CHAPTER 6

セキュリティ基準

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。

（注） 特に指定のないかぎり、[ONS 15454] は ANSI と ETSI の両方のシェルフ アセンブリを意味します。

この章では、次の内容について説明します。

6.1　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 にサインインするときには表示されません。この ID は、ほかの ONS 15454 ユーザを設定する際に使用できます。

1 台の ONS 15454 には、最大 500 のユーザ ID を設定できます。各 CTC ユーザまたは TL1 ユーザには、次に示すセキュリティ レベルの 1 つを割り当てることができます。

- 検索 — CTC の情報を検索し、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 オプションにアクセスできます。
- プロビジョニング — プロビジョニング オプション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 — ほかのユーザの名前、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 レベルに対応したアイドル ユーザのタイムアウトについては、表 6-3 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で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、ユーザごとに 1 つのログインだけを許可し、すべてのユーザに対して、同じユーザ ID を使用して同時に複数ログインできないように、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。

6.2　ユーザ権限とポリシー

ここでは、各 CTC タスクのユーザ権限を示し、プロビジョニングするためにスーパーユーザが利用できるセキュリティ ポリシーについて説明します。

6.2.1　CTC タスクごとのユーザ権限

表 6-1 に、ノード ビューで各権限レベルのユーザが実行できるアクションを示します。

表 6-1　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	検索	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	○	○	○	○
Conditions	—	Retrieve/Filter	○	○	○	○
History	Session	Filter	○	○	○	○
	Node	Retrieve/Filter	○	○	○	○
Circuits	Circuits	Create/Edit/Delete	—	—	○	○
		Filter/Search	○	○	○	○
	Rolls	Complete/ Force Valid Signal/ Finish	—	—	○	○
Provisioning	General	General: Edit	—	—	一部[1]	○
		Multishelf Config: Edit	○	○	○	○
	EtherBridge	Spanning trees: Edit	—	—	○	○
	Network	General: Edit	—	—	—	○
		Static Routing: Create/Edit/Delete	—	—	○	○
		OSPF: Create/Edit/Delete	—	—	○	○
		RIP: Create/Edit/Delete	—	—	○	○
		Proxy: Create/Edit/Delete	—	—	—	○
		Firewall: Create/Edit/Delete	—	—	—	○
	OSI	Main Setup: Edit	—	—	—	○
		TARP: Config: Edit	—	—	—	○
		TARP: Static TDC: Add/Edit/Delete	—	—	○	○
		TARP: MAT: Add/Edit/Remove	—	—	○	○
		Routers: Setup: Edit	—	—	—	○
		Routers: Subnets: Edit/Enable/Disable	—	—	○	○
		Tunnels: Create/Edit/Delete	—	—	○	○

表 6-1　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	検索	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	―	―	―	○
		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	―	―	―	○
		Policy: Edit/View	―	―	―	○
		Access: Edit/View	―	―	―	○
		RADIUS Server: Create/Edit/Delete/Move Up/Move Down/View	―	―	―	○
		Legal Disclaimer: Edit	―	―	―	○
	SNMP	Create/Edit/Delete	―	―	○	○
		Browse trap destinations	○	○	○	○
	Comm Channels	RS-DCC: Create/Edit/Delete	―	―	○	○
		MS-DCC: Create/Edit/Delete	―	―	○	○
		GCC: Create/Edit/Delete	―	―	○	○
		OSC: OSC Terminations: Create/Edit/Delete	―	―	○	○
		OSC: DWDM Ring ID: Create/Edit/Delete	―	―	―	○
		PPC: Create/Edit/Delete	―	―	○	○
	Alarm Profiles	Load/Store/Delete[2]	―	―	○	○
		New/Compare/Available/Usage	○	○	○	○
	Defaults	Edit/Import	―	―	―	○
		Reset/Export	○	○	○	○
	WDM-ANS	Provisioning: Edit	―	―	―	○
		Provisioning: Reset	○	○	○	○
		Internal Patchcords: Create/Edit/Delete/Commit/ Default Patchcords	―	―	○	○
		Port Status: Launch ANS	―	―	―	○
		Node Setup: Setup/Edit	○	○	○	○
Inventory	―	Delete	―	―	○	○
		Reset	―	○	○	○

