管理タスクの分散

この章は、次の項で構成されています。

- ユーザ アカウントを使用する作業 （1 ページ）
- 委任管理のためのカスタム ユーザ ロールの管理 （7 ページ）
- パスフレーズ （17 ページ）
- E メール セキュリティ アプライアンスへの アクセスの設定 （24 ページ）
- 管理ユーザへのメッセージの表示 （29 ページ）
- セキュア シェル（SSH）キーの管理 （30 ページ）
- 管理ユーザ アクセスのモニタリング （32 ページ）

ユーザ アカウントを使用する作業

Cisco アプライアンスには、ユーザ アカウントを追加する 2 つの方法があります。Cisco アプライアンス自体でユーザ アカウントを作成する方法と、LDAP または RADIUS ディレクトリなどの独自の中央認証システムを使用してユーザ認証を有効にする方法です。ユーザと外部認証ソースへの接続を管理するには、GUI で [システム管理（System Administration）] > [ユーザ（Users）] ページを使用します（または、CLI で **userconfig** コマンドを使用します）。ユーザを認証するために外部ディレクトリを使用することについては、外部認証 （19 ページ）を参照してください。

必要に応じて、次を使用して、特定のユーザ ロールに二要素認証を有効にできます。

- Web インターフェイスの [システム管理（System Administration）] > [ユーザ（Users）] ページ。二要素認証 （23 ページ）を参照してください。
- CLI での `userconfig > twofactorauth` コマンド。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

システムのデフォルトのユーザ アカウントである admin はすべての管理権限を持っています。admin ユーザ アカウントは削除できませんが、パスフレーズを変更してアカウントをロックすることはできます。

新しいユーザ アカウントを作成する場合は、そのユーザを定義済みのユーザ ロールまたはカスタム ユーザ ロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。

アプライアンスで作成できる各ユーザアカウントの数に制限はありませんが、システムで予約されている名前とユーザアカウントは作成できません。たとえば、「operator」や「root」という名前のユーザ アカウントは作成できません。

ユーザの役割

表 *1:* ユーザ ロールの一覧

ユーザ ロール	説明
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。
管理者	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。ただし、**resetconfig** コマンドと **revert** コマンドにアクセスできるのは admin ユーザだけです。 （注） AsyncOS は、GUI から E メール セキュリティ アプライアンスを同時に設定する複数の管理者をサポートしません。
専門技術者	Technician ロールを持つユーザアカウントはシステムのアップグレード、アプライアンスの再起動、ライセンス キーの管理を実行できます。専門技術者は、アプライアンスをアップグレードするために以下の処理も実行できます。 • 電子メールの配信および受信の一時停止。 • ワークキューとリスナーのステータスの表示。 • 設定ファイルの保存および電子メール送信。 • セーフリストとブロックリストのバックアップ。専門技術者はこれらのリストを復元できません。 • クラスタからのアプライアンスの接続解除。 • Cisco テクニカル サポートへのリモート サービス アクセスの有効化または無効化。 • サポート要求の申請。

ユーザ ロール	説明
オペレータ	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。 • **resetconfig** コマンドの発行。 • アプライアンスのアップグレード • **systemsetup** コマンドの発行またはシステム設定ウィザードの実行。 • **adminaccessconfig** コマンドの発行。 • 隔離機能の実行（作成、編集、削除、および隔離の中央集中を含む）。 • ユーザ名とパスフレーズ以外の 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有効になっている場合）。 これら以外は、Administrator ロールと同じ権限を持ちます。
ゲスト	Guest ロールを持つユーザ アカウントはステータス情報とレポートだけを参照できます。Guest ロールを持つユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。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。
オペレータ（読み取り専用）	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変更を行って送信できますが、保存できません。このロールのユーザは、アクセスが隔離でイネーブルの場合、隔離エリア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。 • 作成、編集、削除、または隔離の中央集中の設定。
ヘルプ デスク ユーザ	ヘルプデスク ユーザ 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。 • 隔離エリア内のメッセージの管理。 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。このロールのユーザがそのデバイスを管理する前に、各隔離アクセスをイネーブルにする必要があります。

ユーザ ロール	説明
カスタム ユーザ ロール	カスタム ユーザ ロールを持つユーザ アカウントはそのロールに割り当てられている電子メール セキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、隔離、ローカル メッセージ トラッキング、暗号化プロファイル、およびトレース デバッグ ツールの任意の組み合わせになります。ユーザは、機能のグローバルなイネーブル化を含むシステム設定機能にアクセスできません。カスタム ユーザ ロールを定義できるのは管理者だけです。詳細については、委任管理のためのカスタム ユーザ ロールの管理 （7 ページ）を参照してください。 （注） カスタム ユーザ 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。

上記の表に定義されているロールはすべて GUI と CLI の両方にアクセスできます。ただし、Help Desk User ロールとカスタム ユーザ ロールは GUI にのみアクセスできます。

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、外部認証 （19 ページ）を参照してください。

関連項目

- ユーザの管理 （4 ページ）

ユーザの管理

[ユーザ（Users）]ページには、システムの既存のユーザが一覧（ユーザ名、氏名、およびユーザ タイプまたはグループを含む）で表示されます。

[ユーザ（Users）] ページからは、次の操作が行えます。

- 新しいユーザの追加。詳細については、ユーザの追加 （5 ページ）を参照してください。
- ユーザの削除。詳細については、ユーザの削除 （6 ページ）を参照してください。
- ユーザの編集。ユーザのパスフレーズの変更、ユーザのアカウントのロックおよびロック解除など。詳細については、ユーザの編集 （5 ページ）を参照してください。
- ユーザにパスフレーズの変更を強制します。ユーザにパスフレーズの変更を強制 （6 ページ）を参照してください。
- ローカル アカウント用のユーザ アカウントとパスフレーズ設定値の設定。詳細については、制限的なユーザ アカウントとパスフレーズの設定値の構成 （19 ページ）を参照してください。

- ユーザを認証するために LDAP または RADIUS ディレクトリを使用するようアプライアンスをイネーブルにする。詳細については、外部認証 （19ページ）を参照してください。
- 特定のユーザ ロールに二要素認証を有効にします。詳細については、二要素認証 （23ページ）を参照してください。
- メッセージ トラッキング内の DLP Matched Content への管理者以外のアクセスをイネーブルにする。詳細については、メッセージ トラッキングでの機密情報へのアクセスの制御（6 ページ）を参照してください。

