
# セキュリティ

この章では、Cisco ONS 15454 のユーザおよびセキュリティについて説明します。セキュリティのプロビジョニング方法については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

次の内容について説明します。

# 9.1　ユーザ ID およびセキュリティ レベル

ONS 15454 には、ノードへの初回ログイン用として CISCO15 ユーザ ID が設定されていますが、Cisco Transport Controller（CTC）の起動時のプロンプトには、このユーザ ID は表示されません。この ID は、他の ONS 15454 ユーザ ID を設定するために使用します。

ONS 15454 には、最大 500 のユーザ ID を設定できます。CTC ユーザまたは Transaction Language One（TL1）ユーザには、次のいずれかのセキュリティ レベルを割り当てることができます。

- Retrieve — CTC 情報を取得して表示できますが、パラメータの設定または修正はできません。
- Maintenance — ユーザは、ONS 15454 メンテナンス オプションにのみアクセスできます。
- Provisioning — ユーザは、プロビジョニングおよびメンテナンス オプションにアクセスできます。
- Superuser — 他のユーザの名前、パスワード、セキュリティ レベルの設定のほか、セキュリティ レベルのすべての機能を実行できます。

各セキュリティ レベルのユーザ タイムアウト情報については、表 9-3 を参照してください。

デフォルトでは、ノード上で複数のユーザ ID セッションを同時に実行できます。つまり、複数のユーザが、同じユーザ ID を使用してノードにログインできます。ただし、1 つのユーザ ID に対して単一ログインだけが許可されるようにノードをプロビジョニングすれば、全ユーザの同時ログインを防ぐことができます。

# 9.2　ユーザの権限およびポリシー

ここでは、CTC の各操作におけるユーザの権限、および Superuser がプロビジョニングに使用できるセキュリティ ポリシーについて説明します。

## 9.2.1　CTC 操作におけるユーザの権限

表 9-1 に、ノード ビューで各権限レベルのユーザが実行できる操作を示します。

**表 9-1　ONS 15454 のセキュリティ レベル ― ノード ビュー**

| CTC タブ | サブタブ | [サブタブ]：操作 | Retrieve | Maintenance | Provisioning | Superuser |
|---|---|---|---|---|---|---|
| Alarms | — | 同期化、フィルタ、クリアしたアラームの削除 | X | X | X | X |
| Conditions | — | 取得、フィルタ | X | X | X | X |
| History | Session | Filter | X | X | X | X |
| | Shelf | 取得、フィルタ | X | X | X | X |
| Circuits | Circuits | 作成、削除 | — | — | X | X |
| | | 編集、フィルタ、検索 | X | X | X | X |
| | Rolls | 完了、Force Valid Signal、終了 | — | — | X | X |
| Provisioning | General | 全般：編集 | — | — | 一部[1] | X |
| | | Multishelf Config: 編集 | X | X | X | X |
| | | 電源モニタ：編集 | — | — | X | X |
| | EtherBridge | スパニング ツリー：編集 | — | — | X | X |
| | Network | 全般：編集 | — | — | — | X |
| | | 全般：表示 | X | X | X | X |
| | | スタティック ルーティング：作成、編集、削除 | — | — | X | X |
| | | OSPF：作成、編集、削除 | — | — | X | X |
| | | RIP：作成、編集、削除 | — | — | X | X |
| | | プロキシ：作成、編集、削除 | — | — | — | X |
| | | ファイアウォール：作成、編集、削除 | — | — | — | X |
| | OSI | メイン セットアップ編集 | — | — | — | X |
| | | TARPConfig：編集 | — | — | — | X |
| | | TARP スタティック TDC：追加、編集、削除 | — | — | X | X |
| | | TARPMAT：追加、編集、削除 | — | — | X | X |
| | | ルータ：セットアップ：編集 | — | — | — | X |
| | | ルータ：サブネット：編集 / イネーブル / ディセーブル | — | — | X | X |
| | | トンネル：作成、編集、削除 | — | — | X | X |
| | BLSR | 作成、編集、削除、アップグレード | — | — | X | X |
| | | リング マップ、スケルチ テーブル、RIP テーブル | X | X | X | X |