表 6-1　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	検索	メンテナンス	プロビジョニング	スーパーユーザ
Maintenance	Database	Backup	—	○	○	○
		Restore	—	—	—	○
	Network	Routing Table: Retrieve	○	○	○	○
		RIP Routing Table: Retrieve	○	○	○	○
	OSI	IS-IS RIB: Refresh	○	○	○	○
		ES-IS RIB: Refresh	○	○	○	○
		TDC: TID to NSAP/Flush Dynamic Entries	—	○	○	○
		TDC: Refresh	○	○	○	○
	Software	Download/Cancel	—	○	○	○
		Activate/Revert	—	—	—	○
	Diagnostic	Retrieve Tech Support Log	—	—	○	○
	Audit	Retrieve	—	—	—	○
		Archive	—	—	○	○
	DWDM	APC: Run/Disable/Refresh	—	○	○	○
		WDM Span Check: Retrieve Span Loss values/ Reset	○	○	○	○
		ROADM Power Monitoring: Refresh	○	○	○	○

1. プロビジョニング ユーザは、STS-1 Signal Degrade（SD; 信号劣化）パラメータのノード名、接点、または AIS-V 挿入を変更できません。
2. 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、必要なセキュリティ レベルが割り当てられたユーザだけがそのアクションを完全に実行することができます。

表 6-2 に、ネットワーク ビューで各ユーザ権限レベルが実行できるアクションを示します。

表 6-2　ONS 15454 のセキュリティ 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	検索	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	○	○	○	○
Conditions	—	Retrieve/Filter	○	○	○	○
History	—	Filter	○	○	○	○
Circuits	Circuits	Create/Edit/Delete	—	—	○	○
		Filter/Search	○	○	○	○
	Rolls	Complete/ Force Valid Signal/ Finish	—	—	○	○

表 6-2　ONS 15454 のセキュリティ 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	検索	メンテナンス	プロビジョニング	スーパーユーザ
Provisioning	Security	Users: Create/Delete/Clear Security Intrusion Alarm	―	―	―	○
		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	―	―	―	○
		Policy: Change	―	―	―	○
	Alarm Profiles	New/Load/Store/Delete[1]	―	―	○	○
		Compare/Available/Usage	○	○	○	○
	BLSR（ANSI） MS-SPRing（ETSI）	Create/Edit/Delete/Upgrade	―	―	○	○
	Overhead Circuits	Create/Delete/Edit/Merge	―	―	○	○
		Search	○	○	○	○
	Provisionable Patchcords（PPC）	Create/Edit/Delete	―	―	○	○
	Server Trails	Create/Edit/Delete	―	―	○	○
Maintenance	Software	Download/Cancel	―	○	○	○
	Diagnostic	OSPF Node Information: Retrieve/Clear	○	○	○	○

1. 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、必要なセキュリティ レベルが割り当てられたユーザだけがそのアクションを完全に実行することができます。

6.2.2　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することができます。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。さらに、スーパーユーザは、TCC2/TCC2P RJ-45 ポート、バックプレーン LAN 接続、またはその両方を経由して ONS 15454 にアクセスすることができます。

6.2.2.1　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、一連のタスクを実行するためにプロビジョニング ユーザに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 ロードの有効化と復元があります。これらの権限は、PM のクリア権限を除いて CTC Network Element（NE; ネットワーク要素）デフォルトを通じてのみ設定可能です。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 ユーザに与えることができます。スーパーユーザ権限の設定の詳細については、『*Cisco ONS 15454 DWDN Procedure Guide*』を参照してください。

6.2.2.2　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 6-3 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。

表 6-3　ONS 15454 のデフォルト ユーザのアイドル時間

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
検索	無制限

6.2.2.3　ユーザ パスワード、ログイン、およびアクセス ポリシー

スーパーユーザは、ノードごとに現在 CTC または TL1 にログインしているユーザのリストをリアルタイムで表示することができます。スーパーユーザは、次のパスワード、ログイン、およびノード 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。

- パスワードの有効期限と再利用 — スーパーユーザは、パスワードの変更が必要な期限とパスワードが再利用可能になる期限を指定できます。
- ロックアウトとユーザのディセーブル化 — スーパーユーザは、ロックアウトされるまでに許される無効なログインの回数と非アクティブなユーザが無効になるまでの時間の長さをプロビジョニングできます。許容されるロックアウト試行回数は、許容されるログイン試行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 人のユーザが起動できる CTC セッションの数を制限でき、LAN または TCC2/TCC2P RJ-45 接続を使用した ONS 15454 へのアクセスを禁止できます。

  また、スーパーユーザは、CTC の Provisioning > Security > Access タブで、Telnet の代わりに Secure Shell（SSH; セキュア シェル）を選択することができます。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 IP で、非セキュア チャネル上で、認証とセキュア通信を提供します。ポート 22 がデフォルトのポートで、変更することはできません。

6.3　監査証跡

Cisco ONS 15454 は、TCC2/TCC2P カード上に監査証跡ログ（Telcordia GR-839-CORE に準拠）を保持しています。監査証跡は、セキュリティの保守、失われたトランザクションの回復、および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を特定のユーザに関連付けることを意味します。このレコードには、システムにアクセスしたユーザ、およびある一定期間に実行された操作が記録されます。ログには、OS（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、認可済みのシスコ ログインおよびログアウトが含まれます。また、FTP（ファイル転送プロトコル）の動作、回線の作成と削除、およびユーザとシステムによって生成される動作も含まれます。

