FireSIGHT システム のライセンス

組織に対して FireSIGHT システム の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。Defense Center を使用して、それ自体およびその管理対象のデバイスを管理できます。

詳細については、以下を参照してください。

ライセンスについて

ライセンス：任意（Any）

組織に対して FireSIGHT システム の最適な展開を実現するために、さまざまな機能についてライセンスを取得することができます。FireSIGHT ライセンスは Defense Center に含まれており、ホスト、アプリケーション、およびユーザ ディスカバリの実行に必要です。

追加のモデル固有ライセンスにより、管理対象デバイスは次のようなさまざまな機能を実行できます。

- 侵入検知と防御
- セキュリティ インテリジェンス フィルタリング
- ファイル制御および高度なマルウェア防御
- アプリケーション、ユーザ、および URL 制御
- スイッチングとルーティング
- デバイス クラスタリング
- ネットワーク アドレス変換（NAT）
- バーチャル プライベート ネットワーク（VPN）導入環境

FireSIGHT システム のライセンス付き機能にアクセスできなくなる状況がいくつかあります。Defense Center からライセンスを削除できますが、これはこの防御センターにより管理されているすべてのデバイスに影響します。特定の管理対象デバイスでライセンス付き機能を無効にすることもできます。最後に、一部のライセンスには有効期限が設定されています。いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

FireSIGHT ライセンスのような特定のライセンスは永続的です。他のライセンスの場合は、ライセンスを有効にするためにサービス サブスクリプションを購入する必要があります。

詳細については、以下を参照してください。

- ライセンスのタイプと制約事項（65-2 ページ）
- サービス サブスクリプション（65-8 ページ）
- ハイ アベイラビリティ ペアのライセンス（65-9 ページ）
- スタック構成デバイスおよびクラスタ構成デバイスのライセンス（65-9 ページ）
- シリーズ 2 アプライアンスのライセンス付与（65-9 ページ）
- FireSIGHT ホストおよびユーザ ライセンスの制限について（65-10 ページ）

ライセンスのタイプと制約事項

ライセンス：任意（Any）

ここでは、FireSIGHT システム 導入環境で使用可能なライセンスのタイプについて説明します。アプライアンスで有効にできるライセンスは、アプライアンスのモデル、バージョン、および（一部の管理対象デバイスの場合）他の有効なライセンスに応じて異なります。

仮想デバイスおよびシリーズ 3 デバイスの場合、ライセンスはモデルによって異なります。管理対象デバイスのライセンスは、ライセンスがデバイスのモデルと正確に一致しない場合は有効にできません。たとえば、3D8140 デバイスで Protection 機能を有効にする場合に 3D8250 Protection ライセンスは使用できません。組織と導入環境の拡大に伴い、管理対象デバイスを追加し、その追加ライセンスを購入できます。

シリーズ 2 デバイスには Protection 機能（Security Intelligence フィルタリングを除く）が自動的に組み込まれます。シリーズ 2 デバイスで Protection を明示的に有効化する必要はありませんが、その他のライセンスを有効にすることもできません。

また、ユーザ制御とアプリケーション制御を実行するために、仮想デバイスまたは ASA FirePOWER デバイスで Control を有効にできますが、これらのデバイスではスイッチング、ルーティング、スタック構成、クラスタリングがサポートされないので注意してください。

次の表に、FireSIGHT システム ライセンスの要約を示します。

表 65-1　FireSIGHT システム ライセンス

FireSIGHT システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	要件	有効期限設定可/不可
FireSIGHT	none	Defense Center	検出	none	No
Protection（ライセンス済み）	TA（デバイスに付属）	シリーズ 3、仮想、X-シリーズ、ASA FirePOWER	侵入検知と防御 ファイル制御 セキュリティ インテリジェンス フィルタリング	none	No

表 65-1　FireSIGHT システム ライセンス(続き)

