントのパスワードと、特権パスワードの両方を、180 日ごとに変更することを推奨します。

### ソフトウェアのアップデート

ソフトウェア更新マネージャはシスコのデータセンターに置かれ、フル リリース、サービス パック更新、ルール パッケージ、データ プロファイルなど、更新可能な各種のデータ収集ツール ソフトウェアのリポジトリとして機能します。

収集プロセスに関連するソフトウェアのアップデートには、データ収集ツール ダッシュボードが使用されます。このダッシュボードには、お客様の管理者が更新を確認し、可能なダウンロードを行うための一連のコマンドが用意されています。セキュリティ上の問題や脆弱性がシスコによって検出されると、修正がリリースされた時点で、Smart Net Total Care サポート チームがリポジトリから更新を提供します。お客様は、オンデマンドと自動更新のどちらかを選択できます。シスコでは自動更新を推奨しています。ダッシュボードでは、完全なシステム イメージをインストールして、バックアップからデータ収集ツールを元の状態に復元することもできます。

データ収集ツールとソフトウェア更新マネージャ間のすべての通信は、128 ビット HTTPS セキュア チャネルで実行されます。ソフトウェア更新機能の詳細については、『Smart Net Total Care Collector Quick Start Guide（Smart Net Total Care Collector クイック スタート ガイド）』[英語] を参照してください。

### データ収集ツールのロギングおよびモニタリング

データ収集ツール上で発生したセキュリティに関わるすべてのイベントは、ローカルでログに記録されます。セルフモニタリングが使用され、ある時点のデータ収集ツールの状態を監視し、セキュリティに関わるイベントについて警告が行われます。このようなイベントには以下が含まれますが、これらに限定されるものではありません。

- 成功しなかったログインの試み
- セキュアな接続または暗号化処理のエラー
- ポリシー設定の変更
- ローカル データベースやファイル システムなど、データ収集ツールのサブシステムのステータス
- データ収集ツールのユーザ アカウントからのデータ アクセス
- シスコのデータセンターへの情報送信の成功

### 検出と収集

データ収集ツールは、デバイスの種類に基づいてさまざまな情報を収集します。シスコがデバイスを個別に識別するには、シリアル番号と PID が必要になります。デバイスの検出は複数の方法で制御できます。お客様は、Address Resolution Protocol（ARP）、Link Layer Discovery Protocol（LLDP）、Border Gateway Protocol（BGP）など、異なるプロトコルを選択して検出を行うことができます。シスコ OS のバージョン番号、ホスト名、IP アドレス、インストールされているメモリ、ファームウェアのバージョン番号など、さらに多くのデバイス情報が収集されることで、Smart Net Total Care ポータル レポートでより詳細な情報が提供されます。

データ収集ツールは Simple Network Management Protocol（SNMP）、コマンドライン インターフェイス（CLI）コマンド、Simple Object Access Protocol（SOAP）を使用してデバイスのクエリを行い、追加情報を取得します。Cisco IP Phone では、デバイスが登録されている Unified Communications Manager から MAC アドレスが取得されます。MAC アドレスは、シスコ データベース内の電話を識別するために使用されます。

デバイスを任意に収集対象から除外し、またシスコに転送されるネットワーク データの種類を制御できます。付録 A に、Smart Net Total Care のデフォルトのコマンドを示します。

有効なインベントリ収集を実行するには、デバイスの SNMP 読み取り専用（RO）クレデンシャルと基本的な TACACS アクセスが必要になります。この情報をデータ収集ツールに入力するかインポートすると、収集プロセスで使用されます。

収集機能は設定可能です。インストール ベースの収集で、SSH や Telnet など特定のプロトコルだけが使用されるようにポリシーを設定することができます。Smart Net Total Care のデータ収集はネットワークにかける負荷が非常に少なく、スレッド数の削減と収集トラフィックのスロットルが可能であるため、ネットワーク パフォーマンスが重要である場合に有効です。データ収集ツールの検出プロセスの詳細については、『CSPC OVERVIEW（CSPC の概要）』[英語] を参照してください。

### データ収集ツールのデータ ストレージ

インベントリとデバイス収集について収集されたすべての情報は、汎用のファイル システムではなく、データ収集ツールのローカルの Structured Query Language（SQL）データベース内に保存されます。収集されたデバイスのデータは暗号化されませんが、一連の強力な操作を行い、デバイス収集データのあらゆる部分を、データベースへの挿入前やシスコへのアップロードの前にマスクすることができます。

