CHAPTER 64

アプライアンス設定の構成

FireSIGHT システム アプライアンスの *ローカル構成*（[システム（System）] > [ローカル（Local）] > [構成（Configuration）]）は、単一のアプライアンスに特有なものと想定される設定グループです。ローカル構成は、導入全体でほぼ同じになると想定されるアプライアンス設定を制御するシステム ポリシー（システム ポリシーの管理（63-1 ページ））とは対照的です。

次の表は、アプライアンスのローカル構成をまとめたものです。

表 64-1　　ローカル設定のオプション

オプション	説明	詳細
情報	アプライアンスに関する現在の情報が表示されます。アプライアンスの名前を変更することもできます。	アプライアンス情報の表示と変更（64-2 ページ）
HTTPS 証明書（HTTPS Certificate）	信頼できる機関の HTTPS サーバ証明書を要求し（必要な場合）、証明書をアプライアンスにアップロードできます。	カスタム HTTPS 証明書の使用（64-3 ページ）
データベース	外部からアプライアンス データベースへの読み取り専用アクセスを有効化し、ダウンロードするクライアント ドライバを提供します。	データベースへのアクセスの有効化（64-8 ページ）
管理インターフェイス	インストールの一部として最初に設定されたアプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更できます。アプライアンスの管理インターフェイスの設定を表示および変更することもできます。	管理インターフェイスの構成（64-9 ページ）
Process	アプライアンスのシャットダウンやリブート、および FireSIGHT システムに関連するプロセスの再起動を実行できます。	システムのシャット ダウンと再起動（64-14 ページ）
時刻（Time）	現在の時間が表示されます。アプライアンスの現在のシステム ポリシー内の時間同期設定が [手動のローカル設定（Manually in Local Configuration）] に設定されている場合は、このページを使用して時間を変更できます。	手動による時刻の設定（64-16 ページ）
Remote Storage Device	防御センターで、バックアップとレポート用のリモート ストレージを設定できます。	リモート ストレージの管理（64-17 ページ）
Change Reconciliation	過去 24 時間に発生したシステム変更の詳細レポートを電子メールで受信できます。	変更調整について（64-22 ページ）
Console Configuration	VGA またはシリアル ポート、または物理的にアプライアンスの近くにいなくても限られたモニタリングおよび管理タスクを実行できる Lights-Out 管理（LOM）を使用して FireSIGHT システム アプライアンスへのコンソール アクセスを設定できます。	リモート コンソール アクセスの管理（64-23 ページ）

表 64-1　ローカル設定のオプション(続き)

オプション	説明	詳細
クラウド サービス（Cloud Services）	防御センターで Collective Security Intelligence クラウドから URL フィルタリング データをダウンロードしたり、未分類の URL でルックアップを実行したり、検出されたファイルの診断情報をシスコに送信したりできます。	クラウド通信の有効化（64-30 ページ）
VMware Tools	仮想防御センターで、VMwareTools を有効にして使用できます。	VMware ツールの有効化（64-34 ページ）

アプライアンス情報の表示と変更

ライセンス: 任意（Any）

[情報（Information）] ページには、アプライアンスに関する情報が表示されます。これには、製品名とモデル番号、オペレーティング システムとバージョン、現在のアプライアンス レベルのポリシーなどの読み取り専用情報が含まれます。このページには、アプライアンスの名前を変更するオプションも用意されています。

次の表で、各フィールドについて説明します。

表 64-2　アプライアンス情報

フィールド	説明
[名前（Name）]	アプライアンスに割り当てられた名前。この名前は FireSIGHT システムのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名は変更されません。
製品モデル（Product Model）	アプライアンスのモデル名。
ソフトウェア バージョン（Software Version）	現在インストールされているソフトウェアのバージョン。
シリアル番号（Serial Number）	アプライアンスのシャーシのシリアル番号。
イベントを 防御センターにのみ格納（Store Events Only on Defense Center）	管理対象デバイスでこのチェックボックスを選択すると、イベント データは防御センターには格納されますが、その管理対象デバイスに格納されなくなります。このチェックボックスをオフにすると、両方のアプライアンスにイベント データが格納されます。
防御センター へのパケット転送を禁止 (Prohibit Packet Transfer to the Defense Center)	管理対象デバイスでこのチェックボックスを選択すると、その管理対象デバイスはイベントのパケット データを送信しなくなります。このチェックボックスをオフにすると、イベントでパケット データが防御センターに格納されます。
オペレーティング システム（Operating System）	アプライアンス上で現在実行されているオペレーティング システム。

表 64-2　アプライアンス情報（続き）

フィールド	説明
オペレーティング システム バージョン（Operating System Version）	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス（IPv4 Address）	アプライアンスのデフォルトの管理インターフェイス（eth0）の IPv4 アドレス。アプライアンスで IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス（IPv6 Address）	アプライアンスのデフォルトの管理インターフェイス（eth0）の IPv6 アドレス。アプライアンスで IPv6 の管理が無効になっている場合は、このフィールドにそのことが示されます。
現在のポリシー（Current Policies）	現在適用されているアプライアンスレベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシーの名前がイタリック体で表示されます。
モデル番号（Model Number）	アプライアンスのモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

アプライアンスの情報を変更するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　アプライアンス名を変更するには、[名前（Name）] フィールドに新しい名前を入力します。

名前は、英数字である**必要があり**、数字だけで構成することはできません。

手順 3　変更を保存するには、[保存（Save）] をクリックします。

ページが更新され、変更が保存されます。

カスタム HTTPS 証明書の使用

ライセンス：任意（Any）

シスコ 防御センター、および Web ベースのユーザ インターフェイスをサポートしている管理対象デバイスには、デフォルトの SSL（Secure Socket Layer）証明書が含まれています。この証明書を使用して、Web ブラウザとアプライアンス間に暗号化した通信チャネルを確立できます。ただし、アプライアンスのデフォルト証明書は世界的に知られている認証局（CA）に信頼されている CA によって生成されていないため、世界的に知られている CA または内部的に信頼できる CA によって署名されたカスタム証明書に置き換えることができます。

証明書は、アプライアンスのローカル構成で管理できます。詳細については、次のトピックを参照してください。

- 現在の HTTPS サーバ証明書の表示（64-4 ページ）
- サーバ証明書要求の生成（64-5 ページ）
- サーバ証明書のアップロード（64-6 ページ）
- ユーザ証明書の要求（64-6 ページ）

現在の HTTPS サーバ証明書の表示

ライセンス：任意（Any）

アプライアンスに現在適用されているサーバ証明書の詳細を表示できます。証明書には次の情報が含まれています。

表 64-3　HTTPS サーバ証明書の情報

フィールド	説明
Subject	証明書がインストールされているアプライアンスの commonName、countryName、organizationName、および organizationalUnitName を示します。
発行元（Issuer）	証明書を発行したアプライアンスの commonName、countryName、organizationName、および organizationalUnitName を示します。
Validity	証明書の有効期間を示します。
バージョン（Version）	証明書のバージョンを示します。
シリアル番号（Serial Number）	証明書のシリアル番号を示します。
署名アルゴリズム（Signature Algorithm）	証明書の署名に使用されるアルゴリズムを示します。

