CHAPTER 15

セキュリティ リファレンス

この章では、Cisco ONS 15454 のユーザとセキュリティについて説明します。

（注） 特に指定のない限り、「ONS 15454」は、ANSI と ETSI 両方のシェルフ アセンブリを指します。

この章の内容は、次のとおりです。

15.1 ユーザ ID およびセキュリティ レベル

ONS 15454 システムには Cisco Transport Controller（CTC）ID がありますが、このユーザ ID は CTC にログインするときには表示されません。この ID は、他の ONS 15454 ユーザの設定に使用できます。

1 台の ONS 15454 で、最大 500 のユーザ ID を保持できます。各 CTC または TL1 ユーザには、次のセキュリティ レベルのうち 1 つを割り当てることができます。

- 取得：CTC 情報を取得して表示できますが、パラメータの設定や修正はできません。
- メンテナンス：ONS 15454 のメンテナンス オプションにのみアクセスできます。
- プロビジョニング：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。
- スーパーユーザ：他のセキュリティ レベルのすべての機能に加え、他のユーザの名前、パスワード、セキュリティ レベルの設定ができます。

各セキュリティ レベルに対応した、アイドル ユーザのタイムアウトについての情報は、表 15-3（P.15-7）を参照してください。

デフォルトでは、複数のユーザ ID セッションをノード上で同時に行うことができます。つまり、複数のユーザが、同じユーザ ID で 1 つのノードにログインできます。ただし、ユーザごとに単一のログインのみを許可し、すべてのユーザが同じユーザ ID で同時にログインしないようにノードをプロビジョニングできます。

（注） ユーザがアクセスするノードごとに、同じユーザ名とパスワードを追加する必要があります。

（注）　メンテナンス、プロビジョニング、およびスーパーユーザは、レーザー安全性の危険について適切な訓練を受け、安全に関連する手順、ラベル、警告を認識している必要があります。レーザーに関する警告を含む、安全性ラベルと警告の最新の一覧については、『*Cisco Optical Products Safety and Compliance Information*』の文書を参照してください。国際的なレーザー安全基準については IEC 60825-2、または米国のレーザー安全基準については ANSI Z136.1 を参照してください。『*Cisco ONS 15454 DWDM Procedure Guide*』で、メンテナンスや設置中にレーザーの安全性を無効にする方法を説明しています。この手順に従う場合は、危険な状態や光放射への異常な曝露を防ぐため、すべての警告と注意を守ってください。

15.2 ユーザ権限とポリシー

この項では、各 CTC タスクのユーザ権限の一覧を示し、プロビジョニングするためにスーパーユーザが使用できるセキュリティ ポリシーについて説明します。

15.2.1 CTC タスクごとのユーザ権限

表 15-1 は、ノード ビューで各ユーザ権限レベルが実行できるアクションです。

表 15-1　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]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
[Alarms]	—	Synchronize/Filter/Delete Cleared Alarms	X	X	X	X
[Conditions]	—	Retrieve/Filter	X	X	X	X
[History]	[Session]	Filter	X	X	X	X
	[Node]	Retrieve/Filter	X	X	X	X
[Circuits]	[Circuits]	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	[Rolls]	Complete/ Force Valid Signal/ Finish	—	—	X	X

表 15-1　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]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
[Provisioning]	[General]	[General]: Edit	—	—	一部[1]	X
		[Multishelf Config]: Edit	—	—	—	X
	[Network]	[General]: Edit	—	—	—	X
		[Static Routing]: Create/Edit/Delete	—	—	X	X
		[OSPF]: Create/Edit/Delete	—	—	X	X
		[RIP]: Create/Edit/Delete	—	—	X	X
		[Proxy]: Create/Edit/Delete	—	—	—	X
		[Firewall]: Create/Edit/Delete	—	—	—	X
	[OSI]	[Main Setup]: Edit	—	—	—	X
		[TARP]: [Config]: Edit	—	—	—	X
		[TARP]: [Static TDC]: Add/Edit/Delete	—	—	X	X
		[TARP]: [MAT]: Add/Edit/Remove	—	—	X	X
		[Routers]: [Setup]: Edit	—	—	—	X
		[Routers]: [Subnets]: Edit/Enable/Disable	—	—	X	X
		[Tunnels]: Create/Edit/Delete	—	—	X	X

