CHAPTER 13

管理タスクの分散

管理タスクの分散について

ユーザ アカウントに割り当てたユーザ ロールに基づいて、他のユーザにシスコのコンテンツ セキュリティ管理アプライアンスの管理タスクを分散できます。

管理タスクが分散されるように設定するには、事前定義されたユーザ ロールがニーズを満たしているかどうかを判断して、必要なカスタム ユーザ ロールを作成します。次に、セキュリティ アプライアンスでローカルに管理ユーザの認証を行う、および（または）独自の中央集中型の LDAP や RADIUS システムを使用して外部で管理ユーザの認証を行うようにアプライアンスを設定します。

さらに、アプライアンスおよびアプライアンス上の特定の情報へのアクセスに追加の制御を指定できます。

ユーザ ロールの割り当て

セキュリティ管理アプライアンスには、電子メールと Web セキュリティ アプライアンスのモニタリングおよび管理を行うための、事前定義ユーザ ロールとカスタム ユーザ ロールの両方が用意されています。

事前定義ユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザ ロール、またはカスタム ユーザ ロールを各ユーザに割り当てることができます。

表 13-1　ユーザ ロールの説明

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
admin	**admin** ユーザはシステムのデフォルト ユーザ アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザ アカウントをここに記載しましたが、これはユーザ ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。 **resetconfig** コマンドと **revert** コマンドを発行できるのは、**admin** ユーザだけです。	あり / あり
Administrator	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。	あり / あり
Operator	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザ アカウントの作成または編集 • アプライアンスのアップグレード • `resetconfig` コマンドの発行 • システム セットアップ ウィザードの実行 • ユーザ名とパスワード以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対してイネーブルになっている場合）。 • 隔離の設定、編集、削除、または集約。 これら以外は、Administrator ロールと同じ権限を持ちます。	あり / あり
Technician	Technician ロールを持つユーザ アカウントは、アップグレードおよびリブート、アプライアンスからのコンフィギュレーション ファイルの保存、ライセンス キーの管理などのシステム管理アクティビティを開始できます。	[メール（Email）] タブに表示されるシステム キャパシティ レポートへのアクセス
Read-Only Operator	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために大部分の変更を行って送信できますが、保存できません。または保存を必要としない変更を行うことができます。このロールのユーザは、アクセスが有効な場合、隔離内のメッセージを管理できます。 このロールのユーザは、以下にはアクセスできません。 • ファイル システム、FTP、SCP。 • 隔離を作成、編集、削除、または集中管理するための設定。	あり / なし

表 13-1　ユーザ ロールの説明 （続き）

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
Guest	ゲスト ロールを持つユーザ アカウントは、アクセス権限が有効であれば、隔離内のメッセージのステータス情報を確認し管理できます。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。	あり / なし
Web Administrator	Web Administrator ロールを持つユーザ アカウントは、[Web] タブに表示されるすべての設定に対するアクセス権を持ちます。	あり / あり
Web Policy Administrator	Web Policy Administrator ロールを持つユーザ アカウントは、[Web アプライアンス ステータス（Web Appliance Status）] ページと、Configuration Master のすべてのページにアクセスできます。Web ポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシ バイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Web ポリシー管理者は、設定を公開できません。	なし / なし
URL Filtering Administrator	URL Filtering Administrator ロールを持つユーザ アカウントは、URL フィルタリングだけを設定できます。	なし / なし
Email Administrator	メール管理者ロールを持つユーザ アカウントは、隔離など、[メール（Email）] メニューにあるすべての設定へのアクセス権のみを持ちます。	なし / なし

表 13-1　ユーザ ロールの説明 （続き）

ユーザ ロール名	説明	Web レポーティング / 定期レポート機能
Help Desk User	Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • 隔離内のメッセージ管理 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。ユーザにこのロールを割り当てた後、このユーザがアクセスできるように隔離を設定する必要があります。	なし / なし
カスタム ロール	カスタム ユーザ ロールに割り当てられているユーザ アカウントは、ポリシー、機能、またはこのロールに特に与えられた特定のポリシーまたは機能インスタンスに対してのみ、表示および設定を行えます。 新しい Custom Email User ロールまたは新しい Custom Web User ロールは、[ローカル ユーザの追加（Add Local User）] ページから作成できます。ただし、ロールを使用できるようにするには、このカスタム ユーザ ロールに権限を割り当てる必要があります。権限を割り当てるには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] に移動して、ユーザ名をクリックします。 **（注）** Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。 詳細については、「カスタム ユーザ ロール」（P.13-5）を参照してください。	なし / なし

一部のロール（Administrator、Operator、Guest、Technician、および Read-Only Operator）は、GUI と CLI の両方にアクセスできます。他のロール（Help Desk User、Email Administrator、Web Administrator、Web Policy Administrator、URL Filtering Administrator、およびカスタム ユーザ）は GUI だけにアクセスできます。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「外部ユーザ認証」（P.13-18）を参照してください。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）および「ポリシー隔離の作成」（P.8-12）を参照してください。

カスタム ユーザ ロール

Administration 権限を持つユーザは、セキュリティ管理アプライアンスを使用してカスタム ロールに管理権限を委任できます。カスタム ロールは、事前定義されたユーザ ロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザ ロールを割り当てたユーザは、アプライアンス、機能、またはエンド ユーザのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザ ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、以下を参照してください。