証明書の詳細を表示するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[HTTPS 証明書（HTTPS Certificate）] をクリックします。

[HTTPS 証明書（HTTPS Certificate）] ページが表示され、アプライアンスの現在の証明書の詳細が示されます。

サーバ証明書要求の生成

ライセンス: 任意（Any）

アプライアンスの情報と指定した ID 情報に基づいて、証明書要求を生成できます。生成された要求を認証局に送信して、サーバ証明書を要求できます。内部認証局（CA）がインストールされ、ブラウザによって信頼されている場合は、生成された要求を使用して証明書に自己署名することもできます。生成されるキーは、Base 64 符号化（PEM）形式です。

ローカル設定の [HTTPS 証明書（HTTPS Certificate）] ページで証明書要求を生成する場合は、1 つのサーバに対して 1 つの証明書しか生成できないので注意してください。証明書に表示されるとおりに正確に、サーバの完全修飾ドメイン名を [共通名（Common Name）] フィールドに入力する必要があります。一般名と DNS ホスト名が一致しない場合は、アプライアンスに接続するときに警告が表示されます。同様に、世界的に知られている CA または内部的に信頼できる CA によって署名されていない証明書をインストールした場合は、アプライアンスに接続するときにセキュリティ警告が表示されます。

証明書要求を生成するには、次の手順を実行します。

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[HTTPS 証明書（HTTPS Certificate）] をクリックします。

[HTTPS 証明書（HTTPS Certificate）] ページが表示されます。

手順 3　[新しい CSR の生成（Generate New CSR）] をクリックします。

[証明書署名要求の作成（Generate Certificate Signing Request）] ポップアップ ウィンドウが表示されます。

手順 4　[国名（2 桁コード）（Country Name (two-letter code)）] フィールドに、国を表す 2 文字の国コードを入力します。

手順 5　[都道府県（State or Province）] フィールドに、都道府県の名前を入力します。

手順 6　[市区町村（Locality or City）] フィールドに、市区町村の名前を入力します。

手順 7　[組織（Organization）] フィールドに、組織の名前を入力します。

手順 8　[組織部門（Organizational Unit）] フィールドに、組織単位（部門）の名前を入力します。

手順 9　[共通名（Common Name）] フィールドに、証明書の要求先となるサーバの完全修飾ドメイン名を、証明書に表示されるとおりに正確に入力します。

手順 10　[生成（Generate）] をクリックします。

[証明書署名要求（Certificate Signing Request）] ポップアップ ウィンドウが表示されます。

手順 11　テキスト エディタを開きます。

手順 12　証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして、空のテキスト ファイルに貼り付けます。

手順 13　このファイルを *servername*`.csr` として保存します。*servername* は証明書を使用するサーバの名前です。

手順 14　この CSR ファイルを証明書の要求先となる認証局にアップロードするか、またはこの CSR を使用して自己署名証明書を作成します。

サーバ証明書のアップロード

ライセンス:任意（Any）

認証局（CA）から署名付き証明書を取得した後は、その証明書をアップロードできます。証明書を生成した署名認証局から中間 CA を信頼するように要求された場合は、証明書チェーン（証明書パスとも呼ばれる）も提供する必要があります。ユーザ証明書が必要な場合は、証明書チェーンに中間認証局が含まれる認証局によってユーザ証明書が生成されている必要があります。

証明書をアップロードするには、次の手順を実行します。

アクセス:管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[HTTPS 証明書（HTTPS Certificate）] をクリックします。

[HTTPS 証明書（HTTPS Certificate）] ページが表示されます。

手順 3　[HTTPS 証明書のインポート（Import HTTPS Certificate）] をクリックします。

[HTTPS 証明書のインポート（Import HTTPS Certificate）] ポップアップ ウィンドウが表示されます。

手順 4　テキスト エディタでサーバ証明書を開き、テキスト ブロック全体（`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含む）をコピーして、[サーバ証明書（Server Certificate）] フィールドに貼り付けます。

手順 5　必要に応じて、秘密キー ファイルを開き、テキスト ブロック全体（`BEGIN RSA PRIVATE KEY` 行と `END RSA PRIVATE KEY` 行を含む）をコピーして、[秘密キー（Private Key）] フィールドに貼り付けます。

手順 6　提供する必要がある中間証明書を開き、各証明書のテキスト ブロック全体をコピーして、[証明書チェーン（Certificate Chain）] フィールドに貼り付けます。

手順 7　[保存（Save）] をクリックして証明書をアップロードします。

証明書がアップロードされ、新しい証明書を反映するために [HTTPS 証明書（HTTPS Certificate）] ページが更新されます。

ユーザ証明書の要求

ライセンス:任意（Any）

クライアント ブラウザの証明書チェック機能を使用して FireSIGHT システムの Web サーバへのアクセスを制限できます。ユーザ証明書を有効にすると、Web サーバはユーザのブラウザ クライアントで有効なユーザ証明書が選択されていることを確認します。そのユーザ証明書は、サーバ証明書で使用されているのと同じ信頼できる認証局によって生成されている必要があります。ブラウザ内でユーザが有効でない証明書、またはデバイス上の証明書チェーンに含まれる認証局によって生成されていない証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。

サーバに証明書失効リスト（CRL）をロードすることもできます。CRL には認証局によって取り消されたすべての証明書の一覧があるため、Web サーバはクライアント ブラウザの証明書が取り消されていないことを確認できます。ユーザが CRL にある失効した証明書の一覧に含まれる証明書を選択した場合、ブラウザは Web インターフェイスをロードできません。アプライアンスは識別符号化規則（DER）形式による CRL のアップロードをサポートしています。1 つのサーバにロードできる CRL は 1 つだけです。

失効した証明書のリストを最新の状態に保つため、CRL を更新するスケジュール タスクを作成できます。直近に更新された CRL がインターフェイスに表示されます。

サーバ証明書で使用されるのと同じ認証局を使用していること、および証明書の中間証明書をアップロードしたことを確認してください。詳細については、サーバ証明書のアップロード（64-6 ページ）を参照してください。

（注）　ユーザ証明書を有効にし、その後で Web インターフェイスにアクセスするには、ブラウザに有効なユーザ証明書が存在する（またはリーダーに CAC が挿入されている）**必要があります**。

有効なユーザ証明書を要求するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[HTTPS 証明書（HTTPS Certificate）] をクリックします。

[HTTPS 証明書（HTTPS Certificate）] ページが表示されます。

手順 3　[ユーザ証明書の有効化（Enable User Certificates）] を選択します。プロンプトが表示されたら、ドロップダウン リストから適切な証明書を選択します。

[CRL の取得の有効化（Enable Fetching of CRL）] オプションが表示されます。

手順 4　必要に応じて、[CRL の取得の有効化（Enable Fetching of CRL）] を選択します。

残りの CRL 構成オプションが表示されます。

手順 5　既存の CRL ファイルの有効な URL を入力し、[CRL の更新（fresh CRL）] をクリックします。

指定した URL にある最新の CRL がサーバにロードされます。

（注）　CRL のフェッチを有効にすると、CRL を定期的に更新するスケジュール タスクが作成されます。このタスクを編集して、更新の頻度を設定します。詳細については、証明書失効リストのダウンロードの自動化（62-4 ページ）を参照してください。