表 15-1　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]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
	[Security]	[Users]: Create/Delete/Clear Security Intrusion Alarm	—	—	—	X
		[Users]: Change	同じユーザ	同じユーザ	同じユーザ	すべてのユーザ
		[Active Logins]: View/Logout/ Retrieve Last Activity Time	—	—	—	X
		[Policy]: Edit/View	—	—	—	X
		[Access]: Edit/View	—	—	—	X
		[RADIUS Server]: Create/Edit/Delete/Move Up/Move Down/View	—	—	—	X
		[Legal Disclaimer]: Edit	—	—	—	X
	[SNMP]	Create/Edit/Delete	—	—	X	X
		Browse trap destinations	X	X	X	X
	[Comm Channels]	[SDCC]: Create/Edit/Delete	—	—	X	X
		[LDCC]: Create/Edit/Delete	—	—	X	X
		[GCC]: Create/Edit/Delete	—	—	X	X
		[OSC]: Create/Edit/Delete	—	—	X	X
		[PPC]: Create/Edit/Delete	—	—	X	X
		[LMP]: [General]: Edit	X	X	X	X
		[LMP]: [Control Channels]: Create/Edit/Delete	—	—	—	X
		[LMP]: [TE Links]: Create/Edit/Delete	—	—	—	X
		[LMP]: [Data Links]: Create/Edit/Delete	—	—	—	X
	[Alarm Profiles]	Load/Store/Delete[2]	—	—	X	X
		New/Compare/Available/Usage	X	X	X	X
	[Defaults]	Edit/Import	—	—	—	X
		Reset/Export	X	X	X	X
	[WDM-ANS]	[Provisioning]: Edit	—	—	—	X
		[Provisioning]: Reset	X	X	X	X
		[Internal Patchcords]: Create/Edit/Delete/Commit/ Default Patchcords	—	—	X	X
		[Port Status]: Launch ANS	—	—	—	X
		[Node Setup]: Setup/Edit	X	X	X	X
		[Optical Side]: Create/Edit/Delete	X	X	X	X

表 15-1　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]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
[Inventory]	—	Delete	—	—	X	X
		Reset	—	X	X	X
[Maintenance]	[Database]	Backup	—	X	X	X
		Restore	—	—	—	X
	[Network]	[Routing Table]: Retrieve	X	X	X	X
		[RIP Routing Table]: Retrieve	X	X	X	X
	[OSI]	[IS-IS RIB]: Refresh	X	X	X	X
		[ES-IS RIB]: Refresh	X	X	X	X
		[TDC]: TID to NSAP/Flush Dynamic Entries	—	X	X	X
		[TDC]: Refresh	X	X	X	X
	[Software]	Download/Cancel	—	X	X	X
		Activate/Revert	—	—	—	X
	[Diagnostic]	Node Diagnostic Logs	—	—	X	X
	[Audit]	Retrieve	—	—	—	X
		Archive	—	—	X	X
	[DWDM]	[APC]: Run/Disable/Refresh	—	X	X	X
		[WDM Span Check]: Retrieve Span Loss values/ Edit/Reset	X	X	X	X
		[ROADM Power Monitoring]: Refresh	X	X	X	X
		[PP-MESH Internal Patchcord]: Refresh	X	X	X	X
		[Install Without Metro Planner]: Retrieve Installation values	X	X	X	X
		[All Facilities]: Mark/Refresh	X	X	X	X

1. プロビジョニング ユーザはノード名、コンタクト、場所、および AIS-V insertion on STS-1 Signal Degrade（SD; 信号劣化）パラメータの変更はできません。
2. このサブタブのアクション ボタンはすべてのユーザに対して有効になっていますが、アクションを完全に実行できるのは、必要なセキュリティ レベルを割り当てられたユーザだけです。

表 15-2 は、ネットワーク ビューで各ユーザ権限レベルが実施できるアクションです。

表 15-2　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]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
[Alarms]	—	Synchronize/Filter/Delete cleared alarms	X	X	X	X
[Conditions]	—	Retrieve/Filter	X	X	X	X
[History]	—	Filter	X	X	X	X