- 「Custom Email User ロールについて」（P.13-5）
- 「Custom Web User ロールについて」（P.13-9）
- 「カスタム ユーザ ロールの削除」（P.13-11）

Custom Email User ロールについて

カスタム ロールを割り当てると、委任された管理者が セキュリティ管理アプライアンスにある次の項目にアクセスすることを許可できます。

- すべてのレポート（オプションでレポーティング グループによって制限）
- メール ポリシー レポート（オプションでレポーティング グループによって制限）
- DLP レポート（オプションでレポーティング グループによって制限）
- メッセージ トラッキング
- 隔離

これらの各項目の詳細については、以下のセクションで説明します。また、これらの権限を付与されたすべてのユーザは、[管理アプライアンス（Management Appliance）] タブ > [集約管理サービス（Centralized Services）] メニューを使用して、[システム ステータス（System Status）] を表示できます。Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。

（注）　電子メール セキュリティ アプライアンスのカスタム ユーザ ロールは、セキュリティ管理アプライアンスのユーザ ロールよりも、より詳細なアクセス権を提供します。たとえば、メールおよび DLP ポリシーと、コンテンツ フィルタへのアクセス権を委任できます。詳細については、お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Common Administration」の章の「Managing Custom User Roles for Delegated Administration」のセクションを参照してください。

電子メール レポーティング

次のセクションで説明するように、電子メール レポートへのアクセス権をカスタム ユーザ ロールに付与できます。

セキュリティ管理アプライアンスの [メール セキュリティ モニタ（Email Security Monitor）] ページの詳細については、「中央集中型電子メール セキュリティ レポーティングの使用」の該当する章を参照してください。

すべてのレポート

カスタム ロールにすべてのレポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- 概要（Overview）
- 受信メール（Incoming Mail）
- 送信先（Outgoing Destinations）
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ（Internal Users）
- DLP インシデント（DLP Incidents）
- コンテンツ フィルタ（Content Filters）
- ウイルス タイプ（Virus Types）
- TLS 接続（TLS Connections）
- アウトブレイク フィルタ（Outbreak Filters）
- システム容量（System Capacity）
- 有効なレポート データ（Reporting Data Availability）
- 定期レポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

メール ポリシー レポート（Mail Policy Reports）

カスタム ロールにメール ポリシー レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- 概要（Overview）
- 受信メール（Incoming Mail）
- 送信先（Outgoing Destinations）
- 送信メッセージ送信者（Outgoing Senders）
- 内部ユーザ（Internal Users）
- コンテンツ フィルタ（Content Filters）
- ウイルス タイプ（Virus Types）
- アウトブレイク フィルタ（Outbreak Filters）
- 有効なレポート データ（Reporting Data Availability）
- アーカイブ レポート（Archived Reports）

DLP レポート（DLP Reports）

カスタム ロールに DLP レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての 電子メール セキュリティ アプライアンス、または選択したレポーティング グループのいずれかに対する、次の [メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

- DLP インシデント（DLP Incidents）

- 有効なレポート データ（Reporting Data Availability）
- アーカイブ レポート（Archived Reports）

メッセージ トラッキング（Message Tracking）

カスタム ロールにメッセージ トラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザは、セキュリティ管理アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.13-24）を参照してください。

セキュリティ管理アプライアンスでメッセージ トラッキングへのアクセスをイネーブルにするためのアプライアンスの設定方法など、メッセージ トラッキングの詳細については、「電子メール メッセージのトラッキング」を参照してください。

隔離

カスタムロールに隔離へのアクセス権を付与すると、このロールを割り当てられたユーザは、このセキュリティ管理アプライアンスのすべての隔離メッセージを検索、表示、リリース、または削除できます。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。「「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）」、「「ポリシー隔離の作成」（P.8-12）」、および「「カスタム ユーザ ロールの集約隔離アクセスの設定」（P.8-8）」を参照してください。

セキュリティ管理アプライアンスからこの隔離へのアクセスをイネーブルにするためのアプライアンスの設定方法など、スパム隔離の詳細については、「Cisco IronPort スパム隔離の管理」の章を参照してください。

Custom Email User ロールの作成

電子メール レポーティング、メッセージ トラッキング、および隔離へのアクセスに対して、カスタムのメール ユーザ ロールを作成できます。

これらの各オプションに許可されたアクセス権の詳細については、Custom Email User ロールについてとそのサブセクションを参照してください。

（注） より詳細なアクセス権、または他の機能、レポート、ポリシーへのアクセス権を付与するには、各 電子メール セキュリティ アプライアンスで直接カスタム ユーザ ロールを作成してください。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] を選択します。

ステップ 2　[メール ユーザ ロールの追加（Add Email User Role）] をクリックします。

ヒント または、既存の Email User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 3　ユーザ ロールの一意の名前（たとえば「dlp-auditor」）と説明を入力します。

- Email と Web のカスタム ユーザ ロール名を同じにしないでください。
- 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュまたは数字にすることはできません。
- このロールのユーザに集約ポリシー隔離へのアクセス権限を許可し、このロールのユーザが電子メール セキュリティ アプライアンスのメッセージ フィルタやコンテンツ フィルタおよび DLP メッセージ アクション内にもこれらの集約隔離を指定できるようにする場合、カスタム ロールの名前を両方のアプライアンスで同じにする必要があります。