手順 6　サーバ証明書を作成したのと同じ認証局によって生成された有効なユーザ証明書があることを確認します。

注意　ユーザ証明書を有効にして設定を保存すると、ブラウザの証明書ストアに有効なユーザ証明書が存在しない場合に、アプライアンスへのすべての Web サーバ アクセスが無効になります。設定を保存する前に、有効な証明書がインストールされていることを確認してください。

手順 7　ユーザ証明書の構成を Web サーバに適用するため、[保存（Save）] をクリックします。

証明書を有効にしても、ユーザ証明書へのアクセスが有効になっていない場合は、コマンドラインでユーザ証明書の適用を無効にすることができます。詳細については、disable-http-user-cert（D-48 ページ）を参照してください。

データベースへのアクセスの有効化

ライセンス:任意（Any）

サードパーティ製クライアントによるデータベースへの読み取り専用アクセスを許可するよう防御センター を設定できます。これによって、次のいずれかを使用して SQL でデータベースを照会できるようになります。

- 業界標準のレポート作成ツール（Actuate BIRT、JasperSoft iReport、Crystal Reports など）
- JDBC SSL 接続をサポートするその他のレポート作成アプリケーション（カスタム アプリケーションを含む）
- シスコが提供する RunQuery と呼ばれるコマンドライン型 Java アプリケーション（インタラクティブに実行することも、1 つのクエリの結果をカンマ区切り形式で取得することもできる）

ローカル構成の [データベース設定（Database Settings）] ページで、データベース アクセスを有効にして、選択したホストにデータベースの照会を許可するアクセス リストを作成できます。このアクセス リストは、アプライアンスのアクセスは制御しません。アプライアンスのアクセス リストの詳細についてはアプライアンスのアクセス リストの設定（63-9 ページ）を参照してください。

次のツールを含むパッケージをダウンロードすることもできます。

- RunQuery（シスコが提供するデータベース クエリ ツール）
- InstallCert（アクセスしたい防御センターから SSL 証明書を取得して受け入れるために使用できるツール）
- データベースへの接続時に使用する必要がある JDBC ドライバ

外部クライアントからデータベースに接続するときは、防御センターの Administrator または External Database ユーザと一致するユーザ名とパスワードを入力する必要があることに注意してください。詳細については、新しいユーザ アカウントの追加（61-47 ページ）を参照してください。

データベース スキーマとサポートされるクエリに関する情報を含め FireSIGHT システムデータベースへの外部アクセスの設定の詳細については、『*FireSIGHT システム Database Access Guide*』を参照してください。

データベース アクセスを有効にする方法:

アクセス:管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[データベース（Database）] をクリックします。

[データベース設定（Database Settings）] ページが表示されます。

手順 3　[外部のデータベースアクセスを有効にする（Allow External Database Access）] チェックボックスを選択します。

[アクセスリスト（Access List）] フィールドが表示されます。詳細については、ステップ 6 を参照してください。

手順 4　サードパーティ製アプリケーションの要件に応じて、[サーバホスト名（Server Hostname）] フィールドに防御センターの完全修飾ドメイン名（FQDN）、IPv4 アドレス、または IPv6 アドレスを入力します。

FQDN を入力する場合は、クライアントが防御センターの FQDN を解決できることを確認する必要があります。IP アドレスを入力する場合は、クライアントがその IP アドレスを使用して 防御センター に接続できることを確認する必要があります。

手順 5　[クライアント JDBC ドライバ(Client JDBC Driver)] の横にある [ダウンロード(Download)] をクリックし、ブラウザのプロンプトに従って `client.zip` パッケージをダウンロードします。

データベース アクセスを設定するためにダウンロードしたパッケージ内のツールの使用方法については、『*FireSIGHT システム Database Access Guide*』を参照してください。

手順 6　1 つ以上の IP アドレスからのデータベース アクセスを追加するため、[ホストの追加(Add Hosts)] をクリックします。

[アクセスリスト(Access List)] フィールドに [IP アドレス(IP Address)] フィールドが表示されます。

手順 7　[IP アドレス(IP Address)] フィールドでは、追加する IP アドレスに応じて次のオプションがあります。

- 厳密な IP アドレス(192.168.1.101 など)
- CIDR 表記を使用した IP アドレス ブロック(192.168.1.1/24 など)

  FireSIGHT システム での CIDR の使用方法については、IP アドレスの表記規則(1-24 ページ)を参照してください。
- `any`(任意の IP アドレスを指定)

手順 8　[追加(Add)] をクリックします。

IP アドレスがデータベース アクセス リストに追加されます。

手順 9　必要に応じてデータベース アクセス リストのエントリを削除するには、削除アイコン( )をクリックします。

手順 10　[保存(Save)] をクリックします。

データベース アクセス設定が保存されます。

ヒント　最後に保存されたデータベース設定に戻すには、[更新(Refresh)] をクリックします。

管理インターフェイスの構成

ライセンス: 任意(Any)

アプライアンスを最初に設定するときは、内部の保護された管理ネットワーク上で通信できるようにアプライアンスのネットワーク設定を構成します。アプライアンスを最初に設定したときに作成したネットワーク設定を変更して、プロキシなどの追加のネットワーク設定を構成できます。シリーズ 3 アプライアンスおよび仮想防御センターでは、パフォーマンスを向上させるために、トラフィック チャネルを有効にして追加の管理インターフェイスを設定できます。また、異なるネットワーク上の防御センターとデバイス間のトラフィックを管理および分離するためのルートを作成できます。シリーズ 3 デバイスでは、デバイスの LCD パネル アクセスを有効または無効にすることもできます。これらの設定を変更したり、追加のネットワーク設定(プロキシなど)を構成したりするには、[管理インターフェイス(Management Interfaces)] ページ([システム(System)] > [ローカル(Local)] > [構成(Configuration)] を選択して [管理インターフェイス(Management Interfaces)] をクリック)を使用します。

(注)　仮想デバイスのネットワークおよびプロキシ設定を変更する場合と Blue Coat X-Series 向け Cisco NGIPS のネットワーク設定を変更する場合は、コマンドライン ツールを使用する必要があります。Blue Coat X-Series 向け Cisco NGIPS はプロキシをサポート**しない**ことに注意してください。詳細については、『*FireSIGHT システム Virtual Installation Guide*』および『*Blue Coat X-Series 向け Cisco NGIPS Installation and Configuration Guide*』を参照してください。

設定オプションと手順については、次のセクションを参照してください。

- 管理インターフェイスのオプションについて(64-10 ページ)
- 管理インターフェイスの編集(64-13 ページ)

