セキュリティ

この章では、Cisco ONS 15454 SDH のユーザ 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 SDH Procedure Guide*』を参照してください。

この章では、次の内容について説明します。

9.1　ユーザ ID とセキュリティ レベル

ONS 15454 SDH システムにはユーザ ID CISCO15 が用意されていますが、このユーザ ID は Cisco Transport Controller（CTC）にサインインするときには求められません。この ID は、ほかの ONS 15454 SDH ユーザを設定する際に使用できます（ほかのユーザを設定する場合は、『*Cisco ONS 15454 SDH Procedure Guide*』の「Create Users and Assign Security」の手順に従ってください）。

1 台の ONS 15454 SDH 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 Transaction Language One（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。

- 取得 — CTC の情報を取得し、見ることができますが、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 SDH の Maintenance オプションだけにアクセスできます。
- プロビジョニング — Provisioning オプションおよび Maintenance 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 レベルに対するアイドル ユーザのタイムアウトについては、表 9-3（p.9-7）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。

9.2　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一覧表示します。また、Superuser がプロビジョニングの際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 タスク別のユーザ権限

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作業を示します。

表 9-1　ONS 15454 SDH 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]：作業	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	○	○	○	○
Conditions	—	Retrieve/Filter	○	○	○	○
History	Session	Filter	○	○	○	○
	Node	Retrieve/Filter	○	○	○	○
Circuits	—	Create/Edit/Delete	—	—	○	○
		Filter/Search	○	○	○	○
Provisioning	General	General: Edit	—	—	一部[1]	○
		Power Monitor: Edit	—	—	○	○
	Ether Bridge	Spanning trees: Edit	—	—	○	○
	Network	General: Edit	—	—	—	○
		General: View[2]	○	○	○	○
		Static Routing: Create/Edit/ Delete	—	—	○	○
		OSPF: Create/Edit/Delete	—	—	○	○
		RIP: Create/Edit/Delete	—	—	○	○
		Proxy: Create/Delete	—	—	—	○
		Firewall: Create/Delete	—	—	—	○
	OSI	Main Setup	—	—	—	○
		TARP	—	—	—	○
		Routers	—	—	—	○
		GRE Tunnel Routes	—	—	—	○
	MS-SPRing	Create/Edit/Delete	—	—	○	○
		Ring Map/Squelch Table/RIP Table	○	○	○	○
	Protection	Create/Delete/Edit	—	—	○	○
		View	○	○	○	○
	Security	Users: Create/Delete	—	—	—	○
		Users: Change password	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	—	—	—	○
		Policy: Edit	—	—	—	○
		Access: Edit	—	—	—	○
		RADIUS Server	—	—	—	○
		Legal Disclaimer: Edit	—	—	—	○

表 9-1　ONS 15454 SDH 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]：作業	取得	メンテナンス	プロビジョニング	スーパーユーザ
Provisioning	SNMP	Create/Delete/Edit	―	―	○	○
		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	―	○	○	○
		PCC: Create/Delete	―	―	○	○
	Timing	General: Edit	―	―	○	○
		BITS Facilities: Edit	―	―	○	○
	Alarm Profiles	Alarm Behavior: Edit	―	―	○	○
		Alarm Profiles Editor: Store/Delete[3]	―	―	○	○
		Alarm Profile Editor: New/Load/Compare/Available/Usage	○	○	○	○
	Cross-Connect	View	○	○	○	○
	Defaults	Edit/Import	―	―	―	○
		Reset/Export	○	○	○	○
	WDM-ANS	Provisioning: Edit/Import	―	―	―	○
		Provisioning: Reset/Export	○	○	○	○
		Connections: Create/Edit/Delete/Commit/ Calculate	―	―	○	○
		Port Status: Launch	―	―	○	○
Inventory	―	Delete	―	―	○	○
		Reset	―	○	○	○

表 9-1　ONS 15454 SDH 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]：作業	取得	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	—	—	—	○
	EtherBridge	Spanning Trees: View	○	○	○	○
		MAC Table: Retrieve	○	○	○	○
		MAC Table: Clear/Clear All	—	○	○	○
		Trunk Utilization: Refresh	○	○	○	○
		Circuits: Refresh	○	○	○	○
	OSI	IS-IS RIB				
		ES-IS RIB				
		TDC				
	MS-SPRing	Create/Edit/Delete	—	—	○	○
	Software	Download	—	○	○	○
		Upgrade/Activate/Revert	—	—	—	○
	Cross-Connect	Cards: Switch/Lock/Unlock	—	○	○	○
		Resource Usage: Delete	—	—	○	○
	Overhead XConnect	View	○	○	○	○
	Protection	Switch/Lock out/Lockon/ Clear/ Unlock	—	○	○	○
	Diagnostic	Retrieve/Lamp Test	—	○	○	○
	Timing	Source: Edit	—	○	○	○
		Report: View/Refresh	○	○	○	○
	Audit	Retrieve/Archive	—	—	—	○
	RIP Routing Table	Retrieve	○	○	○	○
	Routing Table	Retrieve	○	○	○	○
	Test Access	View	○	○	○	○
	DWDM	APC: Run/Disable/Refresh	—	○	○	○
		WDM Span Check: Retrieve Span Loss values, Reset	○	○	○	○
		ROADM Power Monitoring: Refresh	○	○	○	○