FireSIGHT システムで割り当てるライセンス	購入するサービス サブスクリプション	プラットフォーム	付与される機能	要件	有効期限設定可/不可
Protection(自動)	なし(デバイスに付属)	シリーズ 2	侵入検知と防御 ファイル制御	none	No
Control	なし(デバイスに付属)	仮想、ASA FirePOWER。	ユーザおよびアプリケーション制御	Protection	No
Control	なし(デバイスに付属)	シリーズ 3	ユーザおよびアプリケーション制御 スイッチングとルーティング クラスタリング	Protection	No
Malware	TAM、TAMC、または AMP	シリーズ 3、仮想、ASA FirePOWER	高度なマルウェア防御(ネットワークベースのマルウェアの検出とブロッキング)	Protection	Yes
URL フィルタリング(URL Filtering)	TAC、TAMC、または URL	シリーズ 3、仮想、X-シリーズ、ASA FirePOWER	カテゴリとレピュテーションに基づく URL フィルタリング	Protection	Yes
VPN	なし(詳細は販売担当者までお問い合わせください)	シリーズ 3	仮想プライベート ネットワークの導入	Control	Yes

ただし、DC500 Defense Center は URL フィルタリング(URL Filtering) または Malware のライセンスよって提供される機能をサポートしていません。

詳細については、以下を参照してください。

- FireSIGHT(65-3 ページ)
- Protection(65-4 ページ)
- Control(65-5 ページ)
- Malware(65-7 ページ)
- URL フィルタリング(URL Filtering)(65-6 ページ)
- VPN(65-8 ページ)

FireSIGHT

ライセンス: FireSIGHT

FireSIGHT ライセンスは Defense Center に含まれており、このライセンスによりホスト、アプリケーション、およびユーザのディスカバリを実行できます。ディスカバリ データにより、システムは完全かつ最新のネットワーク プロファイルを作成し、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ識別情報に関連付けることができます。ディスカバリ データを使用して、トラフィック プロファイリングを実行し、ネットワーク コンプライアンスを評価し、および相関ポリシーを実装することができます。

FireSIGHT ライセンスは、Defense Center とその管理対象デバイスで監視できる個々のホストおよびユーザの数も決定します。ユーザ制限が次の項目に*単独*で適用されることに注意してください。

- Users データベース（FireSIGHT システム で検出された各ユーザのレコードを格納）
- ユーザ制御を実行するためアクセス制御ルールで使用できるユーザ（別名「*アクセス制御ユーザ*」）の数

ライセンス制限に達した場合の結果の詳細については、FireSIGHT ホストおよびユーザ ライセンスの制限について（65-10 ページ）を参照してください。

FireSIGHT のライセンスがない状態でも、基本的なシステム設定、監視、ネットワークベースのアクセス制御（ゾーン、ネットワーク、VLAN、およびポート ルールの条件）、接続のロギング、レポートを実行できます。また、FireSIGHT ライセンスがない状態でも Collective Security Intelligence クラウド からエンドポイントに基づくマルウェア イベントを受信できますが、組織に FireAMP サブスクリプションが必要です。

ヒント　このマニュアルのライセンスに関する説明では、Defense Center に FireSIGHT ライセンスがあることを前提としています。ただし、Defense Center バージョン 4.10.x が以前稼働していた場合は、FireSIGHT ライセンスの代わりに RNA Host および RUA User ライセンス（レガシー）を使用できる場合があります。詳細については、Protection（65-4 ページ）を参照してください。

Protection

ライセンス：Protection

サポートされるデバイス：シリーズ 3、仮想、X-シリーズ、ASA FirePOWER

Protection ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンスのフィルタリングを実行できます。

- *侵入検知および防御*により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- *ファイル制御*により、特定のアプリケーション プロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。Malware ライセンス（Malware（65-7 ページ）を参照）では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- *Security Intelligence フィルタリング*により、トラフィックをアクセス コントロール ルールによる分析対象にする前に、特定の IP アドレスをブラックリストに追加（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミック フィードにより、最新の情報に基づいて接続をただちにブラックリストに追加できます。オプションで、セキュリティ インテリジェンス フィルタリングに「モニタのみ」設定を使用できます。

保護ライセンスは（制御ライセンスとともに）、管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションを購入する必要があります。

ライセンスがない状態でも Protection 関連の検査を実行するようにアクセス制御ポリシーを設定できますが、最初に Protection ライセンスを Defense Center に追加してから、ポリシー適用対象デバイスでこのライセンスを有効にするまではポリシーを適用できません。

Protection ライセンスを Defense Center から削除するか、または管理対象デバイスで Protection を無効にすると、Defense Center は対象デバイスからの侵入イベントとファイル イベントを認識しなくなります。結果として、トリガー条件としてこれらのイベントを使用する相関ルールがトリ

ガーしなくなります。また、Defense Center は シスコ によって提供される情報またはサードパーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。Protection を再度有効にするまでは、既存のポリシーを再適用できません。