表 9-1　ONS 15454 のセキュリティ レベル — ノード ビュー（続き）

| CTC タブ | サブタブ | [サブタブ]：操作 | Retrieve | Maintenance | Provisioning | Superuser |
|---|---|---|---|---|---|---|
| | Protection | 作成、編集、削除 | — | — | X | X |
| | Security | ユーザ：作成、削除、セキュリティ侵入アラームのクリア | — | — | — | X |
| | | ユーザ：編集 | 同じユーザ | 同じユーザ | 同じユーザ | すべてのユーザ |
| | | アクティブ ログイン：表示、ログアウト、最後のアクティビティ タイムの取得 | — | — | — | X |
| | | ポリシー：編集 / 表示 | — | — | — | X |
| | | アクセス：編集 / 表示 | — | — | — | X |
| | | RADIUS サーバ：作成、編集、削除、上昇、下降、表示 | — | — | — | X |
| | | 免責条項：編集 | — | — | — | X |
| | SNMP | 作成、編集、削除 | — | — | X | X |
| | | トラップ先の閲覧 | X | X | X | X |
| | Comm Channels | SDCC：作成、編集、削除 | — | — | X | X |
| | | LDCC：作成、編集、削除 | — | — | X | X |
| | | GCC：作成、編集、削除 | — | — | X | X |
| | | OSC：OSC 終端：作成、編集、削除 | — | — | X | X |
| | | OSC：DWDM リンク ID：作成、編集、削除 | — | — | — | X |
| | | PPC：作成、編集、削除 | — | — | X | X |
| | Timing | 全般：編集 | — | — | X | X |
| | | BITS ファシリティ：編集 | — | — | X | X |
| | アラーム プロファイル | アラーム動作編集 | — | — | X | X |
| | | アラーム プロファイル エディタ：保存、削除[2] | — | — | X | X |
| | | アラーム プロファイル エディタ：新規、ロード、比較、使用可能、使用状況 | X | X | X | X |
| | Cross-Connect | 編集 | — | — | X | X |
| | Defaults | 編集、インポート | — | — | — | X |
| | | リセット、エクスポート | X | X | X | X |
| | WDM-ANS | プロビジョニング：編集 | — | — | — | X |
| | | プロビジョニング：リセット | X | X | X | X |
| | | 内部パッチコード：作成、編集、削除、コミット、デフォルト パッチコード | — | — | X | X |
| | | ポート ステータス：起動 ANS | — | — | — | X |
| | | ノード セットアップ | X | X | X | X |
| Inventory | — | 削除 | — | — | X | X |
| | | リセット | — | X | X | X |

**表 9-1　ONS 15454 のセキュリティ レベル — ノード ビュー（続き）**

| CTC タブ | サブタブ | [サブタブ]：操作 | Retrieve | Maintenance | Provisioning | Superuser |
|---|---|---|---|---|---|---|
| Maintenance | Database | バックアップ | — | X | X | X |
| | | 復元 | — | — | — | X |
| | EtherBridge | スパニング ツリー | X | X | X | X |
| | | MAC テーブル：Retrieve | X | X | X | X |
| | | MAC テーブル : クリア、すべてクリア | — | X | X | X |
| | | トランク利用率：リフレッシュ | X | X | X | X |
| | | 回線：リフレッシュ | X | X | X | X |
| | Network | ルーティング テーブル取得 | X | X | X | X |
| | | RIP Routing Table：取得 | X | X | X | X |
| | OSI | IS-IS RIB：リフレッシュ | X | X | X | X |
| | | ES-IS RIB：リフレッシュ | X | X | X | X |
| | | TDC : NSAP に対する TID、フラッシュ ダイナミック エントリ | — | X | X | X |
| | | TDC：リフレッシュ | X | X | X | X |
| | BLSR | 編集、リセット | — | X | X | X |
| | Protection | 切り替え、ロックアウト、ロックオン、クリア、ロック解除 | — | X | X | X |
| | Software | ダウンロード | — | X | X | X |
| | | 有効化、復元 | — | — | — | X |
| | Cross-Connect | カード : 切り替え、ロック、ロック解除 | — | X | X | X |
| | | リソース使用状況：削除 | — | — | X | X |
| | Overhead XConnect | 表示 | X | X | X | X |
| | Diagnostic | テクニカル サポート ログの取得 | — | — | X | X |
| | | ランプ テスト | — | X | X | X |
| | Timing | 送信元：編集 | — | X | X | X |
| | | レポート : ビュー、リフレッシュ | X | X | X | X |
| | Audit | 取得 | — | — | — | X |
| | | アーカイブ | — | — | X | X |
| | Test Access | 表示 | X | X | X | X |
| | DWDM | APC：実行、無効化、リフレッシュ | — | X | X | X |
| | | WDM スパン チェック：編集、スパン損失値の取得、リセット | X | X | X | X |
| | | ROADM 電源モニタリング：リフレッシュ | X | X | X | X |