データベース内では、すべてのパスワードと SNMP コミュニティ ストリングが、256 ビットの AES で暗号化されます。データベース レコード、アプリケーション コード、バックアップのそれぞれに異なる AES キーが使用されます。デバイスのクレデンシャルがシスコに送信されることはありません。

データ収集ツールでは、直近 20 件の収集ジョブのデータを保存するように設定できます。デフォルトでは、5 つのデータ収集がアーカイブされるように設定されています。

### データ プライバシー機能

Smart Net Total Care では、データ プライバシー機能によってデータのセキュリティを強化できます。この機能により、IP アドレスとホスト名をプライベートに維持できます。データ収集ツールが収集したデータをシスコのデータセンターに送信する前に、データ内の IP アドレス フィールドとホスト名フィールドを別の値にマッピングすることができます。それにより、マッピングされた値のみがシスコのデータセンターに送信され、お客様のホスト名と IP アドレスがお客様のネットワーク外に漏れることがなくなります。ポータル内でレポートを確認する場合は、マッピングされた値を実際の値に変換する必要があります。ダウンロードしたレポートで使用できるように、スプレッドシート変換マクロが用意されています。データ プライバシー機能の詳細については、『Smart Net Total Care Enhanced Data Privacy Feature Application Note（Smart Net Total Care の強化されたデータ プライバシー機能のアプリケーション ノート）』[英語] を参照してください。

### お客様のネットワーク上でのデータ収集ツールとシスコ製品の通信

シスコのデータ収集ツールは、さまざまなプロトコルを使用して、サポート対象のシスコ デバイスからデータを収集します。

SNMP
シスコのデータ収集ツールは SNMP RO アクセスを使用して、ネットワーク内のデバイスのポーリングを行い、デバイスからインベントリの詳細を収集します。

データ収集ツールによって実行されるコマンド
データ収集ツールで実行可能なコマンドのリストは付録 A に記載されています。

SSH
シスコのデータ収集ツールは、ネットワーク デバイスに対して SSH ベースの CLI アクセス方式をサポートします。SSH は、データ収集ツールとネットワーク デバイス間のパスワードを含むすべてのトラフィックを暗号化することで、ネットワーク デバイスへのセキュアなリモート アクセスを実現します。データ収集ツールは SSH バージョン 1.5 と 2.0 の両方をサポートします。シスコは、安全性で劣る Telnet ベースのセッションよりも、この CLI アクセス方式を使用することを推奨します。

表 1. データ収集ツールでのポート用途

| ポート | 説明 | インバウンド | アウトバウンド |
|---|---|---|---|
| 22 TCP | SSH アクセス | 管理タスク用のデータ収集ツールへのシェル アクセス用 | デバイス上で CLI コマンドを実行するための SSH アクセス |
| 23 TCP | Telnet | | デバイス上で CLI コマンドを実行するための Telnet アクセス |
| 53 TCP/UDP | Domain Name Service（DNS） | | DNS サーバへのアウトバウンド接続 |
| 69 UDP | Trivial File Transfer Protocol（TFTP） | データ収集ツール TFTP サービス リスナー | デバイス上の TFTP サービスへの接続用 |
| 80 TCP | HTTP サービス | | Cisco Unified Communications Manager/IPPhone などのデバイス上の HTTP ポート アクセス、またはシスコの DMZ サービスで使用するデータ アップロードの接続用 |
| 161 UDP | SNMP ポート | | デバイス上の SNMP クエリ用 |
| 443 TCP | SSL 接続 | | データ アップロードの HTTPS 接続用 |
| 514 UDP | Syslog ポート | データ収集ツールの syslog サービスがデバイスからの syslog メッセージ受信に使用 | 外部 syslog サーバ向けのメッセージ送信用 |
| 1098 TCP/UDP | Java Remote Method Invocation（RMI）のアクティベーション | | Java RMI サービスへの初回接続確立用 |
| 1099 TCP/UDP | Java RMI ポート | | 外部の API サービスで使用する外部の Java RMI サービス接続用 |
| 3306 TCP/UDP | MySQL データベース ポート | | データ収集ツール ボックス外のデータベース サービスへの接続（設定されている場合） |
| 42605 TCP | データ収集ツールの GUI/XML ポート | データ収集ツールの GUI/XML API ポート<br>お客様のネットワーク内のリモート ボックスからデータ収集ツールの GUI クライアントを使用 | 接続用のデータ収集ツール GUI/XML API ポート |
| 8001/8443 TCP | データ収集ツール Web UI ポート | データ収集ツール Web UI アクセス用 | 接続用のデータ収集ツール Web UI ポート |
| ICMP/IP | ICMP Ping | | デバイスの検出とトラブルシューティング用 ICMP |