ステップ 4　このロールに対してイネーブルにするアクセス権限を選択します。

ステップ 5　[送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

ステップ 6　レポーティング グループごとにアクセス権を制限する場合は、該当するユーザ ロールの [メール レポート（Email Reporting）] カラムにある [グループが選択されていません（no groups selected）] リンクをクリックして、少なくとも 1 つのレポーティング グループを選択します。

ステップ 7　変更を保存します。

ステップ 8　このロールに隔離へのアクセス権を付与する場合は、このロールに対してアクセス権を有効にします。

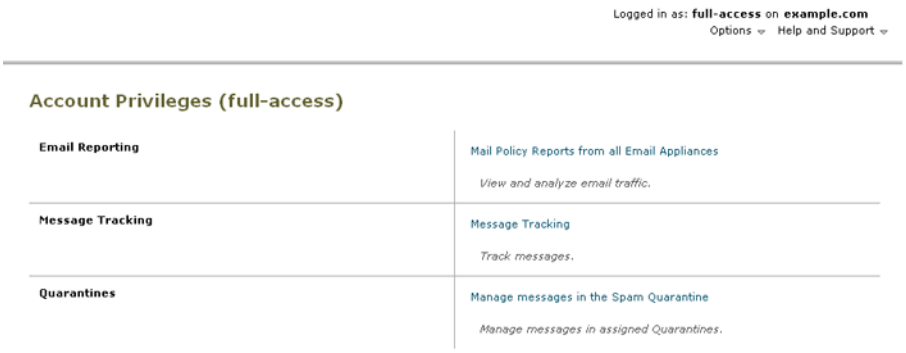
次を参照してください。

- 「Cisco IronPort スパム隔離への管理者ユーザ アクセスの設定」（P.7-8）。
- 「ポリシー隔離の作成」（P.8-12）.

Custom Email User ロールの使用

Custom Email User ロールに割り当てられているユーザがアプライアンスにログインすると、そのユーザには、ユーザがアクセス権を持つセキュリティ機能へのリンクだけが表示されます。そのユーザは、[オプション（Options）] メニューで [アカウント権限（Account Privileges）] を選択することで、いつでもこのメインページに戻ることができます。これらのユーザは、Web ページの上部にあるメニューを使用して、アクセス権を持つ機能にアクセスすることもできます。次の例では、ユーザは Custom Email User ロールによって、セキュリティ管理アプライアンスで使用可能なすべての機能へのアクセス権を持ちます。

図 13-1　Custom Email User ロールが割り当てられている委任管理者の [アカウント権限（Account Privileges）] ページ



Custom Web User ロールについて

Custom Web User ロールでは、ユーザがポリシーを別の Web セキュリティ アプライアンスに公開することができ、カスタム設定を編集したり、別のアプライアンスに公開できるようになります。

セキュリティ管理アプライアンスの [Web] > [設定マスター（Configuration Master）] > [カスタム URL カテゴリ（Custom URL Categories）] ページでは、管理および公開できる URL カテゴリとポリシーを表示できます。また、[Web] > [ユーティリティ（Utilities）] > [今すぐ設定を公開する（Publish Configuration Now）] ページに移動して、可能な設定を表示することもできます。

（注） 公開権限を持つカスタム ロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。つまり、どのカテゴリまたはポリシーも公開または管理できないユーザを作ってしまうことになります。

この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタム カテゴリを作成し、そのユーザに、そのカスタム カテゴリを管理する権限と公開する権限を付与する**必要があります**。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- Custom Web User ロールの作成
- Custom Web User ロールの編集

Custom Web User ロールの作成

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ ロール（User Roles）] を選択します。

ステップ 2　[Web ユーザ ロールの追加（Add Web User Role）] をクリックします。

ヒント または、既存の Web User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複（Duplicate）] アイコンをクリックし、生成されたコピーを編集します。

ステップ 3　ユーザ ロールの一意の名前（たとえば「canadian-admins」）と説明を入力します。

（注） 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュにすることはできません。

ステップ 4　デフォルトで、ポリシーとカスタム URL カテゴリを表示するか、非表示にするかを選択します。

ステップ 5　公開権限をオンにするか、オフにするかを選択します。

この権限を持つユーザは、ユーザがアクセス ポリシーまたは URL カテゴリを編集できるすべての Configuration Master を公開できます。

ステップ 6　新しい（空の）設定で始めるか、既存のカスタム ユーザ ロールをコピーするかを選択します。既存のユーザ ロールをコピーする場合は、コピーするロールをリストから選択します。

ステップ 7　[送信（Submit）] をクリックして [ユーザ ロール（User Roles）] ページに戻ると、新しいユーザ ロールが表示されます。

（注） Web レポーティングで匿名機能をイネーブルにしていた場合、Web レポーティングへのアクセス権を持つすべてのユーザ ロールには、インタラクティブなレポート ページで認識できないユーザ名とロールが表示されるようになります。第 5 章「中央集中型 Web レポーティングおよびトラッキングの使用」の Web レポートのスケジュール設定のセクションを参照してください。Administrator ロールの場合は例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよび Web 管理者によって作成されたスケジュール設定されたレポートは匿名になります。

（注） [Web] > [ユーティリティ（Utilities）] > [セキュリティ サービス表示（Security Services Display）] > [セキュリティ サービス表示の編集（Edit Security Services Display）] ページを使用して Configuration Master の 1 つを非表示にしている場合、[ユーザ ロール（User Roles）] ページでも対応する [設定マスター（Configuration Master）] カラムが非表示になりますが、非表示になっている Configuration Master に対する権限設定は保持されます。