ユーザの追加

はじめる前に

- ユーザが使用するユーザ ロールを設定します。
  - 定義済みのユーザ ロールについては、ユーザの役割 （2 ページ）を参照してください。
  - カスタム ロールを作成するには、委任管理のためのカスタム ユーザ ロールの管理 （7 ページ）を参照してください。
- パスフレーズの要件を指定します。制限的なユーザ アカウントとパスフレーズの設定値の構成 （19 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザ（Users）] を選択します。
ステップ 2 [ユーザを追加（Add User）] をクリックします。
ステップ 3 ユーザのログイン名を入力します。一部の単語（「operator」や「root」など）が予約されています。
ステップ 4 ユーザの氏名を入力します。
ステップ 5 定義済みのユーザ ロールまたはカスタム ユーザ ロール（Custom user role）を選択します。
ステップ 6 パスフレーズを生成するか、または入力します。
ステップ 7 変更を送信し、保存します。

ユーザの編集

パスフレーズなどを変更するには、この手順を使用します。

手順

ステップ 1 [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）] 一覧でユーザの名前をクリックします。

ステップ 3 ユーザに対して変更を行います。

ステップ 4 変更を送信し、保存します。

ユーザにパスフレーズの変更を強制

手順

ステップ 1 [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）] 一覧からユーザを選択します。

ステップ 3 [パスフレーズ変更を適用（Enforce Passphrase Change）] をクリックします。

ステップ 4 次回のログイン時または指定した期間（日数）が経過した後にユーザがパスフレーズを変更する必要があるかどうかを選択します。

ステップ 5 （任意）指定した期間が経過した後にパスフレーズの変更を適用する場合は、パスフレーズの期限切れ後にパスフレーズをリセットするまでの猶予期間（日数）を設定します。

ステップ 6 [OK] をクリックします。

ステップ 7 変更を送信し、保存します。

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 変更を保存します。

メッセージ トラッキングでの機密情報へのアクセスの制御

機密情報が含まれている可能性のあるメッセージの詳細に対し、管理アクセスを制限することが必要になる場合があります。

- データ損失防止（DLP）ポリシーに違反するメッセージには、企業の秘密情報、またはクレジットカード番号や医療記録を含む個人情報などの情報が含まれている可能性があります。デフォルトでは、この内容は、アプライアンスへのアクセスを持つすべてのユーザが閲覧可能です。
- アウトブレイク フィルタ、またはURL レピュテーションもしくはカテゴリに基づくコンテンツ フィルタによって捕捉されるURLも、機密性が高いと見なされる場合があります。デフォルトでは、この内容を閲覧できるのは、管理者特権を持つユーザのみです。

この機密性の高い内容は、メッセージ トラッキング結果に表示されたメッセージの [メッセージの詳細（Message Details）] ページにある専用のタブに表示されます。

これらのタブとその内容は、管理ユーザに対し、そのユーザ ロールに基づいて非表示にできます。ただし、管理者ロールを持つユーザに対してこの機密性の高い内容を非表示にするオプションはありますが、管理者ロールを持つユーザは、これらの権限を変更できるため、機密性の高い情報をいつでも閲覧することができます。

はじめる前に

これらの機能の前提条件を満たしていることを確認します。メッセージ トラッキングの URL 詳細の表示を参照してください。

手順

ステップ 1 [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 [メッセージトラッキング内の機密情報へのアクセス（Access to Sensitive Information in Message Tracking）] で、[設定の編集（Edit Settings）] をクリックします。

ステップ 3 機密情報のタイプごとに、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 トラッキングにアクセスできないカスタム ロールはこの情報を見ることができないため、表示されません。

ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- メッセージ トラッキングの詳細
- メッセージ トラッキングでの機密性の高い DLP データの表示
- メッセージ トラッキングの URL 詳細の表示

委任管理のためのカスタム ユーザ ロールの管理

カスタム ユーザ ロールを設計し、組織内でのそれぞれのロールに一致した特定の責任をユーザに委任することができます。委任管理者は、それぞれが責任を負う電子メールセキュリティ機能にのみアクセスでき、それぞれのロールに関連しないシステム設定機能にはアクセスできません。委任管理を行うことで、アプライアンスの電子メールセキュリティ機能に対するユーザのアクセスを、定義済みの Administrator、Operator、および Help Desk User ロールより柔軟に制御できるようになります。

たとえば、E メール セキュリティ アプライアンスの特定ドメインの電子メール ポリシーの管理に関与しているユーザがいる場合に、それらのユーザに、定義済みの Administrator および Operator ロールで付与されるシステム管理やセキュリティ サービスの設定機能にはアクセスさせたくないことがあります。それぞれのユーザに管理するメール ポリシーへのアクセス権限、

およびそれらのポリシーで処理されるメッセージを管理するために使用できる他の電子メール セキュリティ機能（メッセージ トラッキングやポリシー隔離など）を付与できるメール ポリシー管理者用のカスタム ユーザ ロールを作成できます。

GUI で [システム管理（System Administration）] > [ユーザの役割（User Roles）] ページを使用して（または、CLI で userconfig -> role コマンドを使用して）、カスタム ユーザ ロールを定義し、それぞれが責任を負う電子メール セキュリティ機能（メール ポリシー、DLP ポリシー、電子メール レポート、および隔離など）を管理します。委任管理者が管理できる電子メール セキュリティ機能の一覧については、アクセス権限の割り当て （9 ページ）を参照してください。カスタム ロールは、[システム管理（System Administration）] > [ユーザ（Users）] ページを使用して、ローカル ユーザ アカウントを追加または編集するときにも作成できます。詳細については、ユーザ アカウント追加時のカスタム ユーザ ロールの定義 （15 ページ）を参照してください。

カスタム ユーザ ロールを作成する際には、そのロールの責任が他の委任管理者の責任と重複しすぎないようにする必要があります。たとえば、複数の委任管理者が同じコンテンツ フィルタに対する責任を持ち、そのコンテンツ フィルタを異なるメール ポリシーで使用する場合、1 人の委任管理者がそのフィルタに加えた変更により、他の委任管理者が管理しているメール ポリシーに意図せぬ悪影響を及ぼすことがあります。