1. プロビジョニング担当者ユーザは、ノード名パラメータと連絡先パラメータを変更できません。
2. Retrieve、Maintenance、および Provisioning のユーザには、IP アドレスは表示されません。
3. サブタブの作業ボタンは、すべてのユーザに対してアクティブですが、所定のセキュリティ レベルを割り当てられているユーザだけが最後まで操作を行うことができます。

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作業を示します。

表 9-2　ONS 15454 SDH 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] : 作業	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	○	○	○	○
Conditions	—	Retrieve/Filter	○	○	○	○
History	—	Filter	○	○	○	○
Circuits	—	Create/Edit/Delete	—	—	○	○
		Filter/Search	○	○	○	○
Provisioning	Security	Users: Create/Delete	—	—	—	○
		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	—	—	—	○
		Policy: Change	—	—	—	○
	Alarm Profiles	Store/Delete[1]	—	—	○	○
		New/Load/Compare/Available/Usage	○	○	○	○
	MS-SPRing	Create/Delete/Edit/Upgrade	—	—	○	○
	Overhead Circuits	Create/Delete/Edit/Merge	—	—	○	○
		Search	○	○	○	○
	Provisionable Patchcords (PPC)	Create/ Delete	—	—	○	○
Maintenance	Software	Download/Cancel	○	○	○	○

1. サブタブの作業ボタンは、すべてのユーザに対してアクティブですが、所定のセキュリティ レベルを割り当てられているユーザだけが最後まで操作を行うことができます。

9.2.2　セキュリティ ポリシー

Superuser のセキュリティ権限を持つユーザは、ONS 15454 SDH にセキュリティ 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。また、Superuser は、ユーザが TCC2/TCC2P RJ-45 ポート、MIC-C/T/P LAN 接続、またはその両方から ONS 15454 SDH にアクセスできないようにすることができます。

9.2.2.1　アイドル ユーザのタイムアウト

ONS 15454 SDH 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 SDH Procedure Guide*』を参照してください。

表 9-3　ONS 15454 SDH のユーザのアイドル時間のデフォルト値

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	無制限

9.2.2.2　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、現在 CTC または TL1 にログインしているユーザのリストをノードごとにリアルタイムで表示できます。Superuser は、次のとおり、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使用 — Superuser は、パスワードの変更が必要な期限とパスワードが再使用可能になる期限を指定できます。
- ログイン試行回数 — Superuser は、ユーザが CTC にログイン試行できる回数の上限を指定できます。
- ユーザのロックアウトと無効化 — Superuser は、ユーザに許される無効なログインの回数（これ以降はロックアウトされる）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。
- ノード アクセスとユーザ セッション数 — Superuser 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ます。また、LAN または MIC-C/T/P 接続を使用した、ユーザの ONS 15454 SDH へのアクセスを禁止できます。

  また、Superuser 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。

9.3　監査証跡

ONS 15454 SDH は、TCC2/TCC2P 上に監査証跡ログを保持しています。この記録は、指定した期間内にシステムにアクセスした人物や実行された操作などを示します。ログには、システムのコマンドライン インターフェイス、CTC、および TL1 を用いた正規の Cisco ログインおよびログアウトが記録されます。ログには FTP の動作、回線の作成 / 削除、ユーザ / システムが発生させた動作の記録も含まれます。

イベントのモニタリングも監査ログに記録されます。イベントの定義は、ネットワーク内部の要素のステータスを変更するということです。外部イベント、内部イベント、アトリビュートの変更、ソフトウェアのアップロード / ダウンロード動作も監査証跡に記録されます。

監査証跡は、セキュリティの保持、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現に役立ちます。アカウンタビリティとは、プロセスやアクションを特定のユーザと関連付けて、ユーザの行動を追跡できるという意味です。監査証跡 ログを表示する方法については、『*Cisco ONS 15454 SDH Procedure Guide*』を参照してください。どの管理インターフェイス（CTC、CTM、TL1）からでも監査証跡 ログにアクセスできます。

監査証跡は不揮発性メモリに保存され、プロセッサの切り替え、リセット、またはアップグレードを行っても破損しません。ただし、TCC2/TCC2P が取り外されると、監査証跡 ログは消失します。

9.3.1　監査証跡ログのエントリ

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

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（そのアクションが実行されたかどうか）
Operation	実行したアクション