管理インターフェイスのオプションについて

設定を変更することで、パフォーマンスを向上させたり、さまざまな機能を有効にしたり、導入内のネットワーク構成を変更したりできます。シリーズ 3 アプライアンスでは、トラフィック チャネルを設定したり、追加の管理インターフェイスを有効にしたり、異なるネットワーク上のデバイスからのトラフィックを分離するためのルートを作成することができます。詳細については、管理インターフェイスについて(4-4 ページ)を参照してください。

インターフェイス

FireSIGHT システム は、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。一方または両方のプロトコルを選択できます。使用しないプロトコルは(あれば)無効にしてください。

管理プロトコルごとに、デフォルト管理インターフェイス(`eth0`)の IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを指定する必要があります。これらを手動で設定することも、ローカル DHCP サーバまたは IPv6 ルータからこれらを取得するようにアプライアンスを設定することもできます。ただし、有効にする追加の管理インターフェイス(`eth1` など)はそれぞれ手動で設定する必要があります。

管理インターフェイスに対して、次のオプションを設定できます。

- [有効(Enabled)]:管理インターフェイスを有効にします。別の管理インターフェイスを有効にして保存するまでは、デフォルトの管理インターフェイスを無効に**しないでください**。
- [チャネル(Channels)]:インターフェイス上の [管理トラフィック(Management Traffic)] チャネルと [イベントトラフィック(Event Traffic)] チャネルを有効にします。

  トラフィック チャネル(管理トラフィック、イベント トラフィック、またはその両方)を有効にして、各管理インターフェイスの通信チャネル内に異なる接続を作成できます。また、複数の管理インターフェイスにまたがってトラフィック チャネルを分割し、両方のインターフェイスのスループットを統合してパフォーマンスをさらに向上させることもできます。詳細については、管理インターフェイスについて(4-4 ページ)を参照してください。
- [モード(Mode)]:デフォルトの自動ネゴシエーションを変更したり、リンク モードを指定したりできます。ギガビット インターフェイスでは、[自動ネゴシエーション(Auto Negotiate)] の値を変更しても無視されることに注意してください。

  防御センターに 8000 シリーズ の管理対象デバイスを登録するときは、接続の両側で自動ネゴシエーションするか、または両側を同じ固定速度に設定して安定したネットワーク リンクを確保する必要があります。8000 シリーズ の管理対象デバイスは、半二重のネットワーク リンクをサポートしません。また、接続の反対側の速度構成やデュプレックス構成の違いもサポートしません。

- [MTU]:デフォルト設定を変更できます。

(注)　他のインターフェイスとは異なり、管理インターフェイスの最大伝送単位(MTU)を変更しても、トラフィックは中断されません。

次の表に、管理インターフェイスの MTU 設定範囲を示します。

表 64-4　デバイスごとの管理インターフェイスの MTU の範囲

デバイスのモデル	MTU の範囲
シリーズ 23D6500 および 3D9900 を除く	576-1518
3D6500、3D9900、仮想	576-9018
シリーズ 3 デフォルト(eth0)	576-9234
シリーズ 3非デフォルト(eth1 など)	1518-9018

システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。

- [MDI/MDIX]:[Auto-MDIX] のデフォルト設定を変更できます。
- [IPv4 設定(IPv4 Configuration)]:[静的(Static)]、[DHCP]、または [無効(Disabled)] を設定(選択)できます。
  - IPv4 の管理 IP アドレスとネットマスクを入力するには、[静的(Static)] を選択します。
  - DHCP サーバからネットワーク設定を取得するには、[DHCP] を選択します。(eth0 のみ)
  - このプロトコルを無効にするには、[無効(Disabled)] を選択します。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定(IPv6 Configuration)]:[静的(Static)]、[DHCP]、[ルータ割り当て(Router Assigned)]、または [無効(Disabled)] を設定できます。
  - IPv4 の管理 IP アドレスとネットマスクを入力するには、[静的(Static)] を選択します。
  - DHCP サーバからネットワーク設定を取得するには、[DHCP] を選択します。(eth0 のみ)
  - ローカル IPv6 ルータからネットワーク設定を取得するには、[ルータ割り当て(Router Assigned)] を選択します。
  - このプロトコルを無効にするには、[無効(Disabled)] を選択します。IPv4 と IPv6 の両方を無効にしないでください。

ルート

[編集(Edit)] アイコンをクリックすると、デフォルトの管理インターフェイスへのルートを表示または編集できます。[表示(View)] アイコンをクリックすると、ルートの統計情報を表示できます。

追加のネットワークへの新しいルートを作成できます。[追加(Add)] アイコンをクリックすると、ポップアップ ウィンドウが表示され、宛先ネットワークの IP アドレス、ネットマスクまたはプレフィックス長、インターフェイスのドロップダウン(eth0 など)、およびゲートウェイを入力できます。次の例に、別のネットワークへのルートを使用する方法をいくつか示します。

- 防御センターでは、別のネットワーク上のデバイスへのルートを作成することで、異なるネットワーク上のデバイスからのトラフィックを 1 つの防御センターで管理および分離できるようになります。
- デバイスでは、ルートを作成して 2 つの異なるネットワーク上の防御センターにデバイスを登録することで、より広範な展開において防御センターのハイ アベイラビリティを設定できます。

特定の管理インターフェイスで次の設定を行うことで、ネットワークへのルートを作成できます。

- [宛先(Destination)]: ルートを作成する宛先ネットワークのアドレス。
- [ネットマスク(Netmask)] または [プレフィックス長(Prefix Length)]: ネットワークのネットマスク(IPv4)またはプレフィックス長(IPv6)
- [インターフェイス(Interface)]: 新しいルートに割り当てるアプライアンス上の管理インターフェイス。
- [ゲートウェイ(Gateway)]: 新しいネットワークのゲートウェイ。

共有設定

管理環境に関係なく、デバイスのホスト名とドメインと、最大 3 つの DNS サーバを指定できます。

管理ポートを変更できます。FireSIGHT システム アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。シスコでは、デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。

注意　管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

LCD パネル

シリーズ 3 デバイスでは、デバイス前面の LCD パネルを使用してデバイス情報を表示できます。シリーズ 3 の [管理インターフェイス(Management Interfaces)] ページでは、他のユーザが LCD パネルを使用してネットワーク設定を変更できるように設定できます。

LCD パネルを使用して管理対象デバイスの IP アドレスを編集する場合、管理防御センターに変更が反映されることを確認してください。場合によっては、デバイス管理設定を手動で編集する必要があります。詳細については、デバイス管理設定の編集(4-58 ページ)を参照してください。

注意　LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。

プロキシ

FireSIGHT システムのすべてのアプライアンスは、ポート 443/tcp（HTTPS）および 80/tcp（HTTP）を使用してインターネットに直接接続するように設定されています。セキュリティ、インターネット アクセス、および通信ポート（E-1 ページ）を参照してください。Blue Coat X-Series 向け Cisco NGIPS を除き、FireSIGHT システムのアプライアンスは HTTP ダイジェストで認証できるプロキシ サーバの使用をサポートしています。

注意　NT LAN Manager（NTLM）認証を使用するプロキシは Collective Security Intelligence クラウドと通信して情報を受信できません。クラウドベースの機能を使用する場合は、必ずプロキシに別の認証を設定してください。詳細については、クラウド通信の有効化（64-30 ページ）を参照してください。