表 15-2　ONS 15454 セキュリティ レベル：ネットワーク ビュー（続き）

CTC タブ	サブタブ	[サブタブ]: アクション	取得	メンテナンス	プロビジョニング	スーパーユーザ
[Circuits]	[Circuits]	Create/Edit/Delete	—	—	X	X
		Filter/Search	X	X	X	X
	[Rolls]	Complete/ Force Valid Signal/ Finish	—	—	X	X
[Provisioning]	[Security]	[Users]: Create/Delete/Clear Security Intrusion Alarm	—	—	—	X
		[Users]: Change	同じユーザ	同じユーザ	同じユーザ	すべてのユーザ
		[Active logins]: Logout/Retrieve Last Activity Time	—	—	—	X
		[Policy]: Change	—	—	—	X
	[Alarm Profiles]	New/Load/Store/Delete[1]	—	—	X	X
		[Compare]/[Available]/[Usage]	X	X	X	X
	[BLSR (ANSI)] [MS-SPRing (ETSI)]	Create/Edit/Delete/Upgrade	—	—	X	X
	[Overhead Circuits]	Create/Delete/Edit/Merge	—	—	X	X
		[Search]	X	X	X	X
	[Provisionable Patchcords (PPC)]	Create/Edit/Delete	—	—	X	X
	[Server Trails]	Create/Edit/Delete	—	—	X	X
	[VLAN DB Profile]	Load/Store/Merge/Circuits	X	X	X	X
		Add/Remove Rows	—	—	X	X
[Maintenance]	[Software]	Download/Cancel	—	X	X	X
	[Diagnostic]	[OSPF Node Information]: Retrieve/Clear	X	X	X	X
	[APC]	Run APC/Disable APC	—	—	—	X
		[Refresh]	X	X	X	X

1. このサブタブのアクション ボタンはすべてのユーザに対して有効になっていますが、アクションを完全に実行できるのは、必要なセキュリティ レベルを割り当てられたユーザだけです。

15.2.2 セキュリティ ポリシー

スーパーユーザは、ONS 15454 でセキュリティ ポリシーをプロビジョニングできます。これらのセキュリティ ポリシーには、アイドル ユーザのタイムアウト、パスワードの変更、パスワードの有効期限、およびユーザのロックアウト パラメータが含まれます。加えて、スーパーユーザは TCC2/TCC2P/TCC3 RJ-45 ポートまたはバックプレーン LAN 接続、あるいはその両方を経由して ONS 15454 にアクセスできます。

15.2.2.1 プロビジョニング ユーザに対するスーパーユーザ権限

スーパーユーザは、プロビジョニング ユーザに、一連のタスクを実行する権限を与えることができます。このタスクには、監査ログの取得、データベースの復元、PM のクリア、およびソフトウェアのロードの有効化と復元が含まれます。これらの権限は、CTC Network Element（NE; ネットワーク要素）のデフォルトを通じてのみ設定できます。ただし、PM のクリア権限を除きます。PM のクリア権限は、[CTC Provisioning] > [Security] > [Access] タブを使用してプロビジョニング ユーザに付与できます。スーパーユーザ権限の設定の詳細については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。

15.2.2.2 アイドル ユーザのタイムアウト

ONS 15454 CTC または TL1 ユーザはそれぞれ、ログイン セッションの間、指定した時間アイドルでいることができ、指定した時間が経過すると CTC ウィンドウがロックされます。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ぎます。表 15-3 に示すように、デフォルトのアイドル期間は、より上位レベルのユーザほど短くなり、低位レベルのユーザほどより長く、あるいは無制限になります。

表 15-3　ONS 15454 のデフォルトのユーザ アイドル時間

セキュリティ レベル	アイドル時間
スーパーユーザ	15 分
プロビジョニング	30 分
メンテナンス	60 分
取得	制限なし

15.2.2.3 ユーザ パスワード、ログイン、アクセス ポリシー

スーパーユーザは、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、ノードごとに表示できます。また、スーパーユーザは、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することもできます。

