ユーザ設定の指定

ホーム ページ、アカウント パスワード、タイム ゾーン、ダッシュボード、イベント ビューの設定など、単一のユーザ アカウントに関連付けられたプリファレンスを設定できます。

ユーザ ロールに応じて、パスワード、イベント ビューのプリファレンス、タイム ゾーンの設定、ホーム ページのプリファレンスなど、ユーザ アカウントに固有のプリファレンスを指定できます。詳細については、次の各項を参照してください。

- パスワードの変更（71-1 ページ）では、ユーザ アカウントのパスワードを変更する方法を説明します。
- ホームページの指定（71-2 ページ）では、既存のページの 1 つをデフォルトのホーム ページとして使用する方法を説明します。この値を設定した後は、このページがアプライアンスにログインする際に最初に表示されるページになります。
- イベント ビュー設定の設定（71-3 ページ）では、イベント プリファレンス設定によって、イベントの表示内容がどのように変化するかを説明します。
- デフォルトのタイム ゾーン設定（71-8 ページ）では、ユーザ アカウントのタイム ゾーンを設定する方法、およびその設定によって、表示されるイベントのタイムスタンプがどのように変化するかを説明します。
- デフォルトのダッシュボードの指定（71-9 ページ）では、どのダッシュボードをデフォルトのダッシュボードとして使用するかを選択する方法を説明します。

パスワードの変更

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 2、シリーズ 3

サポートされる防御センター：任意（Any）

すべてのユーザ アカウントはパスワードで保護されています。パスワードはいつでも変更することができ、ユーザ アカウントの設定によっては定期的にパスワードを変更しなければならない場合もあります。期限切れのパスワードの変更（71-2 ページ）を参照してください。

パスワードの強度チェックが有効な場合、パスワードは 8 文字以上の英数字からなり、大文字と小文字、および 1 つ以上の数字を使用する必要があることに注意してください。辞書に記載されている単語や、同じ文字を連続して使用することはできません。

（注） LDAP または RADIUS ユーザの場合、Web インターフェイスを介してパスワードを変更することはできません。

パスワードを変更するには、次の手順を実行します。

アクセス: 任意（Any）

手順 1　ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

[パスワードの変更（Change Password）] ページが表示されます。

手順 2　[現在のパスワード（Current Password）] フィールドに、現在のパスワードを入力して、[変更（Change）] をクリックします。

手順 3　[新しいパスワード（New Password）] および [確認（Confirm）] フィールドに、新しいパスワードを入力します。

手順 4　[変更（Change）] をクリックします。

新しいパスワードがシステムによって受け入れられると、成功を示すメッセージが表示されます。

期限切れのパスワードの変更

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 2、シリーズ 3

サポートされる防御センター: 任意（Any）

ユーザ アカウントの設定によっては、パスワードが期限切れになることがあります。パスワードの有効期間は、アカウントが作成されたときに設定され、変更できないことに注意してください。パスワードが期限切れになった場合、[パスワード有効期限の警告（Password Expiration Warning）] ページが表示されます。

パスワード有効期限の警告に応答するには、次のようにします。

アクセス: 任意（Any）

手順 1　次の 2 つの選択肢があります。

- すぐにパスワードを変更するには、[パスワードの変更（Change Password）] をクリックします。

  残りの警告日数がゼロの場合は、パスワードを変更する**必要があります**。また、パスワードの強度チェックが有効な場合、パスワードは 8 文字以上の英数字からなり、大文字と小文字、および 1 つ以上の数字を使用する必要があります。辞書に記載されている単語や、同じ文字を連続して使用することはできません。
- 後でパスワードを変更するには、[スキップ（Skip）] をクリックします。

ホームページの指定

ライセンス: 任意（Any）

Web インターフェイス内のページをアプライアンスのホームページに指定できます。デフォルトのホームページはサマリー ダッシュボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）ですが、ダッシュボードにアクセスできないユーザ アカウントの場合は [ようこそ（Welcome）] ページが使用されます。

ホームページを指定するには、次のようにします。

アクセス：External Database User を除くすべてのユーザ

手順 1　ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

[パスワードの変更（Change Password）] ページが表示されます。

手順 2　[ホームページ（Home Page）] をクリックします。

[ホームページ（Home Page）] ページが表示されます。

手順 3　ホームページとして使用するページをドロップダウン リストから選択します。

ドロップダウン リスト内のオプションは、ユーザ アカウントのアクセス権限に基づいて表示されます。詳細については、ユーザ アカウント特権について（61-61 ページ）を参照してください。

