CHAPTER 3

# ユーザ アクセスの管理

この章では、ユーザ プロファイルの作成によって Cisco Guard（Guard）へのアクセスを制御する方法について説明します。ユーザが WBM にログインしようとすると、Guard がログイン ユーザ名とパスワードをユーザ プロファイル データベースと照合して、認証します。

ここでは、Guard の付属製品である Cisco Traffic Anomaly Detector（Detector）について説明します。Detector は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃検出デバイスで、ゾーンのトラフィックのコピーを分析します。Detector は、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector はゾーンの設定を Guard と同期させることもできます。Detector の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』および『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

この章は、次の項で構成されています。

# ユーザの認証および認可の方式について

CLI を使用して Guard をどのように設定したかに応じて、Guard は次のいずれかまたは両方の方式を使用して、ユーザを認証および認可します。

- ローカル：ユーザ名とパスワードを自身の内部データベースと照合して認証します。ユーザ名ごとに、定義済みの一連のコマンドの実行をユーザに許可するためのユーザ特権レベルを、システム管理者が設定できます。

  ローカルでの認証および認可の方式がデフォルトです。ローカルでのユーザの認証および認可は、WBM を使用して設定します。

- AAA（認証、認可、アカウンティング）：1 つまたは複数の Terminal Access Controller Access Control System Plus（TACACS+）サーバに常駐している外部データベースと照合してユーザ名とパスワードを認証します。AAA 認証では、コマンドごとにアクセス権を指定できます。AAA サービスは、ユーザの認証と認可を設定する機能のほかに、アカウンティングを設定する機能も備えています。この機能を使用すると、デバイスのイベントを追跡できます。たとえば、ユーザが開始したイベント（Guard の設定変更など）を追跡できます。

  Guard 上で AAA サービスをイネーブルにして TACACS+ サーバを定義するには、CLI を使用する必要があります（『*Cisco Guard Configuration Guide*』を参照）。

# 定義済みのシステム ユーザ プロファイルの使用

Guard では、次の 2 つのシステム ユーザ プロファイルがローカル データベース上に事前設定されています。

- admin：このデフォルトのユーザ名は、Guard 上で CLI に最初にアクセスするときに使用します。初めて Guard にログインしたときは、admin ユーザ プロファイルにパスワードを割り当てます。管理者としてログインすると、すべての CLI コマンドおよび WBM のウィンドウにアクセスできます。Guard を設定し、他のユーザ プロファイルを作成する場合は、admin ユーザ プロファイルを使用します。
- riverhead：Detector は、Guard に最初にアクセスして双方の間に通信チャネルを確立するときに、ユーザ名 riverhead を使用します。初めて Guard にログインしたときは、riverhead ユーザ プロファイルにパスワードを割り当てます。Detector と Guard の間に最初の通信リンクが確立されると、2 つのデバイスは、以後の通信リンクを確立するときに秘密鍵と公開鍵のペアを使用します。このため、ユーザの操作は必要なくなります。riverhead システム ユーザ プロファイルには、Dynamic ユーザ特権レベルが設定されています。

システム ユーザのパスワードは変更できますが、Guard のデータベースからシステム ユーザを削除することはできません。

**（注）** 初期設定が完了した後は、ユーザのアクションを監視できるように新しいアカウントを作成し、システム ユーザ アカウントは使用しないことをお勧めします。

# ユーザ リストの表示

WBM では、ローカル ユーザ データベースに定義されているユーザのリストを表示できます。ユーザ リストでは、ユーザ プロファイルを追加または削除できます。ユーザ リストは、次の 2 つのカテゴリに分かれています。

- **System users**：シスコによってあらかじめ定義されているユーザ プロファイル。削除することはできません（「定義済みのシステム ユーザ プロファイルの使用」の項を参照）。
- **Users**：システム管理者が定義するユーザ プロファイル。

ローカル ユーザ データベースに定義されているユーザのリストを表示するには、次の手順を実行します。

**ステップ 1**　ナビゲーション ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

**ステップ 2**　Guard の要約メニューから **Users > Users list** を選択します。ユーザ リストが表示されます。

# ユーザ プロファイルの作成

ローカル データベースにユーザ プロファイルを作成するには、管理者アクセス権が必要です。

（注）　Guard が、ユーザの認証に認証用のローカル サービスと AAA サービス（または AAA サービスのみ）を使用するように設定されている場合は、認証に使用されるユーザ プロファイル情報も、各 TACACS+ サーバ上で設定する必要があります（「TACACS+ サーバ上でのユーザ プロファイルの設定」の項を参照）。

新しいユーザ プロファイルを作成するには、次の手順を実行します。

**ステップ 1**　ナビゲーション ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

**ステップ 2**　次のいずれかの方法で、Create User 画面を表示します。

- Guard の要約メニューから **Users > Create user** を選択します。
- Guard の要約メニューから **Users > Users list** を選択し（*Users List* が表示されます）、**Add** をクリックします。