Protection ライセンスは URL フィルタリング（URL Filtering）、Malware、および Control ライセンスに必要であるため、Protection ライセンスを削除または無効にすると、URL フィルタリング（URL Filtering）、Malware、または Control ライセンスを削除または無効にすることと同じ効果があります。

(注)　シリーズ 2 デバイスにはほとんどの Protection 機能が自動的に組み込まれるため、これらのデバイスの Protection ライセンスを購入または有効にする必要はありません。ただし シリーズ 2 デバイスは Security Intelligence フィルタリングを実行できません。

Control

ライセンス: Control

サポートされるデバイス: シリーズ 3、仮想、ASA FirePOWER

サポートされる防御センター: 機能に応じて異なる

Control ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。また、スイッチングおよびルーティング（DHCP リレーおよび NAT を含む）を実行するように シリーズ 3 管理対象デバイスを設定し、クラスタ管理対象デバイスを設定することができます。管理対象デバイス上で Control を有効にするには、Protection も有効にする必要があります。

(注)　仮想デバイスまたは ASA FirePOWER デバイスで Control ライセンスを有効にできますが、これらのデバイスではスイッチング、ルーティング、スタック構成、またはクラスタ構成がサポート**されません**。

制御ライセンスは（保護ライセンスとともに）、管理対象デバイスの購入時に自動的に付属します。このライセンスは無期限ですが、システムの更新を有効にするには、TA サブスクリプションを購入する必要があります。

Control ライセンスがない状態でアクセス制御ルールにユーザ条件とアプリケーション条件を追加できますが、ポリシーを適用するには、最初に Control ライセンスを Defense Center に追加し、ポリシー適用対象デバイスで有効にする必要があります。

DC500 Defense Center ではアクセス コントロール ルールへのユーザ条件の追加がサポートされていないことに注意してください。

Control ライセンスがないと、管理対象デバイス上のスイッチド、ルーテッド、またはハイブリッド インターフェイスの作成、NAT エントリの作成、または仮想ルータの DHCP リレーの設定を行うことはできません。仮想スイッチおよびルータを作成できますが、データを取り込むスイッチド インターフェイスおよびルーテッド インターフェイスがない状態ではこれらのスイッチとルータは有用ではありません。さらに、Control を有効にしていない管理対象デバイスにスイッチングまたはルーティングを組み込むデバイス設定を適用することはできません。また、管理対象デバイス間でクラスタ構成を確立するには、デバイスが Control に対して有効になっている必要があります。

Control ライセンスを Defense Center から削除するか、または個別のデバイスで Control を無効にしても、対象デバイスでのスイッチングとルーティングの実行しなくなったり、デバイス クラスタが破損したりは**しません**。既存の設定を編集または削除できますが、対象デバイスに変更を適用することはできません。新しいスイッチド インターフェイス、ルーテッド インターフェイス、またはハイブリッド インターフェイスを追加することも、新しい NAT 項目の追加、DHCP リレーの設定、デバイスのクラスタ構成の確立もできません。既存のアクセス コントロール ポリシーに、ユーザ条件またはアプリケーション条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

URL フィルタリング（URL Filtering）

ライセンス：URL フィルタリング（URL Filtering）

サポートされるデバイス：シリーズ 3、仮想、X-シリーズ、ASA FirePOWER

サポートされる防御センター：任意（DC500 を除く）

URL フィルタリングにより、モニタ対象ホストにより要求される URL に基づいて、ネットワークを移動可能なトラフィックを判別するアクセス コントロール ルールを作成し、Defense Center が シスコ クラウドから取得する URL に関する情報に関連付けることができます。URL フィルタリング（URL Filtering）を有効にするには、Protection ライセンスも有効にする必要があります。

ヒント　URL フィルタリング（URL Filtering）ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリング ライセンスは、脅威 & アプリ（TAC）または脅威 & アプリおよびマルウェア（TAMC）と組み合わせてサービス サブスクリプションとして購入できます。また、脅威 & アプリ（TA）がすでに有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

URL フィルタリング（URL Filtering）ライセンスがない状態でも、アクセス コントロール ルールにカテゴリ ベースの URL 条件およびレピュテーション ベースの URL 条件を追加できますが、Defense Center は URL 情報を取得するためにクラウドに接続しません。最初に URL フィルタリング（URL Filtering）ライセンスを Defense Center に追加し、ポリシー適用対象デバイスで有効にするまでは、アクセス コントロール ポリシーを適用できません。