Telnet
シスコのデータ収集ツールは、Telnet を使用して、デバイスの設定、インベントリの追加情報、および重大なイベント後に発生する例外ベースのデータを収集します。データ収集ツールで、追加のインベントリ情報を収集するために必要なユーザ権限は、基本の TACACS ユーザ権限のみです。設定データを収集する必要がある場合は、特権モードでのアクセスが必要となります。シスコでは TACACS+ サーバの

使用を推奨しています。このサーバには、ネットワーク デバイスへのアクセスを認証するためのユーザ名とパスワードが保存されます。このタイプのアクセスを使用すると、お客様は TACACS+ サーバを適切に設定することで、データ収集ツールがデバイス上で実行できるコマンドのタイプを制限できます。CLI への推奨される認証方法は、TACACS サーバを使用して、すべての必要な *show* コマンドを許可しておくことです。

Internet Control Message Protocol（ICMP）
データ収集ツールは、シスコ デバイスの検出手法として、また、デバイスとネットワークの可用性を監視する方法として、ICMP ping メッセージを使用します。

## シスコのデータセンターへのセキュアな接続とデータ伝送

### データ転送におけるセキュリティ

データ転送のための接続は、常にデータ収集ツール側からシスコのデータセンター内にあるシスコのアップロード サーバに向けて開始されます。シスコのアップロード サーバ側から、お客様のネットワーク内のデータ収集ツールへの接続を確立することはありません。データ収集ツールは、外部ソースからの着信接続を受け入れません。すべてのデータ収集ツールをお客様のネットワーク内の既存のファイアウォールの背後に配置して、このポリシーをさらに強化することを推奨します。

SNMP ストリングや符号化されたイネーブル パスワードのような機密性の高いデバイス パスワードおよびクレデンシャルは、関連するデバイス設定ではマスキングされます。そのため、転送中に見られることはありません。管理者は、アップロードされるデータ ファイルから特定のデバイスまたはデータ文字列を除外するよう転送前に指定することもできます。

Smart Net Total Care のアップロード ファイルは暗号化され、パブリック インターネットを通じてシスコ データセンターに転送されます。転送データは、Public Key Infrastructure（PKI）ベースの 128 ビットの AES キーを使用してアプリケーション層レベルで暗号化されます。このキーはアップロードごとに生成されます。エンドポイント側からファイルの転送を行う場合には、HTTPS over SSL 接続が確立されます。この SSL ハンドシェイクの実行時に、クライアントの証明書を使用して認証が行われます。HTTPS over SSL では、2048 ビットの PKI ベース システムを使用して、トランスポート層でデータが暗号化されます。この暗号化は、データ収集ツール ソフトウェアによってアプリケーション層で行われる AES-128 暗号化に加えて実行されます。

データの暗号化には以下の特徴があります。

- データ アップロードごとに、128 ビットの AES キーが動的に生成され、転送データの暗号化に使用されます。
- AES キー自体もシスコが生成する公開キーで暗号化されます。
- さらに、インストールされる各データ収集ツールには、すべてのデータ収集ツールに共通の事前生成された公開キーと秘密キーのペアが付属します。
- 暗号化されたデータと暗号化された 128 ビットの AES キーは、インストール時に事前生成された秘密キーを使用して署名され、デジタル署名を形成します。

お客様はファイル インポート機能により、デバイスの追加情報が含まれた .csv ファイルをシスコ データセンターに安全にアップロードし、収集されたデータを拡張できます。ファイル インポート情報をアップロードできるのは、お客様の管理者だけです。ファイルは上記のように HTTPS over SSL 接続を使用して転送され、データは収集されたデータと同じ安全な方法で送信され保存されます。