管理インターフェイスの編集

ライセンス：任意（Any）

[管理インターフェイス（Management Interface）] ページを使用して、防御センターのデフォルトの管理インターフェイスのデフォルト設定を変更できます。シリーズ 3 アプライアンスおよび仮想防御センターでは、トラフィック チャネルや追加の管理インターフェイスを有効にしたり設定することができます。ギガビット インターフェイスでは、[自動ネゴシエーション（Auto Negotiate）] の値を変更しても無視されます。

注意　アプライアンスに物理的にアクセスできない場合は、管理インターフェイスの設定を変更しないでください。Web インターフェイスへのアクセスが困難になる設定を選択する可能性があります。

管理インターフェイスを編集する方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[管理インターフェイス（Management Interfaces）] をクリックします。

[管理インターフェイス（Management Interfaces）] ページが表示され、防御センターの各インターフェイスの現在の設定が一覧表示されます。

手順 3　必要に応じて、[インターフェイス（Interfaces）] で、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

デフォルトの管理インターフェイス（`eth0`）を変更したり、追加の管理インターフェイス（`eth1` など）を有効にして設定したりできます。追加の管理インターフェイスごとに、一意の静的 IP アドレス（IPv4 または IPv6）またはホスト名を割り当てる必要があります。モード、リンク、MTU、および IP 構成の設定に加えて、伝送するトラフィック チャネルを選択できます。

手順 4　必要に応じて、[ルート（Routes）] で、宛先ネットワークの IP アドレス、ネットマスクまたはプレフィックス長、およびゲートウェイを入力し、このネットワーク ルートに使用する管理インターフェイスを指定します。

虫眼鏡アイコンをクリックして、ルートの統計情報を表示することもできます。

手順 5　必要に応じて、[共有設定（Shared Settings）] で、管理ネットワーク プロトコルに依存しないネットワーク設定を指定します。

アプライアンスのホスト名とドメインと、最大 3 つの DNS サーバを指定できます。前の手順で [DHCP] を選択した場合は、これらの共有設定を手動で指定できないことに注意してください。

注意　シスコ デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべて**のアプライアンスの管理ポートを変更する必要があります。

手順 6　必要に応じてシリーズ 3デバイスで [LCD パネル（LCD Panel）] の [ネットワーク設定の再構成を許可（Allow reconfiguration of network settings）] チェックボックスを選択し、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

注意　LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCD パネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

手順 7　必要に応じて、[プロキシ（Proxy）] で、プロキシを有効にするチェックボックスを選択してから、次の手順を実行します。

- [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。[ポート（Port）] フィールドにポートを入力します。
- 必要に応じて、[プロキシ認証を使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

手順 8　アプライアンスのネットワーク設定の構成が完了したら、[保存（Save）] をクリックします。

ネットワーク設定が変更されます。アプライアンスのホスト名を変更した場合は、アプライアンスをリブートした後で新しい名前が syslog に反映されます。

システムのシャット ダウンと再起動

ライセンス: 任意（Any）

アプライアンス上のプロセスを制御するために、いくつかのオプションが用意されています。次の操作を実行できます。

- アプライアンスのシャット ダウン

注意　電源ボタンを使用してアプライアンスを停止**しないでください**。データが失われる可能性があります。アプライアンスを完全にシャット ダウンするには、[アプライアンスのプロセス（Appliance Process）] ページを使用します。

- アプライアンスのリブート
- アプライアンス上の通信、データベース、および HTTP サーバ プロセスの再起動（通常はトラブルシューティング時に使用される）
- Snort プロセスの再起動

注意 Snort プロセスを再起動すると、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

アプライアンスをシャット ダウンまたは再起動する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[プロセス（Process）] をクリックします。

[アプライアンスのプロセス（Appliance Process）] ページが表示されます。

手順 3　実行するコマンドを指定します。

防御センターので、

- アプライアンスをシャット ダウンするには、[防御センターのシャットダウン（Shutdown Defense Center）] の横にある [コマンド実行（Run Command）] をクリックします。
- アプライアンスをリブートするには、[防御センターの再起動（Reboot Defense Center）] の横にある [コマンド実行（Run Command）] をクリックします。これによってユーザが防御センターからログアウトすることに注意してください。
- アプライアンスを再起動するには、[防御センター コンソールの再起動（Restart Defense Center Console）] の横にある [コマンド実行（Run Command）] をクリックします。防御センターを再起動すると、ネットワーク マップ内に削除されたホストが再表示されることがあります。

（注） 防御センターをリブートすると、データベースのチェックが実行されます。このチェックが完了するまでに最大 1 時間かかることがあります。

管理対象デバイスで:

- アプライアンスをシャット ダウンするには、[アプライアンスのシャット ダウン（Shutdown Appliance）] の横にある [コマンド実行（Run Command）] をクリックします。
- アプライアンスをリブートするには、[アプライアンスの再起動（Reboot Appliance）] の横にある [コマンド実行（Run Command）] をクリックします。これによってユーザがそのデバイスからログアウトすることに注意してください。
- アプライアンスを再起動するには、[アプライアンス コンソールの再起動（Restart Appliance Console）] の横にある [コマンド実行（Run Command）] をクリックします。
- Snort プロセスを再起動するには、[Snort の再起動（Restart Snort）] の横にある [コマンド実行（Run Command）] をクリックします。

（注） 管理対象デバイスをリブートすると、データベースのチェックが実行されます。このチェックが完了するまでに最大 1 時間かかることがあります。

手動による時刻の設定

ライセンス:任意（Any）

現在適用されているシステム ポリシー内の時間同期設定が [手動のローカル設定（Manually in Local Configuration）] に設定されている場合は、ローカル構成の [時間（Time）] ページを使用して手動でアプライアンスの時間を設定できます。

Blue Coat X-Series 向け Cisco NGIPS の時間設定を管理するには、コマンドライン インターフェイスやオペレーティング システム インターフェイスなどのネイティブ アプリケーションを使用する必要があります。詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』を参照してください。

アプライアンスが NTP に基づいて時間を同期している場合は、時間を手動で変更できません。代わりに、[時間（Time）] ページの [NTP ステータス（NTP Status）] セクションに次の情報が表示されます。

表 64-5　NTP のステータス

カラム（Column）	説明
NTP サーバ	構成済みの NTP サーバの IP アドレスと名前。
ステータス（Status）	NTP サーバの時間同期のステータス。次の状態が表示されます。 • [使用中（Being Used）] は、アプライアンスが NTP サーバと同期していることを示します。 • [使用可能（Available）] は、NTP サーバが使用可能であるものの、時間がまだ同期していないことを示します。 • [使用不能（Not Available）] は、NTP サーバが構成に含まれているものの、NTP デーモンがその NTP サーバを使用できないことを示します。 • [保留（Pending）] は、NTP サーバが新しいか、または NTP デーモンが最近再起動されたことを示します。この値は、時間の経過とともに [使用中（Being Used）]、[使用可能（Available）]、または [使用不能（Not Available）] に変わるはずです。 • [不明（Unknown）] は、NTP サーバのステータスが不明であることを示します。
オフセット	アプライアンスと構成済みの NTP サーバ間の時間の差（ミリ秒）。負の値はアプライアンスの時間が NTP サーバより遅れていることを示し、正の値は進んでいることを示します。
Last Update	NTP サーバと最後に時間を同期してから経過した時間（秒数）。NTP デーモンは、いくつかの条件に基づいて自動的に同期時間を調整します。たとえば、更新時間が大きい（300 秒など）場合、それは時間が比較的安定しており、NTP デーモンが小さい更新増分値を使用する必要がないと判断したことを示します。