Defense Center からライセンスを削除するか、または管理対象デバイスで URL フィルタリング（URL Filtering）を無効にすると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング（URL Filtering）ライセンスが期限切れになることがあります。ライセンスが期限切れになるか、ライセンスを削除または無効にすると、URL 条件が含まれているアクセス制御ルールは URL フィルタリングをただちに停止し、Defense Center はクラウドにアクセスできなくなります。既存のアクセス コントロール ポリシーに、カテゴリ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

Malware

ライセンス: Malware

サポートされるデバイス: シリーズ 3、仮想、ASA FirePOWER

サポートされる防御センター: 任意（DC500 を除く）

Malware ライセンスでは、高度なマルウェア防御を実行できます。つまり、管理対象デバイスを使用して、ネットワーク上で送信されるファイルからマルウェアを検出してブロックできます。管理対象デバイス上で Malware を有効にするには、Protection も有効にする必要があります。

（注） Malware ライセンスが有効になっている管理対象デバイスは、動的分析を設定していない場合でも、定期的に シスコ クラウドへの接続を試行します。このため、デバイスの [インターフェイス トラフィック（Interface Traffic）] ダッシュボード ウィジェットには、送信済みトラフィックが表示されます。これは正常な動作です。

ファイル ポリシーの一部としてマルウェア検出を設定し、その後 1 つ以上のアクセス コントロール ルールを関連付けます。ファイル ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。Malware ライセンスでは、限られたファイル タイプのセットを調べてマルウェアが存在するかどうかを確認し、特定のファイル タイプをダウンロードし、シスコ クラウドに送信し、動的分析および Spero 分析を実行してこれらのファイルにマルウェアが含まれているかを判断することができます。Malware ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

マルウェア ライセンスは、脅威 & アプリ（TAM）または脅威 & アプリおよび URL フィルタリング（TAMC）と組み合わせてサブスクリプションとして購入できます。また、脅威 & アプリ（TA）がすでに有効になっているシステムの場合は、アドオン サブスクリプションとして購入できます。

Malware ライセンスがなくてもアクセス コントロール ルールにマルウェア検出ファイル ポリシーを追加できますが、アクセス コントロール ルール エディタでこのファイル ポリシーに警告アイコン（⚠）が付きます。ファイル ポリシー内でも、マルウェア クラウド ルックアップ ルールに警告アイコンが付きます。マルウェア検出ファイル ポリシーを含むアクセス コントロール ポリシーを適用する前に、Malware ライセンスを追加してから、そのポリシー適用対象デバイスで有効にする**必要があります**。後でデバイス上でライセンスを無効にすると、マルウェア検出を実行するファイル ポリシーが含まれている既存のアクセス コントロール ポリシーをこれらのデバイスに対して再適用することはできません。

Malware ライセンスをすべて削除するか、それらがすべて期限切れになると、Defense Center はマルウェア クラウド検索の実行と、シスコ クラウドから送信されるレトロスペクティブ イベントの認識を停止します。既存のアクセス コントロール ポリシーにマルウェア検出を実行するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再適用することはできません。Malware ライセンスの期限切れまたは削除後のごく短い時間内は、マルウェア クラウド ルックアップ ファイル ルールで検出されたファイルのキャッシュされた性質を、システムが使用できることに注意してください。この時間枠の経過後は、システムは検索を実行せず `Unavailable` という性質をこれらのファイルに割り当てます。

Malware ライセンスが必要であるのは、システムでネットワーク トラフィックのマルウェアを検出する必要がある場合だけであることに注意してください。Malware ライセンスがない状態でも、組織に FireAMP サブスクリプションがある場合は、Defense Center はシスコ クラウドからエンドポイント ベースのマルウェア イベントを受信できます。詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

VPN

ライセンス: VPN

サポートされるデバイス: シリーズ 3

VPN を使用すると、インターネットやその他のネットワークなどの公共ソースを経由してエンドポイント間にセキュア トンネルを確立できます。シスコ管理対象デバイスの仮想ルータ間にセキュア VPN トンネルを確立するように FireSIGHT システムを設定できます。VPN を有効にするには、Protection および Control ライセンスも有効にする必要があります。VPN ライセンスを購入するには、販売担当者までお問い合わせください。