**ステップ 3**　表 3-1 の説明に従って、ユーザ プロファイルのパラメータを定義します。

**表 3-1　ユーザ プロファイルのパラメータ**

| パラメータ | 説明 |
|---|---|
| User name | ユーザ プロファイルの名前。アルファベットで始まる 1 ～ 63 文字の英数字の文字列を入力します。大文字と小文字は区別されます。文字列にスペースを含めることはできませんが、アンダースコア（_）を含めることはできます。 |
| Initial password | ユーザのパスワード。スペースを含まない 6 ～ 24 文字の文字列を入力します。大文字と小文字は区別されます。 |
| Type | ユーザの特権レベル。次のユーザ特権レベルのいずれかを Type ドロップダウン リストから選択します。<br>• show：監視操作と診断操作にアクセスできます。<br>• dynamic：監視と診断、保護、およびラーニングに関する操作にアクセスできます。Dynamic 特権を持つユーザは、フレックスコンテンツ フィルタと動的フィルタを設定することもできます。<br>• config：ユーザ プロファイルの管理を除くすべての WBM 機能にフル アクセスできます。<br>• admin：すべての WBM 機能にフル アクセスできます。 |

**ステップ 4**　次のいずれかのオプションを選択します。

- **OK**：ユーザ プロファイル情報をローカル データベースに保存します。ユーザの詳細画面が表示され、新しいユーザ プロファイルのパラメータが示されます。
- **Clear**：User フォームに追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Create User 画面を終了します。ユーザ リストが表示されます。

# ユーザ プロファイルの削除

ユーザ プロファイルを削除すると、ローカル ユーザ データベースだけを使用して認証を実行する場合に、関連付けられたユーザが Guard にアクセスできなくなります。

ユーザ プロファイルを削除するには、次の手順を実行します。

**ステップ 1**　ナビゲーション ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

**ステップ 2**　Guard の要約メニューから **Users > Users list** を選択します。ユーザ リストが表示されます。

**ステップ 3**　削除するユーザ名の隣にあるチェックボックスをオンにし、**Delete** をクリックします。表示されているユーザ名をすべて削除するには、**User** チェックボックスをオンにし、**Delete** をクリックします。削除の確認メッセージが表示されます。

**ステップ 4**　次のいずれかのオプションを選択します。

- **OK** : ユーザ プロファイルをローカル データベースから削除します。ユーザ リストが表示されます。
- **Cancel**：ユーザ削除要求を無視します。ユーザ リストが表示されます。

# パスワードの変更

ユーザは、自分のパスワードを変更できます。管理者は、自分のパスワードと他のユーザのパスワードを変更できます（「別のユーザのパスワードの変更」の項を参照）。

自分のパスワードを変更するには、次の手順を実行します。

**ステップ 1**　ナビゲーション ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

**ステップ 2**　Guard の要約メニューから **Users > Change Password** を選択します。**Change Password** 画面が表示されます。

**ステップ 3**　現在のパスワードを **Old Password** フィールドに入力します。

**ステップ 4**　新しいパスワードを **New Password** フィールドに入力します。パスワードは、スペースを含まない 6 ～ 24 文字の文字列とします。大文字と小文字は区別されます。

**ステップ 5**　Confirm New Password フィールドに新しいパスワードを再入力します。

**ステップ 6**　次のいずれかのオプションを選択します。

- **OK**：新しいパスワードを Guard のデータベースのユーザ プロファイルに保存します。Guard の要約画面が表示されます。
- **Cancel**：情報を保存せずに **Change Password** 画面を終了します。Guard の要約画面が表示されます。

現在無効になっているパスワードが入力された場合、Guard は新しいパスワードを確認できないため、エラー メッセージを表示します。**Go Back** をクリックして手順を繰り返してください。

# 別のユーザのパスワードの変更

admin ユーザ特権レベルを持つユーザは、他のユーザのパスワードを変更できます。

他のユーザのパスワードを変更するには、次の手順を実行します。

**ステップ 1**　ナビゲーション ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

**ステップ 2**　Guard の要約メニューから **Users > Change Password** を選択します。**Change Password** 画面が表示されます。

**ステップ 3**　ユーザ名をクリックします。ユーザの詳細画面が表示されます。

**ステップ 4**　**Config** をクリックします。Config User 画面が表示されます。

**ステップ 5**　新しいパスワードを入力します。パスワードは、スペースを含まない 6 ～ 24 文字の文字列とします。大文字と小文字は区別されます。

**ステップ 6**　次のいずれかのオプションを選択します。

- **OK**：新しいパスワードをローカル データベースのユーザ プロファイルに保存します。User List 画面が表示されます。
- **Clear**：User フォームに追加した情報をすべて消去します。
- **Cancel**：情報を保存せずに Config User 画面を終了します。User List 画面が表示されます。