Custom Web User ロールの編集

手順

ステップ 1　[ユーザ ロール（User Roles）] ページでロール名をクリックし、[ユーザ ロールの編集（Edit User Role）] ページを表示します。

ステップ 2　名前、説明、およびポリシーとカスタム URL カテゴリを表示するかどうかなどの設定を編集します。

ステップ 3　[送信（Submit）] をクリックします。

カスタム ユーザ ロールの権限を編集するには、次の手順を実行します。

[ユーザ ロール（User Roles）] ページに移動します。

- アクセス ポリシー権限を編集するには、[アクセス ポリシー（Access policies）] をクリックして、Configuration Master に設定されているアクセス ポリシーのリストを表示します。[含める（Include）] カラムで、ユーザ編集アクセス権を付与するポリシーのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザ ロール（User Roles）] ページに戻ります。

または

- カスタム URL カテゴリ権限を編集するには、カスタム URL カテゴリをクリックして、Configuration Master に定義されているカスタム URL カテゴリのリストを表示します。[含める（Include）] カラムで、ユーザ編集アクセス権を付与するカスタム URL カテゴリのチェックボックスをオンにします。[送信（Submit）] をクリックして、[ユーザ ロール（User Roles）] ページに戻ります。

カスタム ユーザ ロールの削除

1 人以上のユーザに割り当てられているカスタム ユーザ ロールを削除する場合、エラーは受信しません。

管理ユーザの認証の管理

許可されたユーザをアプライアンスでローカルに定義したり、外部認証を使用することで、アプライアンスに対するアクセスを制御できます。

- 「管理者ユーザのパスワード変更」（P.13-11）
- 「Locally-Defined 管理ユーザの管理」（P.13-11）
- 「外部ユーザ認証」（P.13-18）

管理者ユーザのパスワード変更

「管理者」ユーザのパスワードは GUI または CLI から変更できます。

GUI を使用してパスワードを変更するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択して、管理ユーザを選択します。

管理者ユーザのパスワードを CLI から変更するには `password` コマンドを使用します。パスワードは 6 文字以上である必要があります。`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。

管理者ユーザ アカウントのパスワードを忘れた場合は、パスワードをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

（注） パスワードの変更はすぐに有効になり、変更を送信する必要がありません。

Locally-Defined 管理ユーザの管理

- 「Locally-Defined ユーザの追加」（P.13-12）
- 「Locally-Defined ユーザの編集」（P.13-12）
- 「Locally-Defined ユーザの削除」（P.13-13）
- 「ローカルに定義されたユーザのリストの表示」（P.13-13）
- 「パスワードの設定と変更」（P.13-13）
- 「パスワードの設定およびログインの要件」（P.13-13）
- 「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）
- 「ローカル ユーザ アカウントのロックおよびロック解除」（P.13-17）

Locally-Defined ユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザを セキュリティ管理アプライアンスに直接追加します。または、CLI で **userconfig** コマンドを使用します。

（注）　外部認証もイネーブルである場合は、ローカル ユーザ名が外部認証されたユーザ名と重複しないことを確認してください。

アプライアンスに作成できるユーザ アカウントの数に制限はありません。

手順

ステップ 1　カスタム ユーザ ロールを割り当てる場合は、そのロールを先に定義しておくことを推奨します。「カスタム ユーザ ロール」（P.13-5）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 3　[ユーザを追加（Add User）] をクリックします。

ステップ 4　ユーザの一意の名前を入力します。システムで予約されている語（「operator」や「root」など）を入力することはできません。

外部認証も使用する場合は、ユーザ名を外部認証されたユーザ名と重複させることはできません。

ステップ 5　ユーザの氏名を入力します。

ステップ 6　事前定義されたロールまたはカスタム ロールを選択します。ユーザ ロールの詳細については、表 13-1 を参照してください。

新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、「Custom Email User ロールの作成」（P.13-7）または「Custom Web User ロールの作成」（P.13-9）を参照してください。

ステップ 7　パスワードを入力し、パスワードを再入力します。

ステップ 8　変更を送信し、保存します。

ステップ 9　このページにカスタム ユーザ ロールを追加する場合は、この時点でそのロールに権限を割り当てます。「カスタム ユーザ ロール」（P.13-5）を参照してください。

Locally-Defined ユーザの編集

たとえば、パスワードを変更するには、次の手順を実行します。

手順

ステップ 1　[ユーザ（Users）] 一覧でユーザの名前をクリックします。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　変更を送信し、保存します。

Locally-Defined ユーザの削除

手順

ステップ 1　[ユーザ（Users）] 一覧でユーザの名前に対応するゴミ箱のアイコンをクリックします。

ステップ 2　表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 3　[確定する（Commit）] をクリックして変更を保存します。

ローカルに定義されたユーザのリストの表示

ローカルに定義されたユーザのリストを表示するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

（注）　アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除された場合は、[割り当てなし（Unassigned）] と赤く表示されます。カスタム ユーザ ロールの詳細については、「カスタム ユーザ ロール」（P.13-5）を参照してください。