VPN ライセンスがないと、管理対象デバイスで VPN 導入環境を設定できません。導入環境の作成はできますが、データを取り込むための 1 つ以上の VPN 対応スイッチド インターフェイスおよびルーテッド インターフェイスがない状態では、導入環境は有用ではありません。

VPN ライセンスを Defense Center から削除するか、または個別のデバイスで VPN を無効にすると、対象デバイスは現在の VPN 導入環境をブレイク**しません**。既存の導入環境を編集または削除できますが、対象デバイスに変更を適用することはできません。

サービス サブスクリプション

ライセンス: 任意（Any）

サービス サブスクリプションは、所定の時間内限定で、管理対象デバイス上の特定の機能を有効にします。サービス サブスクリプションは、1 年、3 年、または 5 年単位で購入できます。サブスクリプションの期限が切れると、サブスクリプションを更新する必要があることが通知されます。サブスクリプションの期限が切れた場合、機能のタイプによっては、関連機能を使用できなくなることがあります。

管理対象デバイスを購入すると、制御および保護のライセンスが自動的に付属します。これらのライセンスは無期限ですが、システムの更新を有効にするには、TA サービス サブスクリプションを購入する必要があります。その他のサービス サブスクリプションはオプションです。

サービス サブスクリプションは、FireSIGHT システムで管理対象デバイスに割り当てるライセンスと、次のように対応しています。

表 65-2　FireSIGHT サービス サブスクリプション

購入するサブスクリプション	FireSIGHT システムで割り当てるライセンス
TA	制御 + 保護（別名「脅威 & アプリ」、システム更新に必要）
TAC	制御 + 保護 + URL フィルタリング
TAM	制御 + 保護 + マルウェア
TAMC	制御 + 保護 + URL フィルタリング + マルウェア
AMP	マルウェア（TA がすでに存在する場合はアドオン）
URL	URL フィルタリング（TA がすでに存在する場合はアドオン）

ハイ アベイラビリティ ペアのライセンス

ライセンス:任意（Any）

サポートされる防御センター:DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

高可用性ペアの Defense Center は、ライセンスを共有**しません**。ペアの各メンバーに同等のライセンスを適用する必要があります。シスコは各 Defense Center の固有ライセンス キーに基づいてライセンスが生成するため、異なる Defense Center で同じキーを使用することはできません。

スタック構成デバイスおよびクラスタ構成デバイスのライセンス

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

個々のデバイスをスタック構成またはクラスタ構成する前に、これらの各デバイスに同等のライセンスがインストールされている必要があります。デバイスのスタック構成後に、スタック全体のライセンスを変更できます。ただし、デバイス クラスタでは有効なライセンスを変更することはできません。

スタック構成のデバイスの管理（4-47 ページ）で説明する要件に準拠する同一モデルの 3D8140、3D8200 ファミリ、3D8300 ファミリ、および 3D9900 デバイスをスタック構成にできます。デバイスのクラスタリング（4-31 ページ）で説明する要件に準拠する同一 シリーズ 3 モデルの 2 つのデバイスをクラスタ構成にできます。

シリーズ 2 アプライアンスのライセンス付与

ライセンス: Protection

サポートされるデバイス:シリーズ 2

DC500 を除き、シリーズ 2、およびシリーズ 3 Defense Center のライセンス付与方法は同一です。DC500 は URL フィルタリングおよびネットワークベースのマルウェア検出をサポートしていないため、URL フィルタリング（URL Filtering）や Malware のライセンスのメリットを活用できません。

シリーズ 2 デバイスには、Protection ライセンスにより有効になるセキュリティ インテリジェンス以外の機能を自動的に組み込まれています。シリーズ 2 デバイスでは Protection ライセンスを無効にできません。また、その他のライセンスを有効にできません。

詳細については、次の各項を参照してください。

- サービス サブスクリプション（65-8 ページ）では、FireSIGHT システム導入環境で使用可能なライセンスのタイプについて説明します。
- 管理対象デバイスの各モデルでサポートされる機能の概要（1-6 ページ）では、シリーズ 2 アプライアンスでサポートされている機能とサポートされていない機能の要約を示します。

FireSIGHT ホストおよびユーザ ライセンスの制限について

ライセンス: FireSIGHT

Defense Center での FireSIGHT ライセンスは、Defense Center とその管理対象デバイスで監視可能なホストおよびユーザの数、ユーザ制御を実行ために使用可能なユーザの数を決定します。次の表に示すように、FireSIGHT のホスト ライセンスとユーザ ライセンスの制限はモデル固有です。