カスタム ユーザ ロールを作成すると、他のユーザ ロールと同様にローカル ユーザと外部認証グループをそのカスタム ユーザ ロールに割り当てることができます。詳細については、ユーザ アカウントを使用する作業 （1 ページ）を参照してください。カスタム ロールに割り当てられているユーザは CLI にアクセスできないことに注意してください。

関連項目

- [アカウント権限（Account Privileges）] ページ （8 ページ）
- アクセス権限の割り当て （9 ページ）
- カスタム ユーザ ロールの定義 （14 ページ）
- ユーザ アカウント追加時のカスタム ユーザ ロールの定義 （15 ページ）
- カスタム ユーザ ロールの責任のアップデート （16 ページ）
- カスタム ユーザ ロールの編集 （16 ページ）
- カスタム ユーザ ロールの複製 （16 ページ）
- カスタム ユーザ ロールの削除 （17 ページ）

[アカウント権限（Account Privileges）] ページ

委任管理者がアプライアンスにログインすると、[アカウント権限（Account Privileges）] ページに委任管理者が責任を持つセキュリティ機能へのリンク、およびそれぞれのアクセス権限についての簡単な説明が表示されます。委任管理者は、[オプション（Options）] メニューで [アカウント権限（Account Privileges）] を選択することでこのページに戻ることができます。委任管理者は、Web ページの上部にあるメニューを使用して、管理する機能にアクセスすることもできます。

次の図は、メール ポリシー、電子メール レポーティング、メッセージ トラッキング、および隔離にアクセスできる委任管理者の [アカウント権限（Account Privileges）] ページを示しています。

図 *1 :* 委任管理者の *[*アカウント権限（*Account Privileges*）*]* ページ

アクセス権限の割り当て

カスタム ユーザ ロールを作成する場合、委任管理者が責任を負うセキュリティ機能へのアクセス レベルを定義します。

委任管理者が管理できるセキュリティ機能は以下のとおりです。

- 送受信のメール ポリシーとコンテンツ フィルタ。
- データ消失防止（DLP）ポリシー。
- 電子メール レポーティング。
- メッセージ トラッキング。
- トレース デバッグ ツール。
- スパム、ポリシー、ウイルス、およびアウトブレイク隔離。
- Cisco Email Encryption プロファイル。

カスタム ユーザ ロールのアクセス レベルを定義したら、委任管理者が責任を負うことになる具体的なメールポリシー、コンテンツ フィルタ、DLP ポリシー、隔離、または暗号化プロファイルを割り当てる必要があります。

たとえば、異なる DLP ポリシーに対して責任を負う 2 つの異なる DLP ポリシー管理者ロールを作成できます。1 つのロールは企業の秘密保持や許容範囲での使用に関する DLP 違反にのみ責任を負い、他のロールはプライバシー保護に関する DLP 違反に責任を負うようにできます。DLP ポリシーへのアクセスに加えて、これらのカスタム ユーザ ロールにはメッセージ データのトラッキング、隔離とレポートの表示に対する権限を割り当てることもできます。それらのロールは、メッセージ トラッキングの使用において責任を負うポリシーに関連する DLP 違反を検索できます。

カスタム ユーザ ロールに割り当てることができる責任については、[ユーザの役割（User Roles）] ページの [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブル内の割り当て済み権限のリンクをクリックして確認できます。カスタム ユーザ ロールの責任のアップデート （16 ページ）を参照してください。

関連項目

- メール ポリシーとコンテンツ フィルタ （10 ページ）
- DLP ポリシー （11 ページ）
- 電子メール レポーティング （12 ページ）
- メッセージ トラッキング （13 ページ）
- トレース （14 ページ）
- 隔離 （14 ページ）
- 暗号化プロファイル （14 ページ）

メール ポリシーとコンテンツ フィルタ

メール ポリシーとコンテンツ フィルタのアクセス権限では、E メール セキュリティ アプライアンス上の送受信メール ポリシーとコンテンツ フィルタへの委任管理者のアクセス レベルを定義します。特定のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当て、そのロールに属する委任管理者、および Operator と Administrator だけがメール ポリシーとコンテンツ フィルタを管理できるようにすることができます。

このアクセス権限を持つすべての委任管理者は、デフォルトの送受信メール ポリシーを表示できますが、すべてのアクセス権限を持っている場合のみそれらのポリシーを編集できます。

アクセス権限を持つすべての委任管理者は、それぞれのメール ポリシーで使用する新しいコンテンツ フィルタを作成できます。委任管理者が作成したコンテンツ フィルタは、そのカスタム ユーザ ロールに割り当てられているの他の委任管理者が使用できます。いずれのカスタム ユーザ ロールにも割り当てられていないコンテンツ フィルタはパブリックであり、メール ポリシーのアクセス権限を持つすべての委任管理者が表示できます。Operator や Administrator が作成したコンテンツ フィルタは、デフォルトでパブリックです。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーの既存のコンテンツ フィルタはすべてイネーブルまたはディセーブルにできますが、パブリック コンテンツ フィルタは変更も削除もできません。

委任管理者が自分のポリシー以外のメール ポリシーで使用されているコンテンツ フィルタを削除した場合、またはそのコンテンツ フィルタが他のカスタム ユーザ ロールに割り当てられている場合、AsyncOS はそのコンテンツ フィルタをシステムから削除しません。代わりに、AsyncOS はそのカスタム ユーザ ロールからコンテンツ フィルタのリンクを解除し、委任管理者のメール ポリシーから削除します。そのコンテンツ フィルタは、他のカスタム ユーザ ロールとメール ポリシーでは引き続き使用可能です。

委任管理者は、それぞれのコンテンツ フィルタで任意のテキスト リソースやディクショナリを使用できますが、GUI で [テキスト リソース（Text Resources）] ページや [ディクショナリ（Dictionaries）] ページにアクセスして、それらを表示または変更することはできません。委任管理者は、新しいテキスト リソースやディクショナリを作成することもできません。

送信メール ポリシーの場合、委任管理者は DLP ポリシーをイネーブルまたはディセーブルできますが、DLP ポリシーの権限も持っている場合を除き、DLP の設定をカスタマイズすることはできません。