手順 4　[保存（Save）] をクリックします。

ホームページの設定が保存されます。

イベント ビュー設定の設定

ライセンス：任意（Any）

[イベント ビューの設定（Event View Settings）] ページを使用して、FireSIGHT システムのイベント ビューの特性を設定します。一部のイベント ビュー設定は、特定のユーザ ロールでのみ使用可能であることに注意してください。External Database User ロールを持つユーザは、イベント ビュー設定のユーザ インターフェイスの一部を表示できますが、それらの設定を変更しても意味のある結果は生じません。詳しくは、以下にリンクされている個々の項を参照してください。

イベントのプリファレンスを設定するには、次のようにします。

アクセス：機能に応じて異なる

手順 1　ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

[ユーザ設定（User Preferences）] ページが表示されます。

手順 2　[イベント ビューの設定（Event View Settings）] をクリックします。

[イベント ビューの設定（Event View Settings）] ページが表示されます。

手順 3　イベント ビューの基本特性を設定します。

詳細については、イベント設定（71-4 ページ）を参照してください。

手順 4　ファイルのダウンロード設定を設定します。

詳細については、ファイル設定（71-5 ページ）を参照してください。

手順 5　デフォルトの時間枠を設定します（複数可）。

詳細については、デフォルトの時間枠（71-6 ページ）を参照してください。

手順 6　デフォルトのワークフローを設定します。

詳細については、デフォルトのワークフロー（71-8 ページ）を参照してください。

手順 7　[保存（Save）] をクリックします。

変更が反映されます。

イベント設定

ライセンス:任意（Any）

[イベント ビューの設定（Event View Settings）] ページの [イベント設定（Event Preferences）] セクションを使用して、FireSIGHT システムのイベント ビューの基本特性を設定します。このセクションはすべてのユーザ ロールで使用可能ですが、イベントを表示できないユーザには、ほとんどまたはまったく意味がありません。

以下のフィールドが [イベント設定（Event Preferences）] セクションに表示されます。

- [「すべて」の操作を確認（Confirm “All” Actions）] フィールドは、イベント ビューのすべてのイベントに影響を与える操作について、アプライアンスがユーザに確認を要求するかどうかを制御します。

  たとえば、この設定が有効な状態でイベント ビューの [すべて削除（Delete All）] をクリックした場合、アプライアンスがデータベースからこれらを削除する前に、現在の制約を満たすすべてのイベント（現在のページに表示されていないイベントを含む）を削除することをユーザが確認する必要があります。

- [IP アドレスの解決（Resolve IP Addresses）] フィールドを使用すると、可能な場合には常に、アプライアンスで IP アドレスの代わりにホスト名がイベント ビューに表示されるようになります。

  多数の IP アドレスが含まれている場合、このオプションを有効にすると、イベント ビューの表示に時間がかかる可能性があることに注意してください。この設定が有効になるためには、システム設定で DNS サーバが設定済みでなければならないことにも注意してください。管理インターフェイスの構成（64-9 ページ）を参照してください。

- [パケット ビューの展開（Expand Packet View）] フィールドでは、侵入イベントのパケット ビューをどのように表示するかを設定できます。デフォルトでは、アプライアンスによるパケット ビューは折りたたまれた状態で表示されます。
  - [なし（None）]:パケット ビューの [パケット情報（Packet Information）] セクションのサブセクションをすべて折りたたんだ状態にします。
  - [パケット テキスト（Packet Text）]:[パケット テキスト（Packet Text）] サブセクションのみを展開します。
  - [パケット バイト（Packet Bytes）]:[パケット バイト（Packet Bytes）] サブセクションのみを展開します。
  - [すべて（All）]:すべてのセクションを展開します。

  デフォルト設定に関係なく、パケット ビューのセクションを手動で展開することで、検出されたパケットに関する詳細情報をいつでも表示できます。パケット ビューの詳細については、パケット ビューの使用（41-25 ページ）を参照してください。

- [ページごとの行数（Rows Per Page）] フィールドは、ドリル ダウン ページとテーブル ビューに表示する、ページごとのイベントの行数を制御します。
- [更新間隔（Refresh Interval）] フィールドは、イベント ビューの更新間隔を分数で設定します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。