### データ認証

シスコのアップロード サーバのパスワードベースの認証に加えて、各データ収集ツールには、一意のランダムに生成されたデジタル証明書が割り当てられます。このデジタル証明書はシスコのデータセンターに登録され安全に保管されます。そして受信したデータの正当性を検証するために使用されます。未登録または存在しない証明書を伴うクライアントからのデータは、検出次第永久に削除され、その後、復号化や転送が行われることはありません。

### キーの構成

HTTPS セッション キーの暗号化に使用する公開キー/秘密キーのキー長は 2048 ビットです。アプリケーション層では AES-128 暗号化が使用されます。Transport Layer Security（TLS）セッション キーの長さは 56 ビットで、ストリーム モードで使用されます。前のセクションで説明したように、データはこれらの異なる 3 種類のキーで 3 回暗号化されます。

### キーの管理

アプリケーション層での暗号化で使用する PKI キー交換は、アップロードの際に動的に行われます。信頼されたサードパーティの外部サーバは、アプリケーション層での暗号化に使用する公開キーと、SSL セッションのセットアップで使用する公開キーの両方の最新のコピーを保管します。データ収集ツールはすべての TLS プロトコルをサポートします。対称キーの交換は PKI 暗号化を使用して、セッション指定の時間行われます。

### アップロードの完全性

メッセージ ダイジェスト 5（MD5）チェックサムは、アップロード データから計算され、クライアントの秘密キーを使用して最終パッケージ内で暗号化されます。ファイルの MD5 値は標準的なチェックサムと同様の 128 ビット値です。値の長さが追加されたことで、別のファイルや破損したファイルが、対象とするファイルと同じ MD5 値を持つ可能性が大幅に低下します。暗号化された送信前のデータから算出された MD5 値と、シスコ データセンターが受信したデータの MD5 値を比較して、正当性を検証します。

### データ アップロード サーバ

シスコは、セキュアな DMZ 内にホストを設置して、アップロードされた暗号化ファイルを受信しています。これらのホストは、お客様の情報の復号化に必要なキーを保持しておらず、データ ファイルの整合性の検証後、シスコのファイアウォール内の最終的な宛先に向けてデータの転送を行う役割のみを担っています。

## シスコのデータセンターにおけるデータ ストレージ

### データ ストレージ

シスコは、自社で保存するデータのプライバシー保護と機密保持を確約しています。お客様のデータを保護するために、次の措置を講じています。

- お客様のデータを処理する Smart Net Total Care 環境は、シスコのファイアウォール内の、ネットワークのセキュアなスイッチ セグメント上にあります。
- すべてのシスコ IT マシンのインストール プロセスは、マシンを保護するための堅牢化スクリプトの適用を含む厳格なセキュリティ標準に準拠しています。
- マシンは施錠された施設で管理され、施設の利用はシスコ IT 管理者のみに制限されます。

- 企業ネットワークと、バックエンド データが保存された制限付きネットワーク全体にわたって、シスコの侵入検知システムが導入されています。
- アップロードされたネットワーク情報の復元および復号化は、シスコ ファイアウォール内にあるシスコ実稼動マシン上でのみ実行されます。

データは、シスコのファイアウォール内で、厳密な認証とアクセス コントロールによって保護されます。データベースは、Oracle アプリケーション スキーマの許可と権限、および堅牢な監査ログ設定によってネイティブに実装されたロールベースのセキュリティ モデルを使用して保護されます。データへのアプリケーション レベルのアクセスは、業界で広く受け入れられているシングル サインオン メカニズムを使用して保護されます。

データセンターのデータへのアクセスはすべて、CA SiteMinder® ベースの認証を介して行われます。コミュニティ ストリングやパスワードなどの機密情報は、保存前に削除されます。データはシスコの企業 IT のベスト プラクティスと、データ保護および保持ポリシーに従って保存されます。

### ストレージ ポリシー

アップロードされた生データは、シスコの企業保持ポリシーに従ってアーカイブされます。この生データは変換、処理され、データセンターのデータベースに保存されます。そこからポータル レポートが生成されます。データの処理および分析が完了すると、ポータルで表示可能になります。処理されたデータは少なくとも 5 年間アーカイブされます。

処理されたデータはポータルに表示され、次のデータ セットがアップロードされ処理された時点で、それまでのデータ セットが最新のデータで上書きされます。アップロードされたデータを削除して、ポータル レポートまたはオフライン レポートで使用できないようにするには、削除する情報が含まれていない新しいデータ セットをアップロードします。以前処理されたデータはアーカイブされ、デルタ レポートで最大 2 年間使用できます。