1. Provisioning ユーザは、STS-1 Signal Degrade（SD; 信号劣化）パラメータのノード名、連絡先、または AIS-V 挿入は変更できません。
2. サブタブのボタンは全ユーザに有効ですが、動作が完全に実行できるのは、必要なセキュリティ レベルを所有するユーザだけです。

表 9-2 に、ネットワーク ビューで各権限レベルのユーザが実行できる操作を示します。

**表 9-2　ONS 15454 セキュリティ レベル ― ネットワーク ビュー**

| CTC タブ | サブタブ | [サブタブ]：操作 | 取得 | Maintenance | Provisioning | Superuser |
|---|---|---|---|---|---|---|
| Alarms | — | 同期化、フィルタ、クリアしたアラームの削除 | X | X | X | X |
| Conditions | — | 取得、フィルタ | X | X | X | X |
| History | — | Filter | X | X | X | X |
| Circuits | Circuits | 作成、編集、削除 | — | — | X | X |
| | | フィルタ、検索 | X | X | X | X |
| | Rolls | 完了、Force Valid Signal、終了 | — | — | X | X |
| Provisioning | Security | ユーザ：作成、削除 | — | — | — | X |
| | | ユーザ：編集 | 同じユーザ | 同じユーザ | 同じユーザ | すべてのユーザ |
| | | アクティブ ログイン：ログアウト、最後のアクティビティ タイムの取得 | — | — | — | X |
| | | ポリシー：変更 | — | — | — | X |
| | アラーム プロファイル | 保存、削除[1] | — | — | X | X |
| | | 新規、ロード、比較、使用可能、使用状況 | X | X | X | X |
| | BLSR | 作成、削除、編集、アップグレード | — | — | X | X |
| | Overhead Circuits | 作成、削除、編集、マージ | — | — | X | X |
| | | 検索 | X | X | X | X |
| | Provisionable Patchcords（PPC） | 作成、編集、削除 | — | — | X | X |
| | サーバ トレール | 作成、編集、削除 | — | — | X | X |
| Maintenance | Software | ダウンロード、取り消し | — | X | X | X |
| | Diagnostic | OSPF ノード情報取得、クリア | X | X | X | X |

1. サブタブのボタンは全ユーザに有効ですが、動作が完全に実行できるのは、必要なセキュリティ レベルを所有するユーザだけです。

## 9.2.2　セキュリティ ポリシー

Superuser セキュリティ権限を持つユーザは、ONS 15454 のセキュリティ ポリシーをプロビジョニングできます。セキュリティ ポリシーには、アイドル ユーザのタイムアウト、パスワード変更、パスワード期限切れ、およびユーザ ロックアウトのパラメータが含まれます。また、Superuser は、TCC2/TCC2P RJ-45 ポート、バックプレーン LAN 接続、またはその両方を使用して ONS 15454 にアクセスできます。

#### 9.2.2.1　Provisioning ユーザおける Superuser の権限

Superuser は、Provisioning ユーザに監査ログの取得、データベースの復旧、Performance Monitoring（PM; パフォーマンス モニタリング）パラメータのクリア、ソフトウェア ロードのアクティブ化、およびソフトウェア ロードの復帰を行うことを許可できます。これらの権限は、CTC の Network Element（NE; ネットワーク要素）デフォルトを使用することによってのみ設定できます（CTC の Provisioning> Security >Access タブにより Provisioning ユーザを許可できる PM クリア権限を除く）。Superuser の権限の設定の詳細については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

#### 9.2.2.2　アイドル ユーザのタイムアウト

ONS 15454 の CTC または TL1 の各ユーザは、ログイン セッションの間、指定した時間だけアイドル状態でいることができ、指定した時間が経過すると CTC ウィンドウはロックされます。このロックアウトにより、権限のないユーザによる変更を防止しています。表 9-3 に示すように、デフォルトのアイドル時間は、上位レベルのユーザであるほど短くなり、下位レベルになるにつれ長くなるか、無制限になります。Superuser は、ユーザのアイドル時間を変更できます。変更方法については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

**表 9-3　ONS 15454 ユーザのデフォルト アイドル時間**

| セキュリティ レベル | アイドル時間 |
|---|---|
| Superuser | 15 分 |
| Provisioning | 30 分 |
| Maintenance | 60 分 |
| Retrieve | 無制限 |