表 65-3　Defense Center モデル別の FireSIGHT の制限

Defense Center モデル	FireSIGHT のホストとユーザの制限
DC500	1000
DC750	2000
DC1000	20,000
DC1500	50,000
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000
仮想	50,000

たとえば、DC500 では 1000 ホストおよび 1000 ユーザを監視できます。

以前に Defense Center で FireSIGHT システム バージョン 4.10.x が稼働しており、ISO ファイルを使用してアプライアンスをバージョン 5.x の出荷時デフォルトに「復元」した場合、FireSIGHT ライセンスの代わりにレガシー RNA Host および RUA User ライセンスを使用できる場合があります。

詳細については、次の項を参照してください。

- FireSIGHT ホスト制限について（65-10 ページ）
- FireSIGHT ユーザ制限について（65-11 ページ）
- アクセス制御ユーザ制限について（65-12 ページ）
- Protection（65-4 ページ）

FireSIGHT ホスト制限について

ライセンス: FireSIGHT

Defense Center の FireSIGHT ライセンスにより、Defense Center およびその管理対象デバイスで監視できる個々のホストの数、およびネットワーク マップに保管できるホストの数が決定します。

システムでは、IP アドレスと MAC アドレスの両方によって識別されるホストとは別に、MAC 専用ホストがカウントされるので注意してください。1 つのホストに関連付けられているすべての IP アドレスは、まとめて 1 つのホストとしてカウントされます。

システムが（ネットワーク検出ポリシーで定義されている）監視対象ネットワークの IP アドレスを持つホストに関連するアクティビティを検出すると、そのホストがネットワーク マップに追加されます。

ホスト制限に達した後でシステムにより新しいホストが検出される場合、新しいホストがネットワーク マップに追加されるかどうかは、ネットワーク検出ポリシーの [ホストの制限に到達した場合（When Host Limit Reached）] 設定に基づきます。データベースへの新しいホストの追加を停止するか、または最も長い期間にわたり非アクティブなホストを置き換えるようにシステムを設定できます。

(注)　ネットワーク マップに新しいホストを追加できない場合でも、システムはそのホストのネットワーク トラフィックに対してアクセス 制御を実行します。ライセンス制限に達した後でも、FireSIGHT ホストの制限に達したために検出されたホストに対してアクセス制御を実行できなくなることはありませんが、ホスト プロファイル データを使用してこれらのホストの分析を実行または表示することはできません。たとえば、コンプライアンス ホワイトリストを使用してこれらのホストのネットワーク コンプライアンスをモニタしたり、ホスト プロファイル認定にこれらのホストを使用したりすることはできません。

ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除することもできます。ただしシステムは、削除されたホストに関連するアクティビティを検出すると、そのホストをネットワーク マップに再度追加することに注意してください。

ネットワーク検出ポリシーで指定された最後の [ホスト タイムアウト（Host Timeout）] 期間内に、ホストからのネットワーク トラフィックが検出されない場合、ホストはネットワーク マップから削除されることにも注意してください。デフォルト設定は 10080 分（7 日）です。

ホスト ライセンスの使用状況を追跡できるようにするため、残りの設定可能なホスト ライセンスの数よりも少ない場合には、FireSIGHT Host License Limit ヘルス モジュールにより警告が出されます。

FireSIGHT ユーザ制限について

ライセンス：FireSIGHT

Defense Center の FireSIGHT ライセンスにより、監視できる個々のユーザの数が決定します。システムが新しいユーザのアクティビティを検出すると、そのユーザは Users データベースに追加されます。ユーザは次の方法で検出できます。

- ネットワーク検出ポリシーを使用して、LDAP、AIM、POP3、IMAP、Oracle、SIP (VoIP)、FTP、HTTP、MDNS、および SMTP ユーザのログインを受動的に検出するように管理対象デバイスを設定することができます。
- Active Directory 資格情報に対する認証を検出するため、Microsoft Active Directory LDAP サーバに User Agent をインストールできます。

ライセンス制限に達すると、ほとんどの場合、システムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、データベースからユーザを手動で削除するか、またはデータベースからすべてのユーザを消去する必要があります。

ただし、システムは権限のあるユーザ ログインを特別扱いします。ライセンス制限に達した後、システムが以前は検出されなかった信頼できるユーザのログインを検出した場合、システムは、最も長い期間にわたって非アクティブな信頼できないユーザを削除し、このユーザを新しい信頼できるユーザに置き換えます。