パスワードの設定と変更

- ユーザを追加する場合は、そのユーザに初期パスワードを指定します。
- システムに設定されたユーザのパスワードを変更するには、GUI の [ユーザの編集（Edit User）] ページを使用します（詳細は、「Locally-Defined ユーザの編集」（P.13-12）を参照してください）。
- システムのデフォルト管理ユーザ アカウントのパスワードを変更するには、「管理者ユーザのパスワード変更」（P.13-11）を参照してください。
- ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）を参照してください。
- GUI 右側上部の [オプション（Options）] メニューをクリックして、[パスワードの変更（Change Password）] オプションを選択することで、ユーザは自分のパスワードを変更できます。

  [パスワードの変更（Change Password）] ページで、古いパスワードを入力してから、新しいパスワードを入力し、確認のため、その新しいパスワードを再入力します。[送信（Submit）] をクリックして、ログアウトします。ログイン画面が表示されます。

パスワードの設定およびログインの要件

ユーザ アカウントとパスワードの制限を定義して、組織全体にパスワード ポリシーを強制的に適用することができます。ユーザ アカウントとパスワードの制限は、セキュリティ管理アプライアンスで定義されているローカル ユーザに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザがアカウントからロックアウトされるまでの、ログイン試行の失敗回数を定義できます。
- **パスワード期限の規則。**ログイン後にユーザがパスワードの変更を要求されるまでの、パスワードの使用期間を定義できます。
- **パスワードの規則。**どの文字が任意で、どの文字が必須かなど、ユーザが選択できるパスワードの種類を定義できます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ローカル ユーザ アカウントとパスワードの設定（Local User Account and Password Settings）] セクションまでページを下にスクロールします。

ステップ 3　[設定を編集（Edit Settings）] をクリックします。

ステップ 4　表 13-2 に示す設定値を設定します。

表 13-2　ローカル ユーザ アカウントとパスワードの設定

設定	説明
ユーザ アカウントのロック（User Account Lock）	ユーザが正常にログインできない場合に、ユーザ アカウントをロックするかどうかを決定します。アカウントがロックされるまでの、ログイン失敗回数を指定します。1 ～ 60 の範囲で任意の数字を入力できます。デフォルト値は 5 です。 アカウントのロックを設定する場合は、ログインしようとしているユーザに表示されるメッセージを入力します。7 ビットの ASCII 文字を使用して、テキストを入力します。このメッセージは、ユーザがロックされたアカウントに正しいパスワードを入力した場合だけ表示されます。 ユーザ アカウントがロックされた場合は、管理者が GUI の [ユーザの編集（Edit User）] ページか、`userconfig` CLI コマンドを使用して、ロック解除できます。 ユーザが接続に使用したマシン、または接続の種類（SSH または HTTP）に関係なく、失敗したログイン試行はユーザごとに追跡されます。ユーザが正常にログインすると、失敗したログイン試行回数はゼロ（0）にリセットされます。 失敗したログイン試行の最大数に達したためにユーザ アカウントがロックアウトされた場合、アラートが管理者に送信されます。このアラートは「Info」重大度レベルに設定されます。 **（注）**　個々のユーザ アカウントを手動でロックすることもできます。「手動によるユーザ アカウントのロック」（P.13-17）を参照してください。

表 13-2　ローカル ユーザ アカウントとパスワードの設定 （続き）

設定	説明
パスワードのリセット（Password Reset）	管理者がユーザのパスワードを変更後、ユーザにパスワードの変更を強制するかどうかを決定します。 また、パスワードの有効期限が切れた後に、ユーザにパスワードの変更を強制するかどうかを決定することもできます。ユーザによるパスワードの変更が必要になるまでの、パスワードの有効日数を入力します。1 ～ 366 の範囲で任意の数字を入力できます。デフォルトは 90 です。スケジュール外の時間に、ユーザにパスワードの変更を強制するには、「ユーザに対する次回ログイン時のパスワード変更の義務付け」（P.13-16）を参照してください。 パスワードの期限が切れた後、ユーザにパスワードの変更を強制する場合は、次回のパスワード期限切れについての通知を表示できます。期限切れの何日前に通知が行われるかを選択します。 パスワードが期限切れになると、ユーザは次回のログイン時にアカウントパスワードの変更を強制されます。 **（注）** ユーザ アカウントがパスワード チャレンジではなく SSH キーを使用している場合も、パスワードのリセット規則は適用されます。SSH キーを持つユーザ アカウントが期限切れになると、そのユーザは古いパスワードを入力するか、管理者に依頼して、パスワードを手動で変更し、アカウントに関連付けられたキーを変更してもらう必要があります。
パスワードルール：（Password Rules:） <number> 文字以上必要です。（Require at least <number> characters.）	パスワードに含める最小文字数を入力します。 ゼロ（0）以上のどんな数字も入力できます。
パスワードルール：（Password Rules:） 数字（0 ～ 9）が 1 文字以上必要です。（Require at least one number (0-9).）	パスワードに 1 文字以上の数字を含める必要があるかどうかを決定します。

パスワードルール：（Password Rules:）
特殊文字が 1 文字以上必要です。（Require at least one special character.）
	パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。
	`~ ?!@ # $ % ^ & * - _ + =`
	`\ | / [ ] ( ) < > { } ` ' " ; : , .`