システム ポリシー内の時間設定の詳細については、時間の同期（63-28 ページ）を参照してください。

時間を手動で設定する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[時間（Time）] をクリックします。

[時間（Time）] ページが表示されます。

手順 3　[時間の設定（Set Time）] ドロップダウン リストから、以下を選択します。

- year
- month
- day
- 時
- 分

手順 4　[適用（Apply）] をクリックします。

時間が更新されます。タイム ゾーンの変更については、デフォルトのタイム ゾーン設定（71-8 ページ）を参照してください。

リモート ストレージの管理

ライセンス: 任意（Any）

防御センター の では、バックアップとレポート用にローカルまたはリモート ストレージを使用できます。バックアップとレポートのリモート ストレージでは、ネットワーク ファイル システム（NFS）、セキュア シェル（SSH）、またはサーバ メッセージ ブロック（SMB）/Common Internet File System（CIFS）を使用できます。1 つのリモート システムにバックアップを送信し、別のリモート システムにレポートを送信することはできませんが、どちらかをリモート システムに送信し、もう一方をローカルの防御センターに格納することは可能です。バックアップと復元については、バックアップと復元の使用（70-1 ページ）を参照してください。

ヒント　リモート ストレージを構成して選択した後は、接続データベースの制限を**増やさなかった**場合に**のみ**、ローカル ストレージに戻すことができます。

外部リモート ストレージ システムが機能しており防御センターからアクセスできることを確認してください。

バックアップとレポートのストレージ オプションとして、次のいずれかを選択してください。

- 外部リモート ストレージを無効にして、バックアップとレポートのストレージ用にローカルの防御センターを使用するには、ローカル ストレージの使用（64-18 ページ）を参照してください。
- バックアップとレポートのストレージ用に NFS を使用するには、リモート ストレージでの NFS の使用（64-18 ページ）を参照してください。

- バックアップとレポートのストレージ用に SSH 経由のセキュア シェル（SCP）を使用するには、リモート ストレージでの SSH の使用（64-19 ページ）を参照してください。
- バックアップとレポートのストレージ用に SMB を使用するには、リモート ストレージでの SMB の使用（64-20 ページ）を参照してください。

（注）　リモート バックアップおよび復元を使用して Blue Coat X-Series 向け Cisco NGIPS 上のデータを管理することはできません。

ローカルストレージの使用

ライセンス：任意（Any）

ローカルの防御センターにバックアップとレポートを格納できます。

バックアップとレポートをローカルで格納する方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

[リモート ストレージ デバイス（Remote Storage Device）] ページが表示されます。

手順 3　[ストレージタイプ（Storage Type）] ドロップダウン リストから [ローカル（リモートストレージ以外）（Local (No Remote Storage)）] を選択します。

手順 4　[保存（Save）] をクリックします。

選択したストレージの場所が保存されます。

ヒント　ローカル ストレージでは [テスト（Test）] ボタンを使用しません。

リモート ストレージでの NFS の使用

ライセンス：任意（Any）

ネットワーク ファイル システム（NFS）プロトコルを選択して、レポートとバックアップを格納できます。必要に応じて、NFS マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[詳細オプションの使用（Use Advanced Options）] チェックボックスを選択します。

NFS を使用してバックアップとレポートを格納する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[リモート ストレージ デバイス（Remote Storage Device）] をクリックします。

[リモート ストレージ デバイス（Remote Storage Device）] ページが表示されます。

手順 3　[ストレージタイプ（Storage Type）] ドロップダウン リストから [NFS] を選択します。

ページが更新され、NFS ストレージ構成オプションが表示されます。

手順 4　接続情報を追加します。

- [ホスト（Host）] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [ディレクトリ（Directory）] フィールドに、ストレージ領域へのパスを入力します。

手順 5　必要なコマンドライン オプションがある場合は、[詳細オプションの使用（Use Advanced Options）] を選択します。

[コマンドライン オプション（Command Line Options）] フィールドが表示され、マウント バイナリ オプションを入力できます。

手順 6　[システムの用途（System Usage）] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[バックアップで使用（Use for Backups）] を選択します。
- 指定したホストにレポートを格納するには、[レポートで使用（Use for Reports）] を選択します。
- リモート ストレージへのバックアップに関する [ディスクスペースしきい値（Disk Space Threshold）] を入力します。デフォルトは 90 % です。

手順 7　必要に応じて、[テスト（Test）] をクリックします。

このテストは、防御センターが指定されたホストおよびディレクトリにアクセスできることを確認します。

手順 8　[保存（Save）] をクリックします。

リモート ストレージの構成が保存されます。

リモート ストレージでの SSH の使用

ライセンス: 任意（Any）

セキュア コピー（SCP）を使用してレポートとバックアップを格納するには、[SSH] を選択します。必要に応じて、SSH マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[詳細オプションの使用（Use Advanced Options）] チェックボックスを選択します。

注意　アプライアンスの STIG コンプライアンスを有効にすると、そのアプライアンスのリモート ストレージでは SSH を使用できません。詳細については、STIG コンプライアンスの有効化（63-27 ページ）を参照してください。

SSH を使用してバックアップとレポートを格納する方法:

アクセス:管理

手順 1　[システム(System)] > [ローカル(Local)] > [構成(Configuration)] の順に選択します。

[情報(Information)] ページが表示されます。

手順 2　[リモート ストレージ デバイス(Remote Storage Device)] をクリックします。

[リモート ストレージ デバイス(Remote Storage Device)] ページが表示されます。

手順 3　[ストレージのタイプ(Storage Type)] で [SSH] を選択します。

ページが更新され、SSH 経由の SCP ストレージ構成オプションが表示されます。

手順 4　接続情報を追加します。

- [ホスト(Host)] フィールドに、ストレージ システムの IP アドレスまたはホスト名を入力します。
- [ディレクトリ(Directory)] フィールドに、ストレージ領域へのパスを入力します。
- [ユーザ名(Username)] フィールドにストレージ システムのユーザ名を入力し、[パスワード(Password)] フィールドにそのユーザのパスワードを入力します。ドメインを指定するには、ユーザ名の前にドメインとスラッシュ(/)を付けます。
- SSH キーを使用するには、[SSH 公開キー(SSH Public Key)] フィールドの内容をコピーして authorized_keys ファイルに貼り付けます。