監査証跡の記録は、次のアクティビティをキャプチャします。

- User — その動作を実行しているユーザの名前
- Host — そのアクティビティが記録されたホスト
- Device ID — そのアクティビティに関わるデバイスの IP アドレス
- Application — そのアクティビティに関わるアプリケーションの名前
- Task — そのアクティビティに関わるタスクの名前（View a dialog［ダイアログの表示］、apply configuration [設定の適用] など）
- Connection Mode — Telnet、Console、SNMP
- Category — 変更の種類（Hardware、Software、Configuration）
- Status — ユーザの動作のステータス（Read、Initial、Successful、Timeout、Failed）
- Time — 変更時刻
- Message Type — イベントの種類に関する Success/Failure の表示
- Message Details — 変更の内容説明

9.3.2　監査証跡のキャパシティ

システムは 640 件のログ エントリを格納できます。この上限に達すると、最も古いエントリが新しいイベントに上書きされます。

ログ サーバの使用率が 80% になると、AUD-LOG-LOW 状態が発生して記録されます（CORBA/CTC による）。

ログ サーバが上限の 640 件に到達し、アーカイブされていない記録が上書きされると、AUD-LOG-LOSS 状態が発生して記録されます。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。ユーザがファイルをオフロードするまで、このイベントはシステムが上書きしたエントリの件数に関わりなく一度発生します。監査証跡 ログのエクスポートについては、『*Cisco ONS 15454 SDH 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、Remote Authentication Dial In User Service（RADIUS）認証を使用するためのノードを設定できます。シスコシステムズは、リモート ユーザの ID の検証、アクセスの許可、作業の追跡を実行する Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）と呼ばれる方法を使用します。

9.4.1　RADIUS 認証

RADIUS は、ネットワークとネットワーク サービスへのリモート アクセスを不正アクセスから保護する分散セキュリティ 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 を利用するフレーム形式を持つプロトコル
- サーバ
- クライアント

サーバは、通常はカスタマー サイトにある中央コンピュータで動作します。クライアントは、ダイヤルアップ アクセス サーバに常駐し、ネットワーク全体に分散することができます。

ONS 15454 SDH 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渡し、返された応答に基づいて対応します。RADIUS サーバは、ユーザ接続要求を受信し、ユーザを認証してから、そのユーザにサービスを配信するためにクライアントに必要な構成情報をすべて返します。RADIUS サーバは、その他の種類の認証サーバのプロキシ クライアントとしての役割を果たすこともできます。クライアントと RADIUS サーバ間のトランザクションは、ネットワークを通じて送信されることのない共有秘密を使用して認証されます。また、ユーザ パスワードはすべて、クライアントと RADIUS サーバ間で暗号化されて送信されます。これにより、セキュリティで保護されていないネットワークをスヌーピングしている何者かにユーザのパスワードを判別される可能性が解消されます。RADIUS 認証の実装方法に関する詳細については、『*Cisco ONS 15454 SDH Procedure Guide*』を参照してください。

9.4.2　共有秘密

共有秘密とは、次のそれぞれの間のパスワードとして機能するテキスト ストリングです。

- 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の場合、RADIUS クライアントおよび RADIUS プロキシ間で使用される共有秘密と、RADIUS プロキシおよび RADIUS サーバ間で使用される共有秘密をそれぞれ別のものにすることができます。

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、RADIUS メッセージが中継点（メッセージ インテグリティ）で変更されていないかを検証します。さらに、共有秘密は User-Password と Tunnel-Password などの一部の RADIUS アトリビュートを暗号化するのに使用されます。

共有秘密を作成および使用する場合、次のようにしてください。

- 両方の RADIUS デバイスで大文字と小文字を区別した同じ共有秘密を使用します。
- RADIUS サーバと RADIUS クライアントの各ペアに対しては異なる共有秘密を使用します。
- 確実にランダムな共有秘密にするには、ランダムな文字列を最低 22 文字の長さで生成してください。
- 任意の標準英数字と特殊文字を使用できます。
- 最大 128 文字の長さの共有秘密を使用できます。Brute-Force アタックからサーバと RADIUS クライアントを保護するには、22 文字を超える長い共有秘密を使用してください。
- 辞書攻撃からサーバと RADIUS クライアントを保護するために、共有秘密を文字、数字、および句読点からなるランダムな文字列にし、頻繁に変更してください。共有秘密には、表 9-5 に一覧表示される 3 グループのそれぞれの文字が含まれる必要があります。

表 9-5　共有秘密文字のグループ

グループ	例
文字（大文字と小文字）	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ないすべての文字）	感嘆符（!）、アスタリスク（*）、コロン（:）

共有秘密が強力なほど、共有秘密によって暗号化されるアトリビュート（たとえば、パスワードと暗号鍵に使用されるアトリビュート）が保護されます。強力な共有秘密の一例として、「8d#>9fq4bV)H7%a3-zE13sW$hIa32M#m<PqAa72(」が挙げられます。