表 13-2　ローカル ユーザ アカウントとパスワードの設定 （続き）

設定	説明
パスワードルール：（Password Rules:） ユーザ名とその変化形をパスワードとして使用することはできません。（Ban usernames and their variations as passwords.）	対応するユーザ名またはユーザ名の変化形と同じものを、パスワードに使用できるかどうかを決定します。ユーザ名の変化形の使用を禁止する場合、次の規則がパスワードに適用されます。 • 大文字か小文字かに関係なく、パスワードはユーザ名と同じであってはならない。 • 大文字か小文字かに関係なく、パスワードはユーザ名を逆にしたものと同じであってはならない。 • パスワードは、次の文字置換が行われたユーザ名、またはユーザ名を逆にしたものと同じであってはならない。 – 「a」の代わりに「@」または「4」 – 「e」の代わりに「3」 – 「i」の代わりに「|」、「!」、または「1」 – 「o」の代わりに「0」 – 「s」の代わりに「$」または「5」 – 「t」の代わりに「+」または「7」
パスワードルール：（Password Rules:） 直近 <number> 個のパスワードを再使用することはできません。（Ban reuse of the last <number> passwords.）	ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再利用を禁止した場合、再利用を禁止する最近のパスワードの個数を入力します。 1 ～ 15 の範囲で任意の数字を入力できます。デフォルトは 3 です。

ステップ 5　変更を送信し、保存します。

ユーザに対する次回ログイン時のパスワード変更の義務付け

すべての、または選択したユーザに、次回セキュリティ管理アプライアンスにアクセスしたときにパスワードを変更するように要求するには、次の手順を実行します。これは 1 回限りのアクションです。

パスワードを変更するための定期的な要求を自動化するには、「パスワードの設定およびログインの要件」（P.13-13）で説明されている [パスワードのリセット（Password Reset）] オプションを使用します。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] を選択します。

ステップ 2　[ユーザ（Users）] セクションで、次回のログインでパスワードの変更が必要なユーザの横のチェックボックスを選択します。

ステップ 3　[パスワードのリセット（Password Reset）] をクリックします。

ローカル ユーザ アカウントのロックおよびロック解除

ユーザ アカウントのロックは、ローカル ユーザがアプライアンスにログインするのを防止します。ユーザ アカウントは、次のいずれかの場合にロックされることがあります。

- すべてのローカル ユーザ アカウントを、設定した試行回数の後にユーザが正常なログインに失敗するとロックするように、設定することができます。「パスワードの設定およびログインの要件」（P.13-13）を参照してください。
- 管理者はユーザ アカウントを手動でロックできます。「手動によるユーザ アカウントのロック」（P.13-17）を参照してください。

[ユーザの編集（Edit User）] ページでユーザ アカウントを表示すると、AsyncOS によりユーザ アカウントがロックされた理由が表示されます。

手動によるユーザ アカウントのロック

手順

ステップ 1　初回のみ：アプライアンスを設定して、ユーザ アカウントのロックをイネーブルにします。

a. [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] に移動します。

b. [ローカル ユーザ アカウントとパスワードの設定（Local User Account & Password Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

c. [管理者が手動でユーザ アカウントをロックしている場合、ロックされているアカウント メッセージを表示する（Display Locked Account Message if Administrator has manually locked a user account）] に対するチェックボックスを選択して、メッセージを入力します。

d. 変更を送信します。

ステップ 2　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] に移動して、ユーザ名をクリックします。

（注）　admin アカウントをロックする前に、ロック解除できることを確認してください。「ユーザ アカウントのロック解除」（P.13-17）の（注）を参照してください。

ステップ 3　[アカウントのロック（Lock Account）] をクリックします。

AsyncOS は、ユーザがアプライアンスにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

ユーザ アカウントのロック解除

ユーザ アカウントをロック解除するには、[ユーザ（Users）] 一覧でユーザ名をクリックしてユーザ アカウントを開き、[アカウントのロック解除（Unlock Account）] をクリックします。

（注）　admin アカウントをロックした場合は、シリアル コンソール ポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアル コンソール ポートを使用して常にアプライアンスにアクセスできます。シリアル コンソール ポートを使用してアプライアンスにアクセスする方法の詳細については、お使いの電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Setup and Installation」の章を参照してください。

外部ユーザ認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するよう セキュリティ管理アプライアンスを設定できます。

（注）
- 「ビューのカスタマイズ」（P.14-57）で説明されている一部の機能は、外部認証ユーザには使用できません。
- 展開でローカル認証と外部認証の両方を使用している場合、ローカル ユーザ名と外部認証ユーザ名を同じにしないでください。
- アプライアンスが外部ディレクトリと通信できない場合、外部アカウントとローカル アカウントの両方を持つユーザは、ローカル ユーザ アカウントを使用してアプライアンスにログインできます。

LDAP 認証の設定

LDAP 認証を設定するには、「LDAP を使用した管理ユーザの外部認証の設定」（P.11-14）を参照してください。

RADIUS 認証のイネーブル化

ユーザを認証し、アプライアンスを管理しているユーザ ロールにユーザ グループを割り当てるために RADIUS ディレクトリを使用できます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザをユーザ ロールに割り当てるために CLASS 属性を使用します）。

（注）　外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

はじめる前に

RADIUS サーバへの共有シークレット キーの長さは 48 文字以下でなければなりません。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページで、[有効（Enable）] をクリックします。

ステップ 2　[外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 3　認証タイプとして RADIUS を選択します。