手順 5　必要なコマンドライン オプションがある場合は、[詳細オプションの使用(Use Advanced Options)] を選択します。

[コマンドライン オプション(Command Line Options)] フィールドが表示され、マウント バイナリ オプションを入力できます。

手順 6　[システムの用途(System Usage)] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[バックアップで使用(Use for Backups)] を選択します。
- 指定したホストにレポートを格納するには、[レポートで使用(Use for Reports)] を選択します。

手順 7　必要に応じて、[テスト(Test)] をクリックします。

このテストは、防御センターが指定されたホストおよびディレクトリにアクセスできることを確認します。

手順 8　[保存(Save)] をクリックします。

リモート ストレージの構成が保存されます。

リモート ストレージでの SMB の使用

ライセンス:任意(Any)

サーバ メッセージ ブロック(SMB)プロトコルを選択して、レポートとバックアップを格納できます。必要に応じて、SMB マウントのマニュアル ページに記載されているいずれかのマウント バイナリ オプションを使用するには、[詳細オプションの使用(Use Advanced Options)] チェックボックスを選択します。たとえば、SMB を使用するときは、[コマンドラインのオプション(Command Line Options)] フィールドに次の形式でセキュリティ モードを入力できます。

```
sec=mode
```

mode は、リモート ストレージで使用するセキュリティ モードです。設定オプションについては、セキュリティ モードの設定の表を参照してください。

表 64-6　セキュリティ モードの設定

[モード(Mode)]	説明
<なし>	NULL ユーザ(名前なし)として接続します。
krb5	Kerberos バージョン 5 認証を使用します。
krb5i	Kerberos 認証とパケット署名を使用します。
ntlm	NTLM パスワード ハッシュを使用します。(デフォルト)。
ntlmi	署名付きの NTLM パスワード ハッシュを使用します(/proc/fs/cifs/PacketSigningEnabled がオンになっている場合またはサーバが署名を要求する場合はデフォルト)。
ntlmv2	NTLMv2 パスワード ハッシュを使用します。
ntlmv2i	パケット署名付きの NTLMv2 パスワード ハッシュを使用します。

SMB を使用してバックアップとレポートを格納する方法:

アクセス: 管理

手順 1　[システム(System)] > [ローカル(Local)] > [構成(Configuration)] の順に選択します。

[情報(Information)] ページが表示されます。

手順 2　[リモート ストレージ デバイス(Remote Storage Device)] をクリックします。

[リモート ストレージ デバイス(Remote Storage Device)] ページが表示されます。

手順 3　[ストレージのタイプ(Storage Type)] で [SMB] を選択します。

ページが更新され、SMB ストレージ構成オプションが表示されます。

手順 4　接続情報を追加します。

- [ホスト(Host)] フィールドに、ストレージ システムの IPv4 アドレスまたはホスト名を入力します。
- [共有(Share)] フィールドに、ストレージ領域の共有を入力します。システムに認識されるのは、ファイルのフル パスではなく、最上位の共有だけであることに注意してください。指定した共有ディレクトリをリモート バックアップ先として使用するには、それを Windows システムで共有する必要があります。
- 必要に応じて、[ドメイン(Domain)] フィールドにリモート ストレージ システムのドメイン名を入力します。
- [ユーザ名(Username)] フィールドにストレージ システムのユーザ名を入力し、[パスワード(Password)] フィールドにそのユーザのパスワードを入力します。

手順 5　必要なコマンドライン オプションがある場合は、[詳細オプションの使用(Use Advanced Options)] を選択します。

[コマンドライン オプション(Command Line Options)] フィールドが表示され、セキュリティ モードなどのマウント バイナリ コマンドを入力できます。詳細については、表 64-6セキュリティ モードの設定(64-21 ページ)を参照してください。

手順 6　[システムの用途(System Usage)] で、次のいずれかまたは両方を選択します。

- 指定したホストにバックアップを格納するには、[バックアップで使用(Use for Backups)] を選択します。
- 指定したホストにレポートを格納するには、[レポートで使用(Use for Reports)] を選択します。

手順 7　必要に応じて、[テスト(Test)] をクリックします。

このテストは、防御センターが指定されたホストおよびディレクトリにアクセスできることを確認します。

手順 8　[保存(Save)] をクリックします。

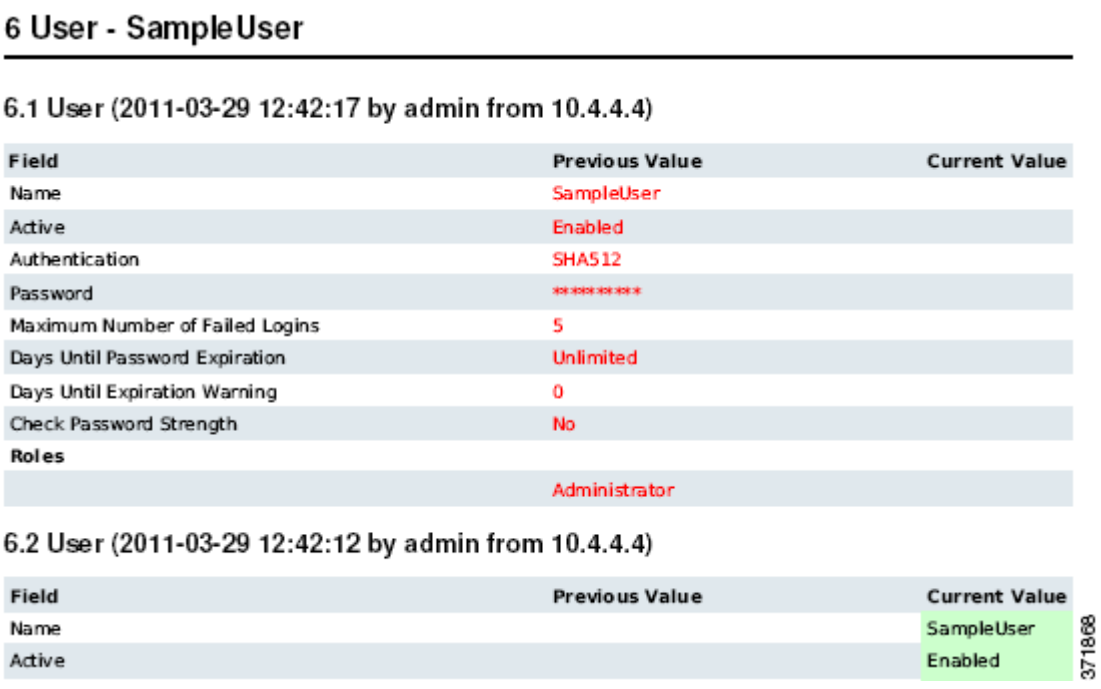
リモート ストレージの構成が保存されます。

変更調整について

ライセンス: 任意(Any)

ユーザが行う変更を監視し、それらが組織の推奨する標準に従っていることを確認するため、過去 24 時間に行われたシステム変更の詳細なレポートを電子メールで送信するようにシステムを設定できます。ユーザが変更をシステム構成に保存するたびに、変更のスナップショットが取得されます。変更調整レポートは、これらのスナップショットによる情報を組み合わせて、最近のシステム変更の概要を提供します。