メール ポリシーとコンテンツ フィルタ用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- アクセスなし（No access）：委任管理者は、E メール セキュリティ アプライアンスのメール ポリシーとコンテンツ フィルタを表示も編集もできません。
- **割り当てられた隔離を表示、割り当てられた隔離を編集（View assigned, edit assigned）**：委任管理者はカスタム ユーザ ロールに割り当てられているメール ポリシーとコンテンツ フィルタを表示および編集でき、新しいコンテンツ フィルタを作成できます。委任管理者は、ポリシーのスパム対策、ウイルス対策、およびアウトブレイク フィルタの設定を編集できます。委任管理者はポリシーに対してそれぞれのコンテンツ フィルタをイネーブルにでき、責任があるものかどうかに関係なく、そのポリシーに割り当てられている既存のコンテンツ フィルタをディセーブルにできます。委任管理者はメール ポリシーの名前、その送信者、受信者、またはグループを変更することはできません。委任管理者は、それぞれのカスタム ユーザ ロールに割り当てられているメール ポリシーのコンテンツ フィルタの順序を変更できます。
- **すべてを表示、割り当てられた隔離を編集（View all, edit assigned）**：委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタを表示できますが、そのカスタム ユーザ ロールに割り当てられているもののみ編集できます。

すべてを表示、すべてを編集(フルアクセス)（View all, edit all (full access)）：委任管理者は、アプライアンスのすべてのメール ポリシーとコンテンツ フィルタ（デフォルトのメール ポリシーを含む）に対するすべてのアクセス権限を持ち、新しいメール ポリシーを作成できます。委任管理者は、すべてのメール ポリシーの送信者、受信者、およびグループを変更できます。メール ポリシーの順序を変更することもできます。

[ユーザの役割（User Roles）] ページの [電子メールセキュリティ マネージャ（Email Security Manager）] または [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）]テーブルを使用して、個々のメール ポリシーとコンテンツ フィルタをカスタム ユーザ ロールに割り当てることができます。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブルを使用したメール ポリシーとコンテンツ フィルタの割り当ての詳細については、カスタム ユーザ ロールの責任のアップデート （16 ページ）を参照してください。

DLP ポリシー

DLP ポリシーのアクセス権限では、E メール セキュリティ アプライアンスの DLP Policy Manager を介した DLP ポリシーへの委任管理者のアクセス レベルを定義します。DLP ポリシーを特定のカスタム ユーザ ロールに割り当て、オペレータと管理者に加えて、委任管理者にそれらのポリシーを管理させることができます。DLP アクセス権を持つ委任管理者は、データ消失防止の Global Settings ページから DLP 設定ファイルをエクスポートできます。

委任管理者がメール ポリシー権限も保持している場合は、 DLP ポリシーをカスタマイズできます。委任管理者は、それぞれの DLP ポリシーの任意のカスタム DLP ディクショナリを使用できますが、カスタム DLP ディクショナリは表示も変更もできません。

DLP ポリシー用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- アクセスなし（No access）：委任管理者は E メール セキュリティ アプライアンスの DLP ポリシーを表示も編集もできません。
- 割り当てられた隔離を表示（View assigned）、割り当てられた隔離を編集（edit assigned）：委任管理者は DLP Policy Manager を使用して、カスタム ユーザ ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの名前変更も順序変更もできません。委任管理者は DLP 設定をエクスポートできます。
- すべてを表示（View all）、割り当てられた隔離を編集（edit assigned）：委任管理者はカスタム ユーザ ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は DLP 設定をエクスポートできます。委任管理者は、そのカスタム ユーザ ロールに割り当てられていない DLP ポリシーをすべて表示できますが、編集することはできません。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序変更やポリシー名の変更はできません。
- すべてを表示、すべてを編集（フルアクセス）（View all, edit all (full access)）：委任管理者は、アプライアンスのすべての DLP ポリシーに対するすべてのアクセス権限を持ち、新しいポリシーを作成することもできます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序を変更できます。また、アプライアンスで使用する DLP モードを変更できません。

[ユーザの役割（User Roles）] ページの [DLPポリシーマネージャ（DLP Policy Manager）] または [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブルを使用して、個々の DLP ポリシーをカスタム ユーザ ロールに割り当てることができます。

DLP ポリシーや DLP Policy Manager の詳細については、データ損失の防止を参照してください。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] の一覧を使用して DLP ポリシーを割り当てる方法の詳細については、カスタム ユーザ ロールの責任のアップデート （16 ページ）を参照してください。

電子メール レポーティング

電子メール レポーティングのアクセス権限では、カスタム ユーザ ロールのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーへのアクセス権限に従い、委任管理者が表示できるレポートと [電子メール セキュリティ モニタ（Email Security Monitor）] ページを定義します。それらのレポートは割り当てられているポリシーに対してフィルタリングされていません。委任管理者は、自分が責任を負っていないメールと DLP ポリシーのレポートを表示できます。

電子メール レポーティング用の以下のアクセス レベルのいずれかをカスタム ユーザ ロールに割り当てることができます。

- **アクセスなし（No access）**：委任管理者は、E メール セキュリティ アプライアンスのレポートを表示できません。

- **関連するレポートを表示（View relevant reports）**：委任管理者は、[電子メール セキュリティ モニタ（Email Security Monitor）] ページにあるそれぞれのメール ポリシー、コンテンツ フィルタ、およびDLPポリシーのアクセス権限に関連するレポートを表示できます。メール ポリシーとコンテンツ フィルタのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。
  - 概要
  - 受信メール
  - 送信先
  - 送信者（Outgoing Senders）
  - 内部ユーザ（Internal Users）
  - コンテンツ フィルタ
  - ウイルス アウトブレイク（Virus Outbreaks）
  - ウイルスの種類
  - アーカイブ レポート（Archived Reports）

  DLPポリシーのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。
  - 概要
  - DLP インシデント（DLP Incidents）
  - アーカイブ レポート（Archived Reports）
- **すべてのレポートを表示（View all reports）**：委任管理者は、E メール セキュリティ アプライアンスのすべてのレポートと [電子メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。

電子メール レポーティングと [電子メール セキュリティ モニタ（Email Security Monitor）] の詳細については、電子メール セキュリティ モニタの使用方法の章を参照してください。