ステップ 4　RADIUS サーバのホスト名を入力します。

ステップ 5　RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。

ステップ 6　RADIUS サーバの共有シークレット キーを入力します。

（注）　電子メール セキュリティ アプライアンスのクラスタに対して外部認証を有効にするには、クラスタ内のすべてのアプライアンスで同じ共有シークレット キーを入力します。

ステップ 7　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 8　認証プロトコルとして、パスワード認証プロトコル（PAP）を使用するか、またはチャレンジ ハンドシェイク認証プロトコル（CHAP）を使用するか選択します。

ステップ 9　（任意）[行の追加（Add Row）] をクリックして別の RADIUS サーバを追加します。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

複数の外部サーバを定義する場合、アプライアンスは、アプライアンスに定義されている順序でサーバに接続します。1 つのサーバが一時的に使用できない場合、フェールオーバーを実行できるように、複数の外部サーバを定義する場合があります。

ステップ 10　Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

（注）　RADIUS サーバがワンタイム パスワード（たとえば、トークンから作成されるパスワード）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 11　グループ マッピングの設定

設定	説明
外部認証されたすユーザを複数のローカル ロールに割り当てます（Map externally authenticated users to multiple local roles）（推奨）	AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件： • 3 文字以上 • 253 文字以下 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。 次のアプライアンス ロールは、制限の少ないものから順番に並べられています。 • Administrator • Email Administrator • Web Administrator • Web Policy Administrator • URL Filtering Administrator • カスタム ユーザ ロール（電子メールまたは Web） ユーザにカスタム ユーザ ロールにマッピングされた複数のクラス属性が割り当てられている場合、RADIUS サーバのリストの最後のクラス属性が使用されます。 • Technician • Operator • Read-Only Operator • Help Desk User • Guest
外部認証されたすべてのユーザを管理者に割り当てます（Map all externally authenticated users to the Administrator role）	AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 12　（任意）[行の追加（Add Row）] をクリックして別のグループを追加します。アプライアンスが認証するユーザの各グループに対してステップ 11 を繰り返します。

ステップ 13　変更を送信し、保存します。

セキュリティ管理アプライアンスへのアクセスに対する追加の制御

IP ベースのネットワーク アクセスの設定

組織がリモート ユーザに逆プロキシを使用する場合、アプライアンスに直接接続するユーザ、および逆プロキシを介して接続するユーザのためのアクセス リストを作成することで、ユーザがどの IP アドレスからセキュリティ管理アプライアンスにアクセスするのかを制御できます。

直接接続

セキュリティ管理アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザは、アクセスを拒否されます。

プロキシ経由の接続

組織のネットワークで、リモート ユーザのマシンとセキュリティ管理アプライアンスの間で逆プロキシが使用されている場合、AsyncOS では、アプライアンスに接続できるプロキシの IP アドレスのアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモート ユーザの IP アドレスを電子メール セキュリティ アプライアンスに送信するには、プロキシで `x-forwarded-for` HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

`x-forwarded-for` ヘッダーは非 RFC 標準 HTTP ヘッダーであり、形式は次のとおりです。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

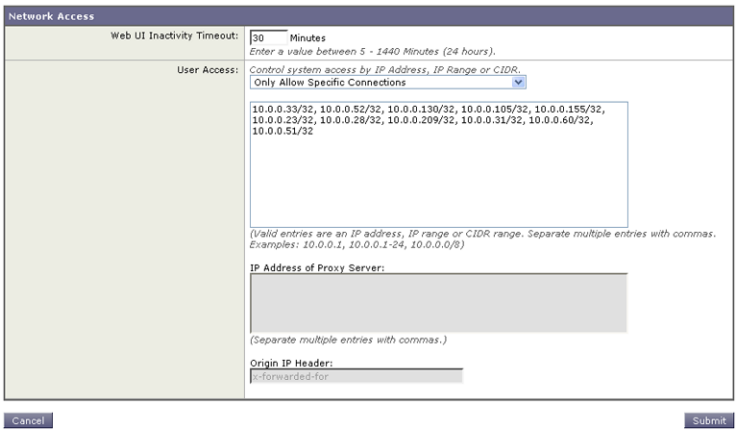
このヘッダーの値はカンマ区切りの IP アドレスのリストであり、左端のアドレスがリモート ユーザ マシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます。（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーから取得したリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リスト内の許可されたユーザ IP アドレスおよびプロキシ IP アドレスと照合します。

（注）　AsyncOS は、`x-forwarded-for` ヘッダーで IPv4 アドレスだけをサポートします。

アクセス リストの作成

GUI の [ネットワーク アクセス（Network Access）] ページまたは CLI の **adminaccessconfig > ipaccess** コマンドから、ネットワーク アクセス リストを作成できます。図 13-2 は、セキュリティ管理アプライアンスへの直接的な接続が許可されているユーザ IP アドレスのリストが表示された [ネットワークアクセス（Network Access）] ページを示しています。