# ユーザ特権レベルの変更

ユーザは、ユーザ特権レベルを変更できます。

ユーザ特権レベルを変更するには、次の手順を実行します。

**ステップ 1**　情報領域で **Enable** をクリックします。

Enable Authentication ウィンドウが表示されます。

**ステップ 2**　Level ドロップダウン リストから、目的のユーザ特権レベルを選択します。特権レベルは次のいずれかです。

- admin：すべての WBM 機能にフル アクセスできます。
- config：ユーザ プロファイルの管理を除くすべての WBM 機能にフル アクセスできます。
- dynamic：監視と診断、保護、およびラーニングに関する操作にアクセスできます。Dynamic 特権を持つユーザは、フレックスコンテンツ フィルタと動的フィルタを設定することもできます。

**ステップ 3**　Password フィールドに特権レベル パスワードを入力します。

**ステップ 4**　**OK** をクリックして変更を適用します。

# TACACS+ サーバ上でのユーザ プロファイルの設定

この項の情報は、TACACS+ サーバ上で WBM ユーザ プロファイル情報を設定する必要のある管理者を対象としています。TACACS+ サーバと AAA サービスを使用して WBM へのユーザ アクセスを管理するには、Guard の CLI を使用して AAA サービスをイネーブルにし、Guard で TACACS+ サーバを定義する必要があります（『*Cisco Guard Configuration Guide*』を参照）。

（注）　TACACS+ アカウンティングをイネーブルにすると、記録された各イベントにタスク識別（task_id）番号が割り当てられます。WBM イベントの場合、task_id には、40000 から順に番号が付けられます。

TACACS+ サーバ上にユーザ認可を設定すると、ユーザ アクセスを特定のゾーンおよび WBM 機能に制限できます。

（注）　コマンドは、すべて大文字と小文字が区別されます。

この項は、次の内容で構成されています。

- WBM ポータルの管理による特定ゾーンへのユーザ アクセスの制限
- 特定の WBM コマンドへの認可の管理

## WBM ポータルの管理による特定ゾーンへのユーザ アクセスの制限

WBM ポータルをカスタマイズして、ユーザが表示およびアクセスできるゾーンを制限できます。これには、**ShowZonePortal** コマンドと **zone_name** アトリビュートを使用して TACACS+ サーバを設定します。

注意　**ShowGuardPortal** および **ShowZonesList** は、WBM の基本的なナビゲーションを可能にする必須のコマンドです。これらは常に **permit** に設定しておく必要があります。

たとえば、次の TACACS+ サーバの設定では、デバイス上に設定されたゾーン数に関係なく、ユーザ ABC はゾーン ABC_1 および ABC_2 にのみアクセス権を付与されています。

```
user = ABC {
        default service=permit
        login=cleartext 123456

cmd = ShowZonePortal {
        permit "zone_name_ABC_1"
        permit "zone_name_ABC_2"
        deny .*
     }

cmd = ShowDetectorPortal {
        permit .*
     }

cmd = ShowZonesList {
        permit .*
     }
}
```

## 特定の WBM コマンドへの認可の管理

WBM のメニュー項目と機能ボタンには、それぞれコマンドが対応付けられています。管理者は、特定のユーザが特定のメニュー項目や機能ボタンにアクセスすることを認可するかどうかを制御できます。

**注意**　認可を使用して各 WBM コマンドへのユーザ アクセスを管理すると、Guard のアドレスとの間を行き来するトラフィックの量が大幅に増加します。このトラフィックの増加が、Guard の tcp_outgoing_ns 自己保護ポリシーのトリガーとなる場合があります。この問題を回避するため、これらのポリシーのしきい値を上げることをお勧めします（『*Cisco Guard Configuration Guide*』を参照）。

表 3-2 は、WBM 機能へのユーザ アクセスを管理するために TACACS+ サーバに設定可能な WBM コマンドを示しています。

**表 3-2　TACACS+ でサポートされる WBM の操作**

| 特権レベル | 機能 | コマンド |
|---|---|---|
| Admin | ユーザ管理 | ShowUserList |
| | | AddUser |
| | | DeleteUser |
| | | ShowUserDetails |
| | | ConfigUser |
| Config | 作成 / 追加 | CreateUserFilter |
| | | CreateBypassFilter |
| | | CreateZone |
| | | CreateZoneTemplate |
| | | AddZoneIP |
| | | AddPolicyThreshold |
| | | AddService |
| | 削除 | DeleteZones |
| | | DeleteZoneIP |
| | | DeleteZoneTemplate |
| | | DeleteReports |
| | | DeleteUserFilters |
| | | DeleteBypassFilters |
| | | DeletePacketDump |
| | | DeleteSnapshot |
| | | DeletePolicyThreshold |
| | | RemoveService |
| | | ClearCounters |
| | エクスポート | ExportReports |
| | | SetFtpServer |