- [統計情報の更新間隔(Statistics Refresh Interval)] は、[侵入イベント統計(Intrusion Event Statistics)] や [ディスカバリ統計(Discovery Statistics)] ページなどのイベントのサマリー ページの更新間隔を制御します。「0」を入力すると、更新オプションが無効になります。この間隔はダッシュボードに適用されないことに注意してください。
- [非アクティブ化ルール(Deactivate Rules)] フィールドは、標準テキスト ルールによって生成される侵入イベントのパケット ビューに、どのリンクが表示されるかを次のように制御します。
  - [すべてのポリシー(All Policies)]: ローカルで定義されているすべてのカスタム侵入ポリシーに含まれる標準テキスト ルールを非アクティブ化する単一リンク
  - [現在のポリシー(Current Policy)]: 現在適用中の侵入ポリシーのみに含まれる標準テキスト ルールを非アクティブ化する単一リンク。デフォルトのポリシーのルールは非アクティブ化できないことに注意してください。
  - [確認する(Ask)]: これらの個々のオプションへのリンク

  パケット ビューでこれらのリンクを表示するには、Administrator または Intrusion Admin のアクセス権があるユーザ アカウントが必要です。

ファイル設定

ライセンス: 任意(Any)

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

[イベント ビューの設定(Event View Settings)] ページの [ファイル設定(File Preferences)] セクションを使用して、ローカル ファイル ダウンロードの基本特性を設定します。このセクションは、Administrator、Security Analyst、または Security Analyst(読み取り専用)ユーザ ロールを持つユーザのみが利用できます。

検出されたファイルのダウンロードをアプライアンスがサポートしていない場合、これらのオプションは無効になることに注意してください。DC500 ではMalware ライセンスを使用できないので、それらのアプライアンスを使用してファイルをダウンロードしたり、これらのオプションを変更したりすることはできません。

以下のフィールドが [ファイル設定(File Preferences)] セクションに表示されます。

- [「ファイルのダウンロード」アクションを確認(Confirm 'Download File' Actions)] チェックボックスは、[ファイルのダウンロード(File Download)] ポップアップ ウィンドウが表示されるかどうかを制御します。このウィンドウは、ファイルをダウンロードするたびに、警告を表示して続行するかキャンセルするかを選択するように促します。

注意　シスコは、有害な結果が生じるのを防ぐために、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先をセキュアにするために必要な予防措置を行っていることを確認します。

ファイルをダウンロードする際には、いつでもこのオプションを無効にできます。ファイルのダウンロード方法に関する詳細は、保存されているファイルの別の場所へのダウンロード(40-4 ページ)を参照してください。

- キャプチャされたファイルをダウンロードすると、そのファイルを含むパスワード保護された .zip アーカイブがシステムによって作成されます。[Zip ファイルのパスワード（Zip File Password）] フィールドで、zip ファイルへのアクセスを制限するためにユーザが使用するパスワードを定義します。このフィールドを空欄にすると、パスワードなしのアーカイブ ファイルがシステムによって作成されます。
- [Zip ファイル パスワードの表示（Show Zip File Password）] チェック ボックスで、[Zip ファイルのパスワード（Zip File Password）] フィールドにプレーン テキストを表示するか不明瞭な文字を表示するかを切り替えます。このフィールドをオフにすると、[Zip ファイルのパスワード（Zip File Password）] には不明瞭な文字が表示されます。

デフォルトの時間枠

ライセンス：任意（Any）

時間枠（時間範囲と呼ばれることもある）は、任意のイベント ビューでイベントに時間制約を課します。[イベント ビューの設定（Event View Settings）] ページの [デフォルトの時間枠（Default Time Windows）] セクションを使用して、時間枠のデフォルト動作を制御します。

このセクションへのユーザ ロール アクセスは以下のとおりです。

- Administrators と Maintenance Users は、セクション全体にアクセスできます。
- Security Analysts と Security Analysts（読み取り専用）は、[監査ログの時間枠（Audit Log Time Window）] 以外のすべてのオプションにアクセスできます。
- Access Admins、Discovery Admins、External Database Users、Intrusion Admins、Network Admins、および Security Approvers は、[イベントの時間枠（Events Time Window）] オプションにのみアクセスできます。

デフォルトの時間枠設定に関係なく、イベントの分析中にはいつでも手動で個別のイベント ビューの時間枠を変更できます。また、時間枠の設定は、現在のセッションのみに有効であることにも注意してください。ログアウトしてから再ログインすると、時間枠はこのページで設定したデフォルトにリセットされます。詳細については、イベント時間の制約の設定（58-27 ページ）を参照してください。