- パスワードの長さ、有効期限および再使用：スーパーユーザは、NE のデフォルトを使用してパスワードの長さを設定できます。パスワードの長さは、デフォルトで、6 ～ 20 文字に設定されています。この CTC のノード ビューのデフォルト値は、[Provisioning] > [NE Defaults] > [Node] > [security] > [password Complexity] タブで設定できます。最小の長さは 8、10、12 文字のいずれか、最大の長さは 80 文字まで設定できます。パスワードは、英数字（a ～ z、A ～ Z、0 ～ 9）および特殊文字（+、#、%）の組み合わせで、このうち最低 2 文字をアルファベット以外の文字、最低 1 文字を特殊文字にしなければなりません。スーパーユーザは、パスワードの変更が必要な期限と、同じパスワードを再使用できるようになる期限を指定できます。
- ユーザのロック アウトとディセーブル化：スーパーユーザは、ユーザをロック アウトするまでに許される無効なログイン回数と、非アクティブなユーザが無効になるまでの時間をプロビジョニングできます。ロックアウト試行ができる回数は、ログイン試行ができる回数に設定されます。
- ノード アクセスとユーザ セッション：スーパーユーザは、1 ユーザが行える CTC セッション数を制限でき、LAN や TCC2/TCC2P/TCC3 RJ-45 接続を使用した ONS 15454 へのアクセスを禁止できます。

  さらに、スーパーユーザは、Telnet の代わりに Secure Shell（SSH; セキュア シェル）を [CTC Provisioning] > [Security] > [Access] タブで選択できます。SSH は、暗号化されたリンクを使用する端末リモート ホストのインターネット プロトコルです。これにより、非セキュアのチャネルでの認証とセキュアな通信を提供します。ポート 22 がデフォルトのポートで、変更できません。

15.3 監査証跡

Cisco ONS 15454 は、TCC2/TCC2P/TCC3/TNC/TSC カードに Telcordia GR-839-CORE 準拠の監査証跡ログを保持しています。監査証跡は、セキュリティの維持や失われたトランザクションの回復、アカウンタビリティの実行に役立ちます。アカウンタビリティとは、ユーザのアクティビティの追跡、つまりプロセスやアクションと特定のユーザを関連付けることを意味します。システムにアクセスしたユーザと、特定の期間に行わ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 システムのコマンド ライン インターフェイス、CTC、TL 1 を使用した、認可済みのシスコ ログインおよびログアウトや、回線の作成と削除、ユーザやシステムによって生成されるアクションが含まれます。

イベントのモニタリングも、監査ログに記録されます。イベントは、ネットワーク内の要素のステータスの変化と定義されます。外部イベント、内部イベント、属性の変更、ソフトウェアのアップロードとダウンロード アクティビティが、監査証跡に記録されます。

監査証跡は、固定メモリに保存され、プロセッサの切り替え、リセット、アップグレードでも破壊されることはありません。ただし、TCC2/TCC2P/TCC3/TNC/TSC カードを両方とも取り外した場合、監査証跡ログは失われます。

15.3.1 監査証跡ログのエントリ

表 15-4 に、[Audit Trail] ウィンドウの一覧のカラムを示します。

表 15-4　[Audit Trail] ウィンドウのカラム

ヘッダー	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の ID
P/F	成功/失敗（アクションが実行されたかどうか）
Operation	行われたアクション

監査証跡の記録には、次のアクティビティが取得されます。

- User：アクションを実行したユーザの名前
- Host：アクティビティが記録されたホスト
- Device ID：アクティビティに関連するデバイスの IP アドレス
- Application：アクティビティに関連するアプリケーションの名前
- Task：アクティビティに関連するタスク（ダイアログ ボックスの表示、設定の適用など）の名前
- Connection Mode：Telnet、コンソール、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
- Category：変更の種類（ハードウェア、ソフトウェア、構成）
- Status：ユーザのアクションのステータス（読み取り、初回、成功、タイムアウト、失敗）
- Time：変更時刻
- Message Type：イベントの、Success または Failure どちらかのタイプを表示
- Message Details：変更の説明

15.3.2 監査証跡の容量

システムは、640 個のログ エントリを格納できます。この限度に達すると、最も古いエントリが、新しいイベントで上書きされます。ログ サーバの使用率が 80% になると、AUD-LOG-LOW 条件が発生し、ログに記録されます（Common Object Request Broker Architecture（CORBA）/CTC を使用）。