メッセージ トラッキング

メッセージ トラッキングのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がメッセージ トラッキングへのアクセス権限を持つかどうかを定義します。メッセージ トラッキングには、[システム管理（System Administration）] > [ユーザ（Users）] ページで [DLP トラッキング ポリシー（DLP Tracking Policies）] オプションがイネーブルになっていて、カスタム ユーザ ロールに DLP ポリシーのアクセス権限もある場合に、組織の DLP ポリシー違反となる可能性があるメッセージの内容も含まれます。

委任管理者はそれぞれに割り当てられている DLP ポリシーに対する DLP 違反のみ検索できます。

メッセージ トラッキングの詳細については、メッセージ トラッキングを参照してください。

委任管理者に、メッセージ トラッキング内の一致した DLP の内容を表示するためのアクセスを許可する方法の詳細については、メッセージ トラッキングでの機密情報へのアクセスの制御（6 ページ）を参照してください。

トレース

トレースのアクセス権限では、カスタム ユーザ ロールに割り当てられている委任管理者がトレースを使用して、システムを介したメッセージフローをデバッグできるかどうかを定義します。アクセス権限がある委任管理者は、トレースを実行して、生成されるすべての出力を表示できます。トレース結果は、委任管理者のメールまたは DLP ポリシー権限に基づきフィルタリングはされません。

トレースの使用方法の詳細については、テスト メッセージを使用したメール フローのデバッグ：トレースを参照してください。

隔離

隔離のアクセス権限では、委任管理者が割り当てられた隔離を管理できるかどうかを定義します。委任管理者は、割り当てられた隔離内の任意のメッセージを表示して、メッセージの解放や削除などのアクションを実行できますが、隔離の設定（サイズ、保存期間など）の変更、隔離の作成や削除はできません。

[モニタ（Monitor）] > [隔離（Quarantines）] ページまたは [ユーザの役割（User Roles）] ページの [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブルを使用して、任意の隔離をカスタム ユーザ ロールに割り当てることができます。

管理ユーザに隔離管理タスクを割り当てる方法については、メッセージ処理タスクの他のユーザへの割り当てについてとスパム隔離への管理ユーザ アクセスの設定を参照してください。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧を使用して隔離を割り当てる方法の詳細については、カスタム ユーザ ロールの責任のアップデート （16 ページ）を参照してください。

暗号化プロファイル

暗号化プロファイルのアクセス権限では、委任管理者がコンテンツ フィルタまたは DLP ポリシーの編集時に、それぞれのカスタム ユーザ ロールに割り当てられている暗号化プロファイルを使用できるかどうかを定義します。暗号化プロファイルは、メールまたは DLP ポリシーのアクセス権限があるカスタムユーザロールにのみ割り当てることができます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。委任管理者はいずれの暗号化プロファイルも表示または変更できません。

暗号化プロファイルは、[セキュリティ サービス（Security Services）] > [IronPort メール暗号化（IronPort Email Encryption）] ページを使用して暗号化プロファイルを作成または編集するときに割り当てることができます。

カスタム ユーザ ロールの定義

GUI で [ユーザの役割（User Roles）] ページを使用して（または CLI で userconfig -> role コマンドを使用して）、新しいユーザ ロールを定義し、そのロールのアクセス権限を割り当てま

す。[ユーザの役割（User Roles）]ページには、アプライアンスの既存のすべてのカスタム ユーザ ロールと各ロールのアクセス権限が表示されます。

手順

ステップ 1 [システム管理（System Administration）] > [User Roles（ユーザの役割）] を選択します。
ステップ 2 [ユーザ役割の追加（Add User Role）] をクリックします。
ステップ 3 ユーザ ロールの名前を入力します。
ステップ 4 ユーザ ロールの説明とその権限を入力します。
ステップ 5 ユーザ ロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、アクセス権限の割り当て （9 ページ）を参照してください）。
ステップ 6 変更を送信し、保存します。

ユーザ アカウント追加時のカスタム ユーザ ロールの定義

E メール セキュリティ アプライアンスに対してローカル ユーザ アカウントの追加または編集を行う際に、新しいカスタム ユーザ ロールを作成できます。

ユーザ アカウントの追加の詳細については、ユーザの管理 （4 ページ）を参照してください。

手順

ステップ 1 [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 [ユーザの追加（Add User）] をクリックします。
ステップ 3 ユーザ アカウント作成時には、[カスタム役割（Custom Roles）] を選択します。
ステップ 4 [役割を追加（Add Role）] を選択します。
ステップ 5 新しいロールの名前を入力します。
ステップ 6 新しいユーザ アカウントを送信します。

AsyncOS により、新しいユーザ アカウントとカスタム ユーザ ロールが追加されたという通知が表示されます。

ステップ 7 [システム管理（System Administration）] > [ユーザの役割（User Roles）] ページに移動します。
ステップ 8 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブルでカスタム ユーザ ロールの名前をクリックします。
ステップ 9 ユーザ ロールの説明とその権限を入力します。
ステップ 10 ユーザ ロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、アクセス権限の割り当て （9 ページ）を参照してください）。

ステップ 11 変更を送信し、保存します。

カスタム ユーザ ロールの責任のアップデート

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）] ページに移動します。

ステップ 2 アップデートするカスタム ユーザ ロールのアクセス権限の名前をクリックします。

AsyncOS により、アプライアンスで使用可能なすべてのメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離の一覧、およびその他すべての割り当て済みカスタム ユーザ ロールの名前が表示されます。

ステップ 3 委任管理者に責任を割り当てるメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離を選択します。

ステップ 4 変更を送信し、保存します。

カスタム ユーザ ロールの編集

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）] ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧でユーザ ロールの名前をクリックします。

ステップ 3 ユーザ ロールに変更を加えます。

ステップ 4 変更を送信し、保存します。

カスタム ユーザ ロールの複製

同様のアクセス権限がある複数のカスタム ユーザ ロールを作成し、異なるユーザのセットに異なる責任を割り当てたいことがあります。たとえば、E メール セキュリティ アプライアンスが複数ドメインのメッセージを処理する場合、同様のアクセス権限だが、ドメインに基づく異なるメールポリシーに対する権限であるカスタムユーザロールを作成することができます。こうすることで、委任管理者は、他の委任管理者の責任を妨げることなくそれぞれのドメインのメール ポリシーを管理できます。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）]ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧で、複製するユーザ ロールに対応する複製アイコンをクリックします。