デフォルトの時間枠を設定できるイベントには、次に示す 3 つのタイプがあります。

- [イベントの時間枠（Events Time Window）] は、時間で制約できるほとんどのイベントに関して、デフォルトの時間枠を 1 つ設定します。
- [監査ログの時間枠（Audit Log Time Window）] は、監査ログ用のデフォルトの時間枠を設定します。
- [ヘルス モニタリングの時間枠（Health Monitoring Time Window）] は、ヘルス イベント用のデフォルトの時間枠を設定します。

ユーザ アカウントがアクセスできるイベント タイプに関してのみ、時間枠を設定できます。すべてのユーザ タイプは、イベントの時間枠を設定できます。Administrators、Maintenance Users、および Security Analysts は、ヘルス モニタリングの時間枠を設定できます。Administrators と Maintenance Users は、監査ログの時間枠を設定できます。

すべてのイベント ビューを時間で制約できるとは限りません。このため、時間枠を設定してもホスト、ホスト属性、アプリケーション、クライアント、脆弱性、ユーザの ID、ホワイトリスト違反を表示するイベント ビューは影響を受けないことに注意してください。

複数の時間枠を使用して、上記の各タイプのイベントに 1 つずつ適用するか、または**単一の**時間枠を使用して、それをすべてのイベントに適用することができます。単一の時間枠を使用すると、3 つのタイプの時間枠用の設定が非表示になり、新しく [グローバルな時間枠（Global Time Window）] 設定が表示されます。

以下の 3 つのタイプの時間枠があります。

- [静的（static）]：特定の開始時刻から特定の終了時刻までに生成されたすべてのイベントを表示します
- [拡張（expanding）]：特定の開始時刻から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠が拡張され、新しいイベントがイベント ビューに追加されます。
- [スライド（sliding）]：特定の開始時刻（たとえば 1 日前）から現在までに生成されたすべてのイベントを表示します。時間の進行と共に時間枠は「スライド」し、設定した範囲内（この例では直前の 1 日）のイベントだけが表示されます。

すべての時間枠の最大時間範囲は、1970 年 1 月 1 日午前 0 時（UTC）～ 2038 年 1 月 19 日午前 3 時 14 分 7 秒です。

[時間枠の設定（Time Window Settings）] ドロップダウン リストに、次のオプションが表示されます。

- [最後を表示（スライド型）（Show the Last - Sliding）]：このオプションで、指定した長さのデフォルト時間枠をスライド型で設定できます。

  アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューの変更と共に、時間枠は「スライド」して、常に最後の 1 時間内のイベントが表示されます。

- [最後を表示（静的/拡張）（Show the Last - Static/Expanding）]：このオプションで、指定した長さのデフォルトの時間枠を静的または拡張のどちらかに設定できます。

  静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、特定の開始時間（1 時間前など）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、特定の開始時刻（たとえば 1 時間前）から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。

- [現在の日付（静的/拡張）（Current Day - Static/Expanding）]：このオプションで、現在の日付のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の日付は、現行セッションのタイム ゾーン設定に基づいて午前 0 時に始まります。

  静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

  拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 24 時間を超えて分析を続けた場合、この時間枠は 24 時間よりも長くなる可能性があることに注意してください。

- [現在の週（静的/拡張）（Current Week - Static/Expanding）]：このオプションで、現在の週のデフォルトの時間枠を静的または拡張のどちらかに設定できます。現在の週は、現行セッションのタイム ゾーン設定に基づいて直前の日曜日の午前 0 時に始まります。

  静的時間枠の場合は、[終了時刻を使用（Use End Time）] チェック ボックスをオンにします。アプライアンスは、午前 0 時からユーザがイベントを初めて確認した時刻までに生成されたすべてのイベントを表示します。イベント ビューを変更しても時間枠は固定されており、静的な時間枠の間に発生したイベントのみが表示されます。

拡張時間枠にするには、[終了時刻を使用（Use End Time）] チェック ボックスをオフにします。アプライアンスは、日曜日の午前 0 時から現在までに生成されたすべてのイベントを表示します。イベント ビューを変更すると、時間枠は現在まで拡張されます。ログアウトする前に 1 週間を超えて分析を続けた場合、この時間枠は 1 週間よりも長くなる可能性があることに注意してください。