#### 9.2.2.3　ユーザ パスワード、ログイン、およびアクセス ポリシー

Superuser は、ノード単位で CTC または TL1 にログインしているユーザの一覧をリアルタイムで表示できます。また、Superuser は、次のパスワード、ログイン、ノード アクセス ポリシーをプロビジョニングできます。

- パスワードの有効期限と再使用 — パスワードの変更が必要な期限、およびパスワードを再使用できる期限を指定できます。
- ユーザのロックアウトおよび無効化 — ユーザをロックアウトするまでの無効ログインの回数、および非活動状態のユーザを無効にするまでの制限時間を設定できます。
- ノード アクセスおよびユーザ セッション — Superuser は、CTC セッション数を制限できます。1 つのユーザ ログインでは、1 セッションしか許可されません。また Superuser は、LAN または TCC2/TCC2P RJ-45 接続を使用して ONS 15454 にアクセスすることも禁止できます。

  また、Superuser は、CTC の Provisioning > Security > Access タブを使用して、Telnet の代わりに Secure Shell（SSH; セキュア シェル）を選択できます。SSH は、暗号化リンクを使用する端末とリモート ホスト間のインターネット プロトコルです。非セキュア チャネル上で、認証およびセキュアな通信を提供します。デフォルト ポートはポート 22 で、変更はできません。Superuser は、セキュアおよび非セキュア モードに EMS および TL1 アクセス ステートを設定することもできます。

# 9.3　監査証跡

Cisco ONS 15454 は、TCC2/TCC2P カードに保管される Telcordia GR-839-CORE 準拠の監査証跡ログを保持します。監査証跡は、セキュリティの保守、損失トランザクションの回復、アカウンタビリティの強制を実行する場合に役立ちます。アカウンタビリティは、ユーザの動作を追跡し、プロセスまたはアクションを特定のユーザに関連付けます。監査証跡ログには、システムにアクセスしたユーザ、および特定の時間内に実行された操作が記録されます。このログには、オペレーティングシステムの CLI（コマンドライン インターフェイス）、CTC、および TL1 を使用した、シスコがサポートする許可されたログインおよびログアウトが含まれます。また、FTP 動作、回線の作成と削除、ユーザおよびシステムが生成した動作も記録されます。

監査ログには、イベントのモニタリングも記録されます。イベントとは、ネットワーク要素のステータスの変更を意味します。外部イベント、内部イベント、アトリビュート変更、およびソフトウェアのアップロード / ダウンロード操作が、監査証跡に記録されます。

監査証跡ログの表示方法については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。監査証跡ログには、任意の管理インターフェイス（CTC、CTM、TL1）を使用してアクセスできます。

監査証跡は、永続メモリに保管されるので、プロセッサの切り替え、リセット、またはアップグレードによって失われることはありません。ただし、両方の TCC2/TCC2P カードを取り外すと、監査証跡ログは失われます。

## 9.3.1　監査証跡のログ エントリ

表 9-4 に、Audit Trail ウィンドウに表示されるカラムを示します。

**表 9-4　Audit Trail ウィンドウのカラム**

| 見出し | 説明 |
|---|---|
| Date | アクションが発生した日付 |
| Num | アクションの増分カウント |
| User | アクションを開始したユーザ ID |
| P/F | Pass/Fail（アクションが実行されたかどうか） |
| Operation | アクションの内容 |

監査証跡レコードには、次の動作がキャプチャされます。

- ユーザ — アクションを実行するユーザの名前
- ホスト — 動作がロギングされるホスト
- 装置 ID — 動作に含まれる装置の IP アドレス
- アプリケーション — 動作に含まれるアプリケーションの名前
- タスク — 動作に含まれるタスクの名前（ダイアログボックスの表示、設定の適用、など）
- 接続モード — Telnet、コンソール、SNMP
- カテゴリ — 変更の種類（ハードウェア、ソフトウェア、コンフィギュレーション）
- ステータス — ユーザ動作のステータス（Read、Initial、Successful、Timeout、Failed）
- 時間 — 変更の時間
- メッセージ タイプ — イベントが成功または失敗のどちらであるか
- メッセージの詳細 — 変更の説明

## 9.3.2　監査証跡の容量

ONS 15454 は、640 のログ エントリを保管できます。最大数に達すると、最も古いエントリが最新イベントに書き換えられます。ログ サーバの使用率が 80% に達すると、（CORBA/CTC により）AUD-LOG-LOW 条件が発生し、ロギングされます。