### バックアップと復元

インストール ベースのデータは、シスコ データセンターに保管されます。シスコは毎日データのバックアップを行います。情報は暗号化されてローカルに保存されます。

### システムのセキュリティを確認し監査するシスコのプロセス

シスコはメジャー リリースと定期的な脆弱性テストで静的分析の組み合わせを使用し、製品とサービスに対して、セキュリティ リスク分析、セキュリティ標準準拠のテスト、および脆弱性スキャンが実施されるようにします。これらのプロセスで検出された問題については、標準の Cisco Defect and Enhancements Tracking System（CDETS）によってレポートされ、是正措置が実施されます。

## ポータル データとオフライン レポートへのアクセスの制御

### Smart Net Total Care ポータルのセキュリティ

Smart Net Total Care ポータルでは、お客様のネットワーク インベントリと契約情報について処理された情報を確認できます。ポータルでレポートを表示する場合には、お客様の企業データが他の企業のデータから論理的に分離されます。ポータルには、次のセキュリティ メカニズムが適用されます。

- ユーザの対象企業に関連付けられた一意の認定 Cisco.com ID およびパスワード
- お客様による Smart Net Total Care ポータルへのユーザ アクセスの管理
- SSL v3 で認証されたサーバ

- 期限が設定された安全なセッション管理
- 階層型のロールベース アクセス コントロール
- 失敗したログインや無効なリソース アクセス試行など、イベントのロギングとモニタリング

Smart Net Total Care ポータルへのアクセスは、お客様が指定したお客様側の管理者が制御します。管理者は新規ユーザを登録できるほか、ユーザが退社した場合や職務が変更された場合などには、既存のユーザ登録をキャンセルできます。ユーザを登録または削除するプロセスについては、『Smart Net Total Care How-To videos（Smart Net Total Care のハウツー ビデオ）』[英語] に記載されています。

### 契約データ レポートのプライバシー

契約に関連付けられているアドレスがお客様のマスター データ レコード内のアドレスに対して検証できない場合には、Smart Net Total Care のビジネス ロジックによって、お客様の機密データが保護されます。サイト情報の検証済み一致には、さまざまなトランザクションが影響する可能性があります。最も考えられるのは、契約上のアドレスがシスコの正式な顧客レコードに追加されていない場合です。この場合サイト情報は非表示になり、お客様の正式な企業マスター データ カスタマー レコードにサイトが追加されるまでは、「サイトの検証が必要」に分類されます。

## まとめ

Smart Net Total Care サービスは、インストール ベース情報を収集して処理し、シスコ データセンターと Smart Net Total Care ポータルに送信できる、セキュアなエンドツーエンドのアーキテクチャを実現します。そこでは、シスコ デバイスおよびサービス契約に関する実用的な情報が得られる、包括的なレポートにアクセスできます。

シスコは、お客様のデータのセキュリティを非常に重視しています。Smart Net Total Care の詳細、およびシスコによるセキュリティ アーキテクチャの実装方法については、シスコの営業担当者またはシスコ認定パートナーまでお問い合わせください。担当者が技術会議を実施して、お客様の質問について話し合い、お客様の状況について具体的に説明します。

## 関連リソース

シスコがお客様データのプライバシーをどのように保護しているか、詳細については次を参照してください。その他のセキュリティの詳細は、機密保持契約で利用できます。

Cisco Security Vulnerability Policy（シスコのセキュリティ脆弱性ポリシー）[英語]:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

シスコのプライバシー ポータル[英語]:
http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/index.html#~1

Smart Net Total Care How-To Videos（Smart Net Total Care のハウツー ビデオ）[英語]:
http://www.cisco.com/E-Learning/bulk/subscribed/SNTC_3-x/index.htm

Smart Net Total Care Collector Quick Start（Smart Net Total Care データ収集ツール クイック スタート ガイド）[英語]:
http://www.cisco.com/en/US/docs/net_mgmt/inventory_and_reporting/CSPC_Quick_Start_Guide_for_SNTC.pdf

Smart Net Total Care Enhanced Data Privacy Feature Application Note（Smart Net Total Care の強化されたデータ プライバシー機能のアプリケーション ノート）[英語]:
https://supportforums.cisco.com/docs/DOC-39968