デフォルトのワークフロー

ライセンス：任意（Any）

ワークフローとは、アナリストがイベント評価で使用するデータが表示された一連のページです。アプライアンスには、各イベント タイプに少なくとも 1 つの定義済みワークフローが付属しています。たとえば、Security Analyst の場合、実行する分析のタイプに応じて、それぞれが侵入イベントのデータを別の形式で示している、10 の異なる侵入イベントのワークフローから選択できます。

アプライアンスには、イベント タイプごとにデフォルトのワークフローが設定されています。たとえば、侵入イベントでは、[優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローがデフォルトになります。したがって、侵入イベント（確認済みの侵入イベントを含む）を表示するたびに、アプライアンスは [優先順位および分類に基づいたイベント（Events by Priority and Classification）] ワークフローを表示します。

ただし、[イベント ビューの設定（Event View Settings）] ページの [デフォルトのワークフロー（Default Workflows）] セクションを使用すると、各イベント タイプのデフォルトのワークフローを変更できます。

設定可能なデフォルトのワークフローは、ユーザ ロールによって異なることに注意してください。たとえば、侵入イベントのアナリストは、ディスカバリ イベントのデフォルト ワークフローを設定できません。ワークフローの一般情報については、ワークフローの概要と使用（58-1 ページ）を参照してください。

デフォルトのタイム ゾーン設定

ライセンス：任意（Any）

イベントの表示に使用するタイム ゾーンを、アプライアンスが使用している標準 UTC 時間から変更できます。設定したタイム ゾーンは現在のユーザ アカウントにのみ適用され、タイム ゾーンをさらに変更するまで有効になります。

注意　タイム ゾーン機能は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。ローカル タイム ゾーンを使用するようにアプライアンスのシステム クロックを変更した場合は、アプライアンスで正確なローカル時刻が表示されるように、それを変更して UTC 時間に戻す必要があります。防御センター と管理対象デバイスの時間を同期させる方法について詳しくは、時間の同期（63-28 ページ）を参照してください。

タイム ゾーンを変更するには、次のようにします。

アクセス：任意（Any）

手順 1　ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

[パスワードの変更（Change Password）] ページが表示されます。

手順 2　[タイム ゾーンの設定（Time Zone Settings）] をクリックします。

[タイム ゾーン設定（Time Zone Preference）] ページが表示されます。

手順 3　左側のリスト ボックスで、使用するタイム ゾーンを含む大陸または地域を選択します。

たとえば、北米、南米、カナダで標準のタイム ゾーンを使用する場合は、[アメリカ（America）] を選択します。

手順 4　右側のリスト ボックスで、使用するタイム ゾーンに対応するゾーン（都市名）を選択します。

たとえば、東部標準時を使用する場合は、最初のタイム ゾーン ボックスで [アメリカ（America）] を選択した後に、[ニューヨーク（New York）] を選択します。

手順 5　[保存（Save）] をクリックします。

タイム ゾーンが設定されます。

デフォルトのダッシュボードの指定

ライセンス：任意（Any）

アプライアンスにあるダッシュボードの 1 つをデフォルトのダッシュボードとして指定できます。デフォルトのダッシュボードは、[概要（Overview）] > [ダッシュボード（Dashboards）] を選択すると表示されます。デフォルトのダッシュボードが定義されていない場合は、[ダッシュボードのリスト（Dashboard List）] ページが表示されます。ダッシュボードの一般情報については、ダッシュボードの使用（55-1 ページ）を参照してください。

デフォルトのダッシュボードを指定するには、次のようにします。

アクセス：Admin/Maint/Any Security Analyst

手順 1　ユーザ名の下にあるドロップダウン リストから、[ユーザ設定（User Preferences）] を選択します。

[パスワードの変更（Change Password）] ページが表示されます。

手順 2　[ダッシュボードの設定（Dashboard Settings）] をクリックします。

[ダッシュボードの設定（Dashboard Settings）] ページが表示されます。

手順 3　デフォルトとして使用するダッシュボードをドロップダウン リストから選択します。

[なし（None）] を選択した場合、[概要（Overview）] > [ダッシュボード（Dashboards）] を選択すると [ダッシュボードのリスト（Dashboard List）] ページが表示されます。その後、表示するダッシュボードを選択できます。

手順 4　[保存（Save）] をクリックします。

デフォルトのダッシュボード設定が保存されます。