表 3-2　TACACS+ でサポートされる WBM の操作（続き）

| 特権レベル | 機能 | コマンド |
|---|---|---|
| Config（続き） | ラーニング | StartProtect&Learn |
| | | StartPolicyConstruction |
| | | StopPolicyConstruction |
| | | StartThresholdTuning |
| | | StopThresholdTuning |
| | | AcceptPolicyConstruction |
| | | AcceptThresholdTuning |
| | | CreateSnapshot |
| | | DeleteSnapshot |
| | | RejectResults |
| | | NoLearningAccept |
| | | NoLearningReject |
| | | SavePoliciesRecommendations |
| | 設定 | ConfigExtendedFlexFilter |
| | | ConfigWormSrcIPs |
| | | ConfigPolicies |
| | | ConfigPolicyTemplate |
| | | ConfigZone |
| | | ConfigLearn |
| | | ConfigPolicy |
| | | ConfigPolicyGroup |
| | | ConfigPolicyThreshold |
| | | ChangePolicyState |
| | | RecommendationAcceptForever |
| | | SaveAsZone |

表 3-2　TACACS+ でサポートされる WBM の操作（続き）

| 特権レベル | 機能 | コマンド |
|---|---|---|
| Dynamic | 作成 / 追加 / 削除 | CreateExtendedFlexFilter |
| | | DeleteExtendedFlexFilter |
| | | CreateDynamicFilter |
| | | DeleteAllDynamicFilters |
| | | DeleteDynamicFilters |
| | | RecommendationIgnore |
| | | RecommendationAccept |
| | 被害によるアクティブ化 | protectIP |
| | | StartProtection |
| | | StopProtection |
| | | ActivatePolicy |
| | | DeactivatePolicy |
| | | AcceptPendingDynFilter |
| | パケットダンプ | StartPacketDump |
| | | StopPacketDump |
| | | SavePacketDump |
| | | RenamePacketDump |
| | | CopyPacketDump |
| | | ExportPacketDump |
| | | ImportPacketDump |

表 3-2　TACACS+ でサポートされる WBM の操作（続き）

| 特権レベル | 機能 | コマンド |
|---|---|---|
| Show | パスワード/ログイン/ログアウト | UserLogin |
| | | UserLogout |
| | | EnableUser |
| | | ChangePassword |
| | 表示 | ShowGuardPortal |
| | | ShowGuardCounters |
| | | ShowGuardRealtimeCounters |
| | | ShowGuardLog |
| | | ShowZoneList |
| | | ShowTemplateList |
| | | ShowPolicyComparison |
| | | ShowZonePortal |
| | | ShowZoneCounters |
| | | ShowRealtimeCounters |
| | | ShowZoneLog |
| | | ShowAttacksSummary |
| | | ShowAttack |
| | | ShowAttackDetails |
| | | ShowZombiesAttack |
| | | ShowPolicyStatistics |
| | | ShowDropStatistics |
| | | ShowPacketDumpList |
| | | ShowCaptureAnalysis |
| | | ShowDynamicFilters |
| | | ShowDynamicFilterDetails |
| | | ShowPendingRecommendations |
| | | ShowPendingFilters |
| | | ShowSnapshotList |
| | | ShowGeneralConfiguration |
| | | ShowUserFilters |
| | | ShowBypassFilters |
| | | ShowFlexContentFilters |
| | | ShowPolicyTemplate |
| | | ShowPolicies |
| | | ShowPolicyDetails |
| | | ShowLearningParams |
| | | ShowPolicyComparison |
| | | ShowSignatureExtraction |
| | | ShowVersion |

次の TACACS+ サーバの例は、Customer A ユーザに次のゾーンと機能へのアクセス認可を設定する方法を示しています。

- ゾーン A1 および A2 のみ。
- 次の診断機能を除くすべての WBM 機能
  - Guard counters
  - Real time counters
  - Show logs

```
    key = 12345
    default authentication = file /etc/passwd
    accounting file = /var/log/tacacs.log
    default authorization = permit

user = Customer_A {
        default service=permit
        service=connection {}
        login=cleartext 1234

cmd = ShowZonePortal {
        permit "zone_name_zone_A1"
        permit "zone_name_zone_A2"
        deny .*
     }
cmd = ShowGuardCounters {
        deny .*
     }

cmd = ShowGuardRealtimeCounters {
        deny .*
     }

cmd = ShowGuardLog {
        deny .*
        }
     }
```