ステップ 3 カスタム ユーザ ロールの名前を変更します。

ステップ 4 新しいカスタム ユーザ ロールに必要なすべてのアクセス権限の変更を行います。

ステップ 5 変更を送信し、保存します。

カスタム ユーザ ロールの削除

カスタム ロールが削除されると、ユーザは未割り当て状態になり、アプライアンスにアクセスできなくなります。複数の個人に割り当てられたカスタム ユーザ ロールを削除すると、警告メッセージを受信しません。削除したカスタム ユーザ ロールに割り当てられていたすべてのユーザを再割り当てする必要があります。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）]ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧で、削除するユーザ ロール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 3 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 4 変更を保存します。

パスフレーズ

- パスフレーズの変更 （17 ページ）
- ユーザ アカウントのロックおよびロック解除 （18 ページ）
- 制限的なユーザ アカウントとパスフレーズの設定値の構成 （19 ページ）
- 外部認証 （19 ページ）
- 二要素認証 （23 ページ）

パスフレーズの変更

管理ユーザは GUI の最上部にある [オプション（Options）]>[パスフレーズの変更（Change Passphrase）] リンクを使用して自分のパスフレーズを変更できます。

新しいパスフレーズを送信するとすぐにログアウトされ、ログイン画面が表示されます。

CLI で、passphrase コマンドまたは passwd コマンドを使用してパスフレーズを変更します。「admin」ユーザ アカウントのパスフレーズを忘れた場合は、パスフレーズ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。

passphrase コマンドでは、セキュリティのために古いパスフレーズの入力が必要です。

（注） パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

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。

- AsyncOS は、ユーザが [ローカルユーザアカウントとパスフレーズの設定（Local User Account & Passphrase Settings）] セクションで定義されている失敗ログイン試行の最大回数を超えた場合にユーザ アカウントをロックします。
- 管理者は、[システム管理（System Administration）] > [ユーザ（Users）] ページを使用して、セキュリティ目的でユーザ アカウントを手動でロックできます。

[ユーザ役割の編集（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。

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。

ローカル ユーザ アカウントを手動でロックするには、[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（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。

ユーザが設定した試行回数を超えた後でログインに失敗した場合、すべてのローカル ユーザ アカウントをロックするように設定することもできます。詳細については、制限的なユーザ アカウントとパスフレーズの設定値の構成 （19 ページ）を参照してください。

（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、アプライアンスへの接続を参照してください。

制限的なユーザ アカウントとパスフレーズの設定値の構成

ユーザ アカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザ アカウントとパスフレーズ制限は、Cisco アプライアンスに定義されたローカル 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。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。
- **パスフレーズ存続期間のルール。**ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズのルール。**任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。

ユーザ アカウントとパスフレーズの制限は、[システム管理（System Administration）] > [ユーザ（Users）] ページの [ローカル ユーザ アカウントとパスフレーズの設定（Local User Account & Passphrase Settings）] セクションで定義します。

外部認証

ユーザ情報をネットワーク上の LDAP または RADIUS ディレクトリに保存した場合、アプライアンスにログインするユーザの認証に外部ディレクトリを使用するように Cisco アプライアンスを設定できます。認証のために外部ディレクトリを使用するようアプライアンスを設定するには、GUI で [システム管理（System Administration）] > [ユーザ（Users）] ページを使用するか、CLI で userconfig コマンドと external サブコマンドを使用します。

外部認証がイネーブルであり、ユーザが E メール セキュリティ アプライアンスにログインすると、アプライアンスは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、アプライアンスは最初に設定された外部サーバをチェックしてユーザがそこで定義されたかどうかを確認します。アプライアンスが最初の外部サーバに接続できなければ、アプライアンスは一覧の次の外部サーバをチェックします。

LDAP サーバの場合は、ユーザが外部サーバで認証に失敗すると、アプライアンスは E メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスフレーズを入力した場合は、アプライアンスへのアクセスが拒否されます。

外部 RADIUS サーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、アプライアンスは E メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。ただし、外部 RADIUS サーバが何らかの理由（パスフレーズ間違いやユーザ未登録など）でユーザを拒否すると、アプライアンスへのアクセスは拒否されます。

関連項目

- LDAP 認証のイネーブル化 （20 ページ）
- RADIUS 認証の有効化 （20 ページ）

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを Cisco ユーザ ロールに割り当てることができます。たとえば、IT グループのユーザを管理者ユーザ ロールに割り当てたり、Support グループのユーザをヘルプ デスク ユーザ ロールに割り当てたりできます。1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

（注） 外部ユーザが自分の LDAP グループのユーザ ロールを変更する場合は、アプライアンスからログアウトして再度ログインする必要があります。そうすれば、そのユーザに新しいロールの権限が付与されます。

はじめる前に

LDAP サーバの LDAP サーバプロファイルおよび外部認証クエリーを定義します。詳細については、LDAP クエリを参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザ（Users）] を選択します。
ステップ 2 [Web 認証（Web Authentication）] セクションまでスクロールします。
ステップ 3 [有効（Enable）] をクリックします。
ステップ 4 [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 5 認証タイプとして [LDAP] を選択します。
ステップ 6 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。
ステップ 7 ユーザを認証する LDAP 外部認証クエリーを選択します。
ステップ 8 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 9 アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。
ステップ 10 また、[行の追加（Add Row）] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対してステップ 9 とステップ 10 を繰り返します。
ステップ 11 変更を送信し、保存します。

RADIUS 認証の有効化

ユーザの認証に RADIUS ディレクトリを使用し、ユーザのグループを Cisco ロールに割り当てることもできます。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 Cisco ユーザ ロールに割り当てるために CLASS 属性を使用します）。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを Cisco ユーザ ロールに割り当てるには、最初に RADIUS サーバで <radius-group> という文字列値を使用して CLASS 属性を設定します（これは Cisco ユーザ ロールにマップされます）。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザはアプライアンスにログインできません。

アプライアンスが RADIUS サーバと通信できない場合、ユーザはアプライアンスのローカル ユーザ アカウントでログインできます。

（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は、アプライアンスからログアウトして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。

手順

ステップ 1 [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 すでに有効になっていない場合は、[外部認証を有効にする（Enable External Authentication）] オプションをオンにします。