ヒント　管理対象デバイスを使用してユーザ アクティビティを検出する場合、ユーザ名が複雑になることを最小限に抑え、FireSIGHT ユーザ ライセンスを保持するため、ユーザ ロギングをプロトコルにより制限できることに注意してください。たとえば、AIM、POP3、および IMAP で検出されるユーザを監視すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスが原因で、組織に関係のないユーザが追加されることがあります。詳細については、ユーザ ロギングの制限（45-33 ページ）を参照してください。

アクセス制御ユーザ制限について

ライセンス：Control

サポートされるデバイス：シリーズ 3、仮想、ASA FirePOWER

Defense Center の FireSIGHT ライセンスにより、監視できる個々のユーザの数ばかりでなく、ユーザ制御を実行するためにアクセス制御ルールで使用できるユーザの数も決まります。これらのユーザは *アクセス制御ユーザ* と呼ばれます。

（注）　ユーザ制御を実行するには、組織で Microsoft Active Directory が使用されている**必要があります**。システムは Active Directory サーバで稼働している User Agent を使用してアクセス制御ユーザに IP アドレスを関連付けます。これにより、アクセス制御ルールがトリガー可能になります。

Defense Center と Active Directory サーバ間に接続（*ユーザ認証オブジェクト*）を設定して、アクセス制御ユーザが属すべきグループを指定します。次に、Defense Center は定期的にサーバに対してクエリを実行し、認証オブジェクトで指定したグループのユーザのリストを取得します。これらのユーザを使用してアクセス制御を実行できます。

認証オブジェクトに指定したグループのユーザの総数が、FireSIGHT ユーザ ライセンスよりも少ないことを確認する**必要があります**。パラメータが一般的でありすぎると、Defense Center は可能な限り多くのユーザを取得し、タスク キューで取得できなかったユーザの数を報告します。パフォーマンスとライセンスの理由から、シスコはアクセス制御に使用するユーザを表すグループだけを指定することを推奨します。

ライセンスの表示

ライセンス：任意（Any）

[ライセンス（Licenses）] ページで、Defense Center とその管理対象デバイスのライセンスを表示します。導入環境内のアプライアンスのタイプごとに、所有しているライセンスの総数と、使用中のライセンスの割合がこのページにリストされます。

このページでは、使用中の FireSIGHT User ライセンスの数は、FireSIGHT システムにより検出されるユーザの数、つまり Users データベース内のユーザの数を表すことに注意してください。これは、アクセス制御に使用するアクセス制御ユーザの数ではありません。詳細については、FireSIGHT ホストおよびユーザ ライセンスの制限について（65-10 ページ）を参照してください。

[ライセンス（Licenses）] ページには、各ライセンスの詳細も表示されます。モデルごとに、各タイプの所有ライセンス数、各タイプのライセンスでライセンス付与できる管理対象デバイスの数が表示されます。有効期限のあるライセンスの場合、このページに有効期限が表示されます。

[ラインセス（Licenses）] ページ以外にも、ライセンスとライセンス制限を確認できる方法がいくつかあります。

- [製品ライセンス（Product Licensing）] ダッシュボード ウィジェットはライセンスの概要を示します。
- [デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）]）は、各管理対象デバイスに適用されているライセンスをリストします。
- 2 つの ヘルス モジュール（License Monitor および FireSIGHT Host License Limit）をヘルス ポリシーで使用すると、ライセンス ステータスが通知されます。

ライセンスを確認するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ライセンス（Licenses）] を選択します。

[ライセンス（Licenses）] ページが表示されます。

Defense Center へのライセンスの追加

ライセンス：任意（Any）

Defense Center にライセンスを追加する前に、ライセンスの購入時にシスコから提供されたアクティベーション キーがあることを確認してください。

FireSIGHT を除き、ライセンス付き機能を使用する前に、管理対象デバイスでライセンスを有効にする**必要があります**。デバイスを Defense Center に追加するとき、またはデバイスの追加後にデバイスの一般プロパティを編集することで、ライセンスを有効にできます。シリーズ 2 デバイスには Protection の機能（Security Intelligence フィルタリングを除く）が自動的に組み込まれるため、これらの機能を無効にできず、また他のライセンスを シリーズ 2 デバイスに適用できないことに注意してください。デバイスのライセンス付き機能の変更（65-15 ページ）を参照してください。

（注）　バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ライセンスを追加するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ライセンス（Licenses）] を選択します。

[ライセンス（Licenses）] ページが表示されます。

手順 2　[新規ライセンスの追加（Add New License）] をクリックします。

[ライセンスの追加（Add License）] ページが表示されます。

手順 3　ライセンスを電子メールで受信しましたか?