イベント モニタリングも、監査ログに記録されます。各イベントは、ネットワーク内にある何らかの要素のステータス変更として定義されます。外部イベント、内部イベント、アトリビュートの変更、および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格納され、プロセッサの切り替え、リセット、またはアップグレードが原因で破損することはありません。ただし、TCC2/TCC2P の両方のカードを取り外した場合には、監査証跡ログは失われます。

6.3.1　監査証跡ログのエントリ

表 6-4 に、Audit Trail ウィンドウで表示されるカラムを示します。

表 6-4　Audit Trail ウィンドウのカラム

ヘッダ	説明
Date	動作が発生した日付
Num	動作の増分カウント
User	動作を開始したユーザの ID
P/F	成功 / 失敗（その動作が実行されたかどうか）
Operation	行われた動作

監査証跡レコードには、次のアクティビティがキャプチャされます。

- 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るホスト
- Device ID — アクティビティに関連する装置の 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（ダイアログボックスの表示、設定の適用など）に関連するタスクの名前
- Connection Mode — Telnet、コンソール、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 — ユーザの動作のステータス（読み取り、初回、成功、タイムアウト、失敗）
- Time — 変更の時間
- Message Type — イベントの Success（成功）/Failure（失敗）を表示
- Message Details — 変更の説明

6.3.2　監査証跡のキャパシティ

システムには、640 個のログ エントリを格納できます。この上限に到達すると、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 条件が発生してログに記録されます（Common Object Request Broker Architecture [CORBA]/CTC を使用）。

ログ サーバが最大キャパシティの 640 エントリに到達して、アーカイブされていない記録の上書きが開始されると、AUD-LOG-LOSS 条件が発生して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数に関係なく、ユーザがファイルをオフロードするまでの間に 1 回だけ発生します。

6.4 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）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）として知られている機能を使用して、リモート ユーザについて、ID の確認、アクセスの許可、操作の追跡を行います。RADIUS 認証については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。

6.4.1 RADIUS 認証

RADIUS は、認証されていないアクセスに対して、ネットワークおよびネットワーク サービスへのリモート アクセスを防ぐ分散セキュリティ 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。

- UDP/IP を使用した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で実行されます。一方、クライアントはダイヤルアップ アクセス サーバに存在し、ネットワーク全体に存在する可能性があります。

ONS 15454 ノードは RADUIS のクライアントとして動作します。クライアントには指定の RADIUS サーバへユーザ情報を渡す役割があり、その戻り応答に基づいて動作します。RADIUS サーバにはユーザの接続要求を受信して、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に必要なすべての設定情報を返します。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。さらに、ユーザのパスワードはクライアントと RADIUS サーバ間で暗号化して送信されます。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盗まれることがなくなります。

6.4.2 共有秘密

共有秘密は、次の間で、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
- 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 サーバ間で使用する共有秘密とは異なる場合があります。

共有秘密は、RADIUS メッセージ（Access-Request メッセージを除く）が同じ共有秘密で設定されている RADIUS 対応装置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、共有秘密は、変更中に修正されなかった RADIUS メッセージも検証します（メッセージの整合性）。共有秘密は、ユーザのパスワードやトンネル パスワードのような一部の RADIUS アトリビュートの暗号化にも使用されます。

共有秘密の作成および使用には、次の点に注意してください。

- RADIUS 装置間で大文字と小文字が区別される同じ共有秘密を使用する。
- RADIUS サーバと RADIUS クライアントの各ペアごとに、異なる共有秘密を使用する。
- ランダムな共有秘密を確実に作成するには、最低 22 文字以上のランダムな文字列を作成する。
- 標準の英数字および特殊文字を使用できる。

- 最大 128 文字の長さの共有秘密を使用できる。サーバと RADIUS クライアントを総当たり攻撃から保護するには、22 文字を超える長い共有秘密を使用する。
- サーバと RADIUS クライアントを辞書攻撃から保護するために、共有秘密には数字や文字、句読点からなるランダムな文字列を使用し、頻繁に変更する。共有秘密には、表 6-5 に示す 3 つのグループの文字を含めるようにする。

表 6-5　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（文字や数字として定義されないものすべて）	感嘆符（!）、アスタリスク（*）、コロン（:）

共有秘密が強力なほど、共有秘密により暗号化されるアトリビュート（パスワード、暗号鍵として使用されるアトリビュートなど）のセキュリティがより強化されます。たとえば、8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(は、セキュアな共有秘密です。