図 13-2　ネットワーク アクセス設定の例



AsyncOS には、アクセス リストに対する次の 4 つの異なる制御モードが用意されています。

- [すべてを許可（Allow All）]。このモードでは、アプライアンスへのすべての接続が許可されます。これが、デフォルトの動作モードです。
- [特定の接続のみを許可（Only Allow Specific Connections）]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザのアプライアンスへの接続を許可します。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）]。このモードは、次の条件が満たされた場合に、逆プロキシを介したユーザのアプライアンスへの接続を許可します。
  - 接続プロキシの IP アドレスが、[プロキシ サーバ（Proxy Server）] フィールドのアクセス リストの IP アドレスに含まれている。
  - プロキシで、接続要求に `x-forwarded-header` HTTP ヘッダーが含まれている。
  - `x-forwarded-header` の値が空ではない。
  - リモート ユーザの IP アドレスが `x-forwarded-header` に含まれ、それがアクセス リスト内の IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- [特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）]。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの逆プロキシを介した、あるいは直接的なアプライアンスへの接続を許可します。プロキシを介した接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードの場合と同じです。

次のいずれかの条件に該当する場合、変更をサブミットおよびコミットした後に、アプライアンスにアクセスできなくなる可能性があります。

- [特定の接続のみを許可（Only Allow Specific Connections）] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] を選択し、アプライアンスに現在接続されているプロキシの IP アドレスがプロキシ リストになく、元の IP ヘッダーの値が許可された IP アドレスのリストにない場合。
- [特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）] を選択し、次が当てはまる場合。
  - 元の IP ヘッダーの値が許可される IP アドレスのリストにない

    または
  - 元の IP ヘッダーの値が許可される IP アドレスのリストになく、アプライアンスに接続されているプロキシの IP アドレスが許可されるプロキシのリストにない。

アクセス リストを修正せずに続行した場合、ユーザが変更を確定すると、AsyncOS はアプライアンスからユーザのマシンまたはプロキシを切断します。

手順

ステップ 1　[システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] を選択します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　アクセス リストの制御モードを選択します。

ステップ 4　ユーザがアプライアンスへの接続が許可される IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを区切るには、カンマを使用します。

ステップ 5　プロキシ経由の接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続が許可されているプロキシの IP アドレス。複数のエントリを区切るには、カンマを使用します。
- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモート ユーザ マシンの IP アドレスと、要求を転送したプロキシ サーバの IP アドレスが含まれます。デフォルトでは、ヘッダーの名前が `x-forwarded-for` です。

ステップ 6　変更を送信し、保存します。

Web UI セッション タイムアウトの設定

セキュリティ管理アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは、admin を含めて、すべてのユーザに適用され、また HTTP セッションと HTTPS セッションの両方に使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。

（注）　Web UI セッション タイムアウトは IronPort スパム隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

手順

ステップ 1　[システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] ページを使用します。

ステップ 2　[設定を編集（Edit Settings）] をクリックします。

ステップ 3　ユーザが非アクティブ状態になった後、何分経過後にログアウトされるかを入力します。タイムアウト時間には 5 ～ 1440 分を定義できます。

ステップ 4　変更を送信し、保存します。

メッセージ トラッキングでの DLP 機密情報へのアクセスの制御

データ漏洩防止（DLP）ポリシーに違反するメッセージには、通常、企業の機密情報や個人情報（クレジット カード番号や健康診断結果など）といった機密情報が含まれています。デフォルトで、この内容はメッセージ トラッキング結果に表示されているメッセージの [メッセージの詳細（Message Details）] ページにある [DLP に一致した内容（DLP Matched Content）] タブに表示されます。

このタブとその内容は、割り当てられている事前定義されたロールまたはカスタム ロールに基づいて、セキュリティ管理アプライアンスのユーザには表示されないようにすることができます。

手順

ステップ 1　[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページに移動します。

ステップ 2　[DLP トラッキング権限（DLP Tracking Privileges）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3　メッセージ トラッキングでの DLP データへのアクセス権を付与するロールを選択します。

メッセージ トラッキングへのアクセス権を持つカスタム ロールだけが一覧表示されます。

ステップ 4　変更を送信し、保存します。

この設定を有効にするには、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] で中央集中型電子メール メッセージ トラッキング機能をイネーブルにする必要があります。

管理ユーザ アクティビティの表示

- 「Web を使用したアクティブなセッションの表示」（P.13-25）
- 「コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示」（P.13-25）

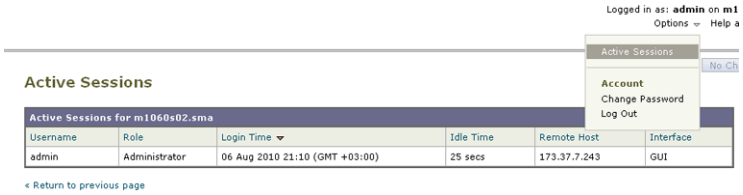
Web を使用したアクティブなセッションの表示

セキュリティ管理アプライアンスでは、すべてのアクティブなセッションと、アプライアンスにログインしているユーザを表示できます。

手順

ステップ 1　ウィンドウの右上から、[オプション（Options）] > [アクティブなセッション（Active Sessions）] を選択します。

図 13-3　　[アクティブなセッション（Active Sessions）] メニュー



[アクティブなセッション（Active Sessions）] ページから、ユーザ名、ユーザが持っているロール、ユーザのログイン時間、アイドル時間、およびユーザがコマンドラインと GUI のどちらからログインしたかを表示できます。

コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示

次に、アプライアンスへの複数ユーザ アクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who

Username  Login Time  Idle Time  Remote Host  What
========  ==========  =========  ===========  ====
admin     03:27PM     0s         10.1.3.201   cli
```

- whoami コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami

Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしたユーザを表示します。リモート ホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last

Username  Remote Host  Login Time        Logout Time       Total Time
```

```
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```