ログ サーバが最大容量の 640 エントリに達し、アーカイブされていないレコードの上書きが始まると、AUD-LOG-LOSS 条件が発生し、ログに記録されます。このイベントは、監査証跡レコードが失われたことを示します。このイベントは、システムが上書きするエントリの量にかかわらずファイルをオフロードするまでの間に 1 回のみ起こります。

15.4 RADIUS セキュリティ

スーパーユーザは、ノードを設定して Remote Authentication Dial In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）認証を使用できます。RADIUS は、Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）として知られる機能を使用して、リモート ユーザの識別、リモート ユーザへのアクセス、リモート ユーザのアクションの追跡を行います。RADIUS 認証の設定については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。

RADIUS サーバは IPv6 アドレスをサポートしており、IPv6 アドレスを使用する GNE または ENE からの認証要求を処理できます。

15.4.1 RADIUS 認証

RADIUS は、ネットワークやネットワーク サービスのリモート アクセスを不正アクセスから保護する分散型セキュリティシステムです。RADIUS は、次の 3 つのコンポーネントで構成されています。

- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）/IP を利用したフレーム形式のプロトコル
- サーバ 1 台
- クライアント 1 台

通常、サーバはカスタマーサイトの中央コンピュータで実行されます。クライアントはダイヤルアップ アクセス サーバにあり、ネットワーク中に分散が可能です。

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、ユーザ情報を目的の RADIUS サーバに渡し、返された応答に基づいて動作します。RADIUS サーバには、ユーザ接続要求を受け取り、ユーザを認証し、クライアントがユーザにサービスを提供するため必要なすべての設定情報を返す役割があります。RADIUS サーバは、他の種類の認証サーバに対しては、プロキシ クライアントとして動作します。クライアントと RADIUS サーバとの間のトランザクションは、共有秘密を使用して認証されます。共有秘密はネットワーク上に送信されることはありません。また、クライアントと RADIUS サーバ間では、すべてのパスワードが暗号化されて送信されます。これにより、保護されていないネットワーク上でユーザのパスワードがスヌーピングされ、特定されることがなくなります。

15.4.2 共有秘密

共有秘密は、次の場合に、パスワードとして使用されるテキスト文字列です。

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

RADIUS クライアント、RADIUS プロキシ、RADIUS サーバを使用する構成では、RADIUS クライアントと RADIUS プロキシ間で使用される共有秘密が、RADIUS プロキシと RADIUS サーバ間で使用される共有秘密とは異なる場合があります。

共有秘密は、Access-Request メッセージを除く RADIUS メッセージが、同じ共有秘密が設定されている RADIUS 対応デバイスによって送信されているかどうかを検証するために使用されます。また、共有秘密で、RADIUS メッセージが中継中に変更されていないこと（メッセージ完全性）も検証されます。共有秘密は、User-Password や Tunnel-Password など一部の RADIUS 属性を暗号化するためにも使用されます。

共有秘密を作成したり使用する際は、次の点に注意してください。

- 両方の RADIUS デバイスで、同じ共有秘密（大文字と小文字は区別されます）を使用してください。
- RADIUS サーバと RADIUS クライアントの組ごとに、異なる共有秘密を使用してください。
- ランダムな共有秘密を確実に作成するため、22 文字以上の長さのランダムなシーケンスを作成してください。
- 通常の英数字と特殊文字を使用できます。
- 長さ 128 文字までの共有秘密を使用できます。サーバと RADIUS クライアントを総当たり攻撃から守るため、22 文字を超える長い共有秘密を使用してください。
- サーバと RADIUS クライアントを辞書攻撃から守るため、共有秘密は、文字、番号、句読点からなるランダムなシーケンスにしてください。また、頻繁に変更してください。共有秘密は、表 15-5 に示す 3 つのグループそれぞれからの文字を含むようにしてください。

表 15-5　共有秘密の文字グループ

グループ	例
文字（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（文字または数字に定義されている以外のすべての文字）	感嘆符（!）、アスタリスク（*）、コロン（:）

共有秘密の強度が高いほど、共有秘密を使用して暗号化される属性（パスワードや暗号化キーに使用されている属性など）が安全になります。たとえば、8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(. などが、強度の高い共有秘密です。