Common Services Platform Collector (CSPC) Overview（Common Services Platform Collector（CSPC）の概要）[英語]:
https://supportforums.cisco.com/docs/DOC-40159

## 付録 A:データ収集ツールのコマンド実行の参照情報

表 2 に、Telnet または SSH を通じて収集できるデフォルトの CLI コマンドを示します。

表 3 は、SNMP を通じて収集できるデフォルトの SNMP MIB を示しています。

表 2:SNTC のデフォルトの CLI コマンド

| |
|---|
| show ap summary |
| show c7200 |
| show diag |
| show gsr chassis-info |
| show hardware |
| show idprom all |
| show inventory |
| show module |
| show rsp chassis-info |
| show running-config |
| show startup-config |
| show version |

以下に示すデフォルトのコマンドは、クラスタ コマンド スイッチの rcommand によって、クラスタ メンバー スイッチで実行されます。

| |
|---|
| cluster rcommand > show cluster |
| cluster rcommand > show env power |
| cluster rcommand > show flash |
| cluster rcommand > show interface |
| cluster rcommand > show inventory |
| cluster rcommand > show running-config |
| cluster rcommand > show startup-config |
| cluster rcommand > show switch |
| cluster rcommand > show version |

表 3:SNTC のデフォルトの SNMP MIB

| MIB | MIB テーブル名 |
|---|---|
| AIRESPACE-SWITCHING-MIB | agentInventoryGroup |
| AIRESPACE-WIRELESS-MIB | bsnAPTable |
| AIRESPACE-WIRELESS-MIB | bsnMobileStationTable |
| ALTIGA-HARDWARE-STATS | alStatsHardwareGlobal |
| ALTIGA-VERSION-STATS | alStatsVersionGlobal |
| ARROWPOINT-CHASSISMGREXT-MIB | apChassisMgrExtModuleTable |
| ARROWPOINT-CHASSISMGREXT-MIB | chassisMgrExt |
| BASIS-GENERIC-MIB | cardInformation |
| BASIS-SHELF-MIB | shelfTable |
| CALISTA-DPA-MIB | dpa |
| CISCO-CCM-MIB | ccmGatewayTable |
| CISCO-CCM-MIB | ccmGlobalInfo |
| CISCO-CCM-MIB | ccmGroupTable |
| CISCO-CCM-MIB | ccmPhoneExtnTable |
| CISCO-CCM-MIB | ccmPhoneTable |
| CISCO-CCM-MIB | ccmProductTypeTable |
| CISCO-CCM-MIB | ccmRegionTable |
| CISCO-CCM-MIB | ccmTable |
| CISCO-CCME-MIB | ccmeConfig |
| CISCO-CCME-MIB | ccmeEphoneActTable |
| CISCO-CCME-MIB | ccmeEphoneConfTable |
| CISCO-CDP-MIB | cdpCacheTable |
| CISCO-CLUSTER-MIB | ccCandidateTable |
| CISCO-CLUSTER-MIB | ccMemberTable |
| CISCO-ENHANCED-MEMPOOL-MIB | cempMemPoolTable |
| CISCO-ENTITY-ASSET-MIB | ceAssetTable |
| CISCO-ENTITY-FRU-CONTROL-MIB | cefcModuleTable |
| CISCO-FLASH-MIB | ciscoFlashDeviceTable |
| CISCO-FLASH-MIB | ciscoFlashFileTable |
| CISCO-FLASH-MIB | ciscoFlashPartitionTable |
| CISCO-IMAGE-MIB | ciscoImageTable |
| CISCO-MEMORY-POOL-MIB | ciscoMemoryPoolTable |
| CISCO-PROCESS-MIB | cpmCPUTotalTable |
| CISCO-PROCESS-MIB | cpmProcessExtTable |
| CISCO-PROCESS-MIB | cpmProcessTable |
| CISCO-RHINO-MIB | ciscoLS1010ChassisGroup |
| CISCO-RHINO-MIB | ciscoLS1010ModuleTable |