- 電子メールで受信した場合は電子メールからライセンスをコピーし、[ライセンス(License)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。

  ライセンスが正しい場合、ライセンスが追加されます。残りの手順は省略します。
- 電子メールで受信していない場合は、[ライセンスの取得(Get License)] をクリックします。

  Licensing Center Web サイトが表示されます。インターネットにアクセスできない場合は、インターネットにアクセスできるコンピュータに切り替えてください。ページ下部に表示されるライセンス キーを書きとめ、https://tools.cisco.com/SWIFT/LicensingUI/Home を参照します。

手順 4　画面の指示に従ってライセンスを取得します。ライセンスは電子メールで送信されます。

ヒント　サポート サイトにログインした後で、[ライセンス(Licenses)] タブでライセンスを要求することもできます。

手順 5　電子メールからライセンスをコピーし、Defense Center の Web インターフェイスの [ライセンス(License)] フィールドに貼り付け、[ライセンスの送信(Submit License)] をクリックします。

ライセンスが有効な場合、ライセンスが追加されます。これで、デバイスのライセンス付き機能の変更(65-15 ページ)の説明に従って管理対象デバイスでライセンスの機能を有効にできます。

ライセンスの削除

ライセンス:任意(Any)

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。シスコは各 Defense Center の固有ライセンス キーに基づいてライセンスを生成するため、ある Defense Center からライセンスを削除し、削除したライセンスを別の Defense Center で再利用する場合は、新しい Defense Center のライセンス キーに基づいた新しいライセンスをリクエストする必要があります。

ほとんどの場合、ライセンスを削除すると、そのライセンスによって有効になる機能を使用することができなくなります。詳細については、サービス サブスクリプション(65-8 ページ)を参照してください。

ライセンスを削除するには:

アクセス:管理

手順 1　[システム(System)] > [ライセンス(Licenses)] を選択します。

[ライセンス(Licenses)] ページが表示されます。

手順 2　削除するライセンスの横にある削除アイコン( )をクリックします。

ライセンスを削除すると、そのライセンスを使用するすべてのデバイスから、ライセンスされている機能が削除されます。たとえば、Protection ライセンスが 100 台の管理対象デバイスで有効である場合、このライセンスを削除すると、100 台のデバイスすべてから Protection の機能が削除されます。

手順 3　ライセンスを削除することを確認します。

ライセンスが削除されます。

デバイスのライセンス付き機能の変更

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3、仮想、X-シリーズ、ASA FirePOWER

シリーズ 3 デバイス、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER のライセンス付き機能を変更するには、[デバイス管理（Device Management）] ページでデバイスの全般プロパティを編集します。一部の例外はありますが、管理対象デバイスでライセンスを無効にすると、そのライセンスに関連付けられている機能は使用できなくなります。

シリーズ 2 デバイスには、セキュリティ インテリジェンス フィルタリングを除く、Protection 機能が自動的に組み込まれています。これらの機能を無効にすることも、他のライセンスをシリーズ 2 デバイスに適用することもできません。DC500 Defense Centerでは Malware または URL フィルタリング（URL Filtering）ライセンスを使用できませんが、DC500 を使用して、シリーズ 3 デバイス、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER デバイスのこれらのライセンス付き機能およびその他のライセンス付き機能を有効にしたり変更したりすることはできます。

有効にできるライセンスの詳細（バージョン、モデル、およびその他の要件を含む）については、サービス サブスクリプション（65-8 ページ）を参照してください。

デバイスのライセンス付き機能を有効または無効にするには、次の手順を実行します。

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　ライセンスを有効または無効にするデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Device）] タブが表示されます。

手順 4　[ライセンス（License）] セクションの横にある編集アイコン（）をクリックします。

[ライセンス（License）] ポップアップ ウィンドウが表示されます。

手順 5　該当するチェック ボックスをオンまたはオフにして、デバイスのライセンス機能を有効または無効にします。

手順 6　[保存（Save）] をクリックします。

変更は保存されますが、デバイス設定を適用するまでは反映されません。デバイスへの変更の適用（4-27 ページ）を参照してください。