ログ サーバ が 640 エントリの最大容量に達し、保管されていないレコードの書き換えが開始されると、AUD-LOG-LOSS 条件が発生し、ロギングされます。このイベントは、監査証跡レコードが失われたことを意味します。ファイルをオフロードしない限り、新しいデータによって書き換えられたエントリの数量に関係なく、このイベントは再発生しません。監査証跡ログのエクスポート方法については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

# 9.4 RADIUS セキュリティ

Superuser セキュリティ権限を持つユーザは、ノードが Remote Authentication Dial In User Service（RADIUS）認証を使用するように設定できます。シスコシステムズは、リモート ユーザの ID 確認、アクセス許可、および動作追跡を実行するために、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）と呼ばれる方式を採用しています。

## 9.4.1 RADIUS 認証

RADIUS は、不正アクセスを防止し、ネットワークおよびネットワーク サービスへのセキュアなリモート アクセスを確保する分散セキュリティ システムです。RADIUS は、3 つのコンポーネントで構成されます。

- UDP/IP を使用するフレーム形式のプロトコル
- サーバ
- クライアント

サーバは通常、カスタマー サイトの中央コンピュータ上で実行しますが、クライアントはダイヤルアップ アクセス サーバ上で実行し、ネットワーク全体に分散できます。

ONS 15454 ノードは、RADIUS のクライアントとして動作します。クライアントは、指定された RADIUS サーバにユーザ情報を送信し、戻された応答に基づいて動作します。RADIUS サーバは、ユーザの接続要求を受信し、ユーザを認証し、ユーザにサービスを提供するために必要なすべての設定情報をクライアントに戻します。RADIUS サーバは、他の種類の認証サーバのプロキシ クライアントとしても使用できます。RADIUS クライアントとサーバ間のトランザクションは、ネットワーク上には送信されない共有シークレットを使用して認証されます。また、ユーザのパスワードはすべて、RADIUS クライアントとサーバ間で暗号化されて送信されます。したがって、セキュアではないネットワークをモニタしている侵入者がいたとしても、ユーザのパスワードが盗まれることはありません。RADIUS 認証の設定方法については、『*Cisco ONS 15454 Procedure Guide*』を参照してください。

## 9.4.2 共有シークレット

共有シークレットは、次の二者間のパスワードとして使用される文字列です。

- RADIUS クライアントと RADIUS サーバ
- RADIUS クライアントと RADIUS プロキシ
- RADIUS プロキシと RADIUS サーバ

RADIUS クライアント、RADIUS プロキシ、および RADIUS サーバを使用する設定では、RADIUS クライアントと RADIUS プロキシ間、および RADIUS プロキシと RADIUS サーバ間に個別の共有シークレットを使用できます。

共有シークレットは、Access-Request メッセージを除く RADIUS メッセージが、同じ共有シークレットが設定された RADIUS 対応装置から送信されたことを確認するために使用します。また、共有シークレットにより、送信中に RADIUS メッセージが変更されていないこと（メッセージの完全性）を確認できます。さらに、共有シークレットによって、ユーザ パスワードおよびトンネル パスワードなどの一部の RADIUS アトリビュートを暗号化できます。

共有シークレットの作成および使用方法：

- 両方の RADIUS 装置上で、大文字と小文字を区別した同じ共有シークレットを使用します。
- 各 RADIUS クライアントと RADIUS サーバの組み合わせには、それぞれ異なる共有シークレットを使用します。

- ランダムな共有シークレットを使用するには、最低 22 文字の長さのランダム シーケンスを生成します。
- 任意の標準の英数字および特殊文字を使用できます。
- 共有シークレットの長さは、最大 128 文字です。サーバおよび RADIUS クライアントを総当り攻撃から保護するには、長い（22 文字以上）共有シークレットを使用します。
- サーバおよび RADIUS クライアントを辞書攻撃から保護するには、共有シークレットを、文字、数字、句読点のランダム シーケンスとし、頻繁に変更します。共有シークレットには、表 9-5 に示す 3 つのすべてのグループの文字を含めるべきです。

**表 9-5　共有シークレットの文字グループ**

| グループ | 例 |
|---|---|
| 英字（大文字および小文字） | A、B、C、D、および a、b、c、d |
| 数字 | 0、1、2、3 |
| 記号（英数字以外のすべての文字） | 感嘆符（!）、アスタリスク（*）、コロン（:） |

共有シークレットが複雑であるほど、暗号化されるアトリビュート（パスワードおよび暗号鍵に使用されるアトリビュートなど）の安全性は高くなります。複雑な共有シークレットの例を以下に示します。8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(