| MIB | MIB テーブル名 |
|---|---|
| CISCO-RHINO-MIB | ciscoLS1010SubModuleTable |
| CISCO-STACK-MIB | chassisGrp |
| CISCO-STACK-MIB | moduleTable |
| CISCO-STACK-MIB | systemGrp |
| CISCO-STACKWISE-MIB | cswGlobals |
| CISCO-STACKWISE-MIB | cswSwitchInfoTable |
| CISCO-TELEPRESENCE-CALL-MIB | ctpcInfoObjects |
| CISCO-TELEPRESENCE-CALL-MIB | ctpcStatObjects |
| CISCO-TELEPRESENCE-CALL-MIB | ctpcTable |
| CISCO-TELEPRESENCE-MIB | ctpPeripheralStatusTable |
| CISCO-UNIFIED-COMPUTING-ADAPTOR-MIB | cucsAdaptorUnitTable |
| CISCO-UNIFIED-COMPUTING-COMPUTE-MIB | cucsComputeBladeTable |
| CISCO-UNIFIED-COMPUTING-COMPUTE-MIB | cucsComputeBoardTable |
| CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB | cucsEquipmentFanTable |
| CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB | cucsEquipmentIOCardTable |
| CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB | cucsEquipmentPsuTable |
| CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB | cucsEquipmentSwitchCardTable |
| CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB | cucsEquipmentXcvrTable |
| CISCO-UNIFIED-COMPUTING-FABRIC-MIB | cucsFabricSwChPhEpTable |
| CISCO-UNIFIED-COMPUTING-FIRMWARE-MIB | cucsFirmwareBootUnitTable |
| CISCO-UNIFIED-COMPUTING-MEMORY-MIB | cucsMemoryUnitTable |
| CISCO-UNIFIED-COMPUTING-NETWORK-MIB | cucsNetworkElementTable |
| CISCO-UNIFIED-COMPUTING-PROCESSOR-MIB | cucsProcessorUnitTable |
| CISCO-UNIFIED-COMPUTING-STORAGE-MIB | cucsStorageLocalDiskTable |
| CISCO-UNIFIED-COMPUTING-VM-MIB | cucsVmInstanceTable |
| CISCO-VDC-MIB | ciscoVdcTable |
| CISCO-VIRTUAL-SWITCH-MIB | cvsChassisTable |
| CISCO-VIRTUAL-SWITCH-MIB | cvsCoreSwitchConfigTable |
| CISCO-VIRTUAL-SWITCH-MIB | cvsGlobalObjects |
| CPQHOST-MIB | cpqHoCpuUtilTable |
| CPQHOST-MIB | cpqHoInfo |
| CPQSINFO-MIB | cpqSiAsset |
| CPQSTDEQ-MIB | cpqSeCpuTable |
| ENTITY-MIB | entPhysicalTable |
| FCMGMT-MIB | connUnitTable |
| HOST-RESOURCES-MIB | hrDeviceTable |
| HOST-RESOURCES-MIB | hrDiskStorageTable |
| HOST-RESOURCES-MIB | hrStorage |

| MIB | MIB テーブル名 |
| --- | --- |
| HOST-RESOURCES-MIB | hrStorageTable |
| HOST-RESOURCES-MIB | hrSWInstalledTable |
| IF-MIB | ifTable |
| IF-MIB | ifXTable |
| IP-MIB | ipAddrTable |
| MSSQLSERVER-MIB | mssqlSrvTable |
| OLD-CISCO-CHASSIS-MIB | cardTable |
| OLD-CISCO-CHASSIS-MIB | chassis |
| OLD-CISCO-SYS-MIB | lsystem |
| PCUBE-SE-MIB | pmoduleTable |
| PCUBE-SE-MIB | pportTable |
| RADVISION-MIB | rvUnitGeneral |
| SNMPv2-MIB | system |
| STARENT-MIB | starentChassis |
| STARENT-MIB | starFanTable |
| STARENT-MIB | starPowerTable |
| STARENT-MIB | starSlotTable |
| STRATACOM-MIB | shelfSlotInfoTable |
| SYSAPPL-MIB | sysApplInstallElmtTable |
| SYSAPPL-MIB | sysApplInstallPkgTable |
| SYSAPPL-MIB | sysApplRunTable |
| TOPSPIN-MIB | tsDevBackplane |
| TOPSPIN-MIB | tsDevCardTable |
| TOPSPIN-MIB | tsDevFanTable |
| TOPSPIN-MIB | tsDevPowerSupplyTable |
| UMSASSETID-MIB | iBMPSGSerialNumberInformationTable |

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-720918-11JA 15.08