ステップ 3 RADIUS サーバのホスト名を入力します。

ステップ 4 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 5 RADIUS サーバの共有秘密パスワードを入力します。

ステップ 6 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 7 （任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS サーバについて、3 ～ 6 のステップを繰り返します。

（注） 最大 10 個の RADIUS サーバを追加できます。

ステップ 8 RADIUS サーバに再度問い合わせ、「External Authentication Cache Timeout」フィールドで再認証するまで、AsyncOS が外部認証クレデンシャルを保存する秒数を入力します。デフォルトはゼロ（0）です。

（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 9 グループ マッピングの設定

設定	説明
外部認証されたユーザを複数のローカル ロールにマッピング。	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。 • admin • 管理者（Administrator） • 専門技術者 • Operator cloudadmin • Read-only Operator • ヘルプ デスク ユーザ • ゲスト
外部認証されたすべてのユーザを管理ロールにマップします。	AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 10 管理者ロールまたは異なるアプライアンス ユーザ ロール タイプにすべての外部認証されたユーザをマッピングするかを選択します。

ステップ 11 異なるロール タイプにユーザをマッピングする場合、[グループ名（Group Name）] または [ディレクトリ（Directory）] フィールドの RADIUS CLASS 属性に定義されているようにグループ名を入力し、[ロール（Role）] フィールドからアプライアンス ロール タイプを選択します。[行を追加（Add Row）] をクリックして、さらにロール マッピングを追加できます。

ユーザ ロール タイプの詳細については、ユーザ アカウントを使用する作業 （1 ページ）を参照してください。

ステップ 12 変更を送信し、保存します。

二要素認証

RADIUSディレクトリを使用して、特定のユーザロールの二要素認証を設定できます。アプライアンスは、RADIUS サーバとの通信用の次の認証プロトコルをサポートします。

- Password Authentication Protocol（PAP）
- Challenge Handshake Authentication Protocol（CHAP）

次のユーザ ロールに対して二要素認証を有効にできます。

- 定義済み
- カスタム

機能は次によりテストされています。

- RSA 認証マネージャ v8.2
- FreeRADIUS v1.1.7 以上
- ISE v1.4 以降

関連項目

- 二要素認証の有効化 （23 ページ）
- 二要素認証の無効化 （24 ページ）

二要素認証の有効化

はじめる前に

IT 管理者から二要素認証に必要な RADIUS サーバの詳細を入手していることを確認します。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザ（Users）]ページで、[二要素認証（Two-Factor Authentication）] の下の [有効にする（Enable）] をクリックします。

ステップ 2 RADIUS サーバのホスト名または IP アドレスを入力します。

ステップ 3 RADIUS サーバのポート番号を入力します。

ステップ 4 RADIUS サーバの共有秘密パスワードを入力します。

ステップ 5 タイムアウトまでに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 6 適切な認証プロトコルを選択します。

ステップ 7 （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。各 RADIUS サーバについて、2 ～ 6 のステップを繰り返します。

（注） 最大 10 個の RADIUS サーバを追加できます。

ステップ 8 二要素認証を有効にする必須ユーザ ロールを選択します。

ステップ 9 変更を送信し、保存します。

二要素認証を有効にすると、ユーザはアプライアンスにログインするために、ユーザ名とパスフレーズを入力した後にパスコードを入力することが求められます。

二要素認証の無効化

はじめる前に

お使いのアプライアンスで二要素認証を有効にしていることを確認します。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザ（Users）] ページで、[二要素認証（Two-Factor Authentication）] の下の [グローバル設定を編集（Edit Global Settings）] クリックします

ステップ 2 [二要素認証を有効にする（Enable Two-Factor Authentication）] の選択を解除します。

ステップ 3 変更を送信し、保存します。

E メール セキュリティ アプライアンスへのアクセスの設定

AsyncOS では E メール セキュリティ アプライアンスへのユーザ アクセスを管理するために、管理者は Web UI セッションのタイムアウトや、アプライアンスにアクセス可能なユーザ IP アドレスと組織のプロキシ サーバ IP アドレスを規定したアクセス リストなどを制御できます。

関連項目

- IP ベースのネットワーク アクセスの設定 （24 ページ）
- セッション タイムアウトの設定 （27 ページ）

IP ベースのネットワーク アクセスの設定

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で接続するユーザ（リモート ユーザに逆プロキシを使用する組織の場合）のアクセス リストを作成して、E メール セキュリティ アプライアンスにアクセスするユーザの IP アドレスを制御できます。

関連項目

- 直接接続 （25 ページ）
- プロキシ経由の接続 （25 ページ）
- ネットワーク アクセスを制限する際の重要な注意事項 （25 ページ）
- アクセス リストの作成 （26 ページ）

直接接続

E メール セキュリティ アプライアンスに接続可能なマシンの 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のアクセスは拒否されます。

プロキシ経由の接続

リモート ユーザのマシンと E メール セキュリティ アプライアンスの間で逆プロキシ サーバが使用される組織のネットワークの場合、AsyncOS ではアプライアンスに接続可能なプロキシの IP アドレスを含むアクセス 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 E 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 RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

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す。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）。E メール セキュリティ アプライアンスは、ヘッダーのリモート 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 リストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。

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

ネットワーク アクセスを制限する際の重要な注意事項

注意：次のいずれかの条件が true の場合、ネットワーク アクセスの変更を送信して確定した後、アプライアンスにアクセスできなくなることがあります。

- [特定の接続のみを許可（Only Allow Specific Connections）] を選択した場合は、現在のマシン（クラスタ化環境内の PC、E メール セキュリティ アプライアンス、またはセキュリティ管理アプライアンスなど）の IP アドレスをリストに含めないでください。
- [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、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシ リスト

に存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。

- [特定の直接接続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、
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合

    または

  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

アクセス リストの作成

ネットワーク アクセス リストは、GUI または **adminaccessconfig > ipaccess** CLI コマンドを使用して作成できます。

はじめる前に

ネットワーク アクセスの設定を変更後、アプライアンスからロックアウトされないようにします。ネットワーク アクセスを制限する際の重要な注意事項 （25 ページ）を参照してください。

手順

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

ステップ 2 [設定の編集（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。

オプション	説明
すべてを許可（Allow All）	このモードはアプライアンスへの接続をすべて許可します。 これが操作のデフォルト 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。

オプション	説明
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、次の条件を満たせば、逆プロキシ経由で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、アクセス リストの [プロキシサーバのIPアドレス（IP Address of Proxy Server）] フィールドに含まれている。 • プロキシの接続要求に **x-forwarded-header** HTTP ヘッダーが記載されている。 • **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 リスト内のユーザに対して定義された 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、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、アプライアンスへの逆プロキシ経由接続または直接接続を許可します。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードと同じです。

ステップ 4 アプライアンスへの接続を許可するユーザの 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。複数のエントリを指定する場合は、カンマで区切ります。

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

1. アプライアンスへの接続を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
2. 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。デフォルトのヘッダー名は x-forwarded-for です。

ステップ 6 変更を送信および確定後にアプライアンスからロックアウトされる変更が構成されていないことを確認します。

ステップ 7 変更を送信し、保存します。

セッション タイムアウトの設定

• Web UI セッション タイムアウトの設定 （28 ページ）
• CLI セッション タイムアウトの設定 （28 ページ）

Web UI セッション タイムアウトの設定

非アクティブな状態によりログアウトになるまで、E メール セキュリティ アプライアンスの Web UI にログイン可能な期間を指定できます。この Web UI セッション タイムアウトは以下に適用されます。

- すべてのユーザ（管理者を含む）
- HTTP セッションおよび HTTPS セッション
- Cisco スパム隔離

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。

手順

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

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

ステップ 3 ログアウトまでにユーザを非アクティブにできる分数を [Web UI 非アクティブ タイムアウト（Web UI Inactivity Timeout）] フィールドに入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 4 変更を送信し、保存します。

次のタスク

また、CLI で adminaccessconfig コマンドを使用して Web UI セッション タイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

CLI セッション タイムアウトの設定

ユーザが非アクティブであるために AsyncOS がそのユーザをログアウトするまで、電子メール セキュリティ アプライアンスにユーザがログインできる期間を指定できます。以下に CLI セッション タイムアウトが適用されます。

- すべてのユーザ（管理者を含む）
- セキュア シェル（SSH）、SCP、および直接シリアル接続を使用している接続のみ

（注） CLIセッション タイムアウト時に未確定の設定変更は失われます。設定を変更したらすぐに確定してください。

手順

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

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

ステップ 3 [CLI 非アクティブ タイムアウト（CLI Inactivity Timeout）] フィールドに、ログアウトされるまでにユーザを非アクティブにできる分数を入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 4 変更を送信し、保存します。

次のタスク

また、CLI で adminaccessconfig コマンドを使用して CLI セッション タイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

管理ユーザへのメッセージの表示

- ログイン前のメッセージの表示 （29 ページ）
- ログイン後のメッセージの表示 （29 ページ）

ログイン前のメッセージの表示

ユーザが SSH、FTP、または Web UI からアプライアンスにログインしようとする前にメッセージを表示するように電子メールセキュリティアプライアンスを設定できます。ログインバナーは、ログインプロンプトの上に表示されるカスタマイズ可能なテキストです。ログインバナーを使用して、内部のセキュリティ情報またはアプライアンスのベストプラクティスに関する説明を表示できます。たとえば、許可しないアプライアンスの使用を禁止する簡単な注意文言を作成したり、ユーザがアプライアンスに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の adminaccessconfig > banner コマンドを使用して、ログイン バナーを作成します。ログイン バナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログイン バナーは、アプライアンスの /data/pub/configuration ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

ログイン後のメッセージの表示

ユーザが SSH、FTP、または Web UI を使用してアプライアンスに正常にログインした後に、ウェルカム バナーを表示するように AsyncOS を設定できます。ウェルカム バナーを使用して、内部のセキュリティ情報またはアプライアンスのベストプラクティスに関する説明を表示できます。

CLI で adminaccessconfig > welcome コマンドを使用して、ウェルカム バナーを作成します。ウェルカム バナーの最大長は 1600 文字です。

ウェルカム バナーは、アプライアンスの /data/pub/configuration ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

セキュア シェル（SSH）キーの管理

sshconfig コマンドを使用して、次の操作を実行します。

- システムで設定されたユーザ アカウント（admin アカウントを含む）の authorized_keys ファイルにセキュア シェル（SSH）公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスフレーズチャレンジではなく SSH キーを使用してユーザ アカウントを認証できるようになります。
- 次の SSH サーバの設定を編集できます。
  - 公開キー認証アルゴリズム
  - 暗号アルゴリズム
  - KEX アルゴリズム
  - MAC メソッド
  - 最小サーバ キー サイズ

（注） Cisco アプライアンスから他のホスト マシンへのログ ファイルの SCP プッシュを実行する場合に使用されるホスト キーを設定するには、**logconfig -> hostkeyconfig** を使用します。詳細については、ログを参照してください。

hostkeyconfig を使用すると、リモート ホストのキーをスキャンし、Cisco アプライアンスに追加できます。

関連項目

- 例：新しい公開キーのインストール （30 ページ）
- 例：SSH サーバ設定の編集 （31 ページ）

例：新しい公開キーのインストール

次の例では、管理者アカウントの新規公開キーをインストールします。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
```

```
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

例：SSH サーバ設定の編集

次に、SSH サーバ設定を編集する方法の例を示します。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
```

```
[rsa1,ssh-dss,ssh-rsa]> rsa1
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
Cipher Algorithms:
        aes192-ctr
MAC Methods:
        hmac-sha1
Minimum Server Key Size:
        2048
KEX Algorithms:
        diffie-hellman-group-exchange-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

リモート SSH コマンド実行

CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。たとえば、Cisco アプライアンスで admin アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモート ホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

管理ユーザ アクセスのモニタリング

目的	操作手順
アプライアンスについて、アクティブユーザすべてのセッション詳細を表示する	ページ右上で [オプション（Options）] > [アクティブなセッション（Active Sessions）] をクリックします コマンドライン インターフェイスで、w、whoami および who コマンドを使用します。

目的	操作手順
アプライアンスに最近ログインしたユーザを表示する また、リモート ホストの IP アドレス、ログイン時間、ログアウト時間、および合計時間も表示する	コマンドライン インターフェイスで last コマンドを使用します。