次の図は、変更調整レポートの [ユーザ(User)] セクションの例を示しています。ここには、各構成の変更前の値と変更後の値の両方が一覧表示されています。ユーザが同じ構成に対して複数の変更を行った場合は、個々の変更の概要が最新のものから順に時系列でレポートに一覧表示されます。



6 User - SampleUser

6.1 User (2011-03-29 12:42:17 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name	SampleUser	
Active	Enabled	
Authentication	SHA512	
Password	*********	
Maximum Number of Failed Logins	5	
Days Until Password Expiration	Unlimited	
Days Until Expiration Warning	0	
Check Password Strength	No	
Roles		
	Administrator	

6.2 User (2011-03-29 12:42:12 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name		SampleUser
Active		Enabled

371868

過去 24 時間に行われた変更を参照できます。ただし、それ以前の変更を確認するには、監査ログを参照する必要があります。詳細については、監査ログを使って変更を調査する（69-9 ページ）を参照してください。

変更調整機能を使用する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[変更調整（Change Reconciliation）] をクリックします。

[変更調整（Change Reconciliation）] ページが表示されます。

手順 3　[有効（Enable）] チェックボックスを選択します。

手順 4　[実行時刻（Time to Run）] ドロップダウン リストから、システムが変更調整レポートを送信する時刻を選択します。

手順 5　[メール送信先（Email to）] フィールドに、レポートの受信者の電子メール アドレスを入力します。いつでも [最新レポートの再送信（Resend Last Report）] をクリックして、最新の変更調整レポートのコピーを受信者に再送信できます。

（注）　変更調整レポートを受信するには、最初にメール リレー ホストと通知アドレスを設定する必要があります。詳細については、メール リレー ホストおよび通知アドレスの設定（63-20 ページ）を参照してください。

手順 6　必要に応じて、変更調整レポートにポリシー変更の記録を含めるには、[ポリシー設定を含める（Include Policy Configuration）] を選択します。これには、アクセス制御、侵入、システム、ヘルス、およびネットワーク検出の各ポリシーの変更が含まれます。このオプションを選択しなかった場合は、ポリシーの変更はどれもレポートに表示されません。

（注）　このオプションは管理対象デバイスでは使用できません。

手順 7　必要に応じて、過去 24 時間に行われたすべての変更の記録を変更調整レポートに含めるには、[すべての変更履歴を表示（Show Full Change History）] を選択します。このオプションを選択しなかった場合は、変更がカテゴリごとに統合された形でレポートに表示されます。

手順 8　[保存（Save）] をクリックします。

変更が保存されます。このレポートは、毎日、ユーザが選択した時刻に実行されます。

リモート コンソール アクセスの管理

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

アプライアンス上でリモート アクセスを行うため、VGA ポート（デフォルト）または物理アプライアンス上のシリアル ポートを介して Linux システムのコンソールを使用できます。組織のシスコ導入の物理レイアウトに最も適したオプションを選択してください。

Serial Over LAN（SOL）接続のデフォルトの管理インターフェイス（eth0）で Lights-Out 管理（LOM）を使用すると、アプライアンスの管理インターフェイスにログインすることなく、リモートで シリーズ 3 アプライアンスをモニタリングまたは管理できます。アウト オブ バンド管理接続のコマンドライン インターフェイスを使用すると、シャーシのシリアル番号の表示や状態（ファン速度や温度など）のモニタリングなど、限定的なタスクを実行できます。シリーズ 2、仮想アプライアンス、ASA FirePOWER モジュール、Blue Coat X-Series 向け Cisco NGIPSは LOM をサポートしていません。

LOM は、アプライアンスとアプライアンスを管理するユーザの両方で有効にする必要があります。アプライアンスとユーザを有効にした後、サードパーティ製の Intelligent Platform Management Interface（IPMI）ユーティリティを使用し、アプライアンスにアクセスして管理します。

（注）　3D71xx、3D82xx、または 3D83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

詳細は、次のトピックを参照してください。

- アプライアンス上のリモート コンソール設定の構成（64-24 ページ）
- Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）
- Serial over LAN 接続の使用（64-27 ページ）
- Lights-Out 管理の使用（64-28 ページ）

アプライアンス上のリモート コンソール設定の構成

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

リモートで管理するアプライアンスの Web インターフェイスを使用して、使用するリモート コンソール アクセスのオプションを選択し設定します。

シリーズ 2、仮想アプライアンス、ASA FirePOWER モジュール、Blue Coat X-Series 向け Cisco NGIPS は LOM をサポートしていないので注意してください。

（注）　LOM/SOL を使用して シリーズ 3 デバイスに接続する前に、デバイスの管理インターフェイスに接続されたサードパーティ製のスイッチング機器のスパニング ツリー プロトコル（STP）を無効にする必要があります。

リモート コンソール設定を構成する方法：

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[コンソール設定（Console Configuration）] を選択します。

[コンソール設定（Console Configuration）] ページが表示されます。

手順 3　リモート コンソール アクセスのオプションを選択します。

- アプライアンスの VGA ポートを使用するには、[VGA] を選択します。これがデフォルトのオプションです。
- アプライアンスのシリアル ポートを使用する場合やシリーズ 3 防御センター、3D7050、8000 シリーズデバイスで LOM/SOL を使用する場合は、[物理シリアルポート（Physical Serial Port）] を選択します。

  3D2100、3D2500、3D3500、および 3D4500 管理対象デバイスにはシリアル ポートはありません。
- 7000 シリーズ デバイス（3D7050 以外）で LOM/SOL を使用する場合は、[Lights-Out 管理（Lights-Out Management）] を選択します。これらのデバイスでは、SOL と通常のシリアル接続を同時に使用することはできません。

[物理シリアルポート（Physical Serial Port）] または [Lights-Out 管理（Lights-Out Management）] を選択した場合は、LOM の設定が表示されます。

（注）　リモート コンソールを [物理シリアルポート（Physical Serial Port）] から [Lights-Out 管理（Lights-Out Management）] に変更した場合や、70xx ファミリデバイス（3D7050 以外）で [Lights-Out 管理（Lights-Out Management）] から [物理シリアルポート（Physical Serial Port）] に変更した場合は、アプライアンスを 2 回リブートしないと期待どおりのブート プロンプトが表示されないことがあります。

手順 4　SOL 経由で LOM を設定するには、次の該当する設定値を入力します。

- アプライアンスの DHCP 設定（[DHCP] または [静的（Static）]）
- LOM に使用する [IP アドレス（IP Address）]

（注）　LOM IP アドレスは、アプライアンスの管理インターフェイスの IP アドレスとは異なる必要があります。

- アプライアンスの [ネットマスク（Netmask）]
- アプライアンスの [デフォルト ゲートウェイ（Default Gateway）]

手順 5　[保存（Save）] をクリックします。

アプライアンスのリモート コンソール構成が保存されます。Lights-Out 管理を構成した場合は、少なくとも 1 人のユーザに対してそれを有効にする必要があります。Lights-Out 管理ユーザ アクセスの有効化（64-25 ページ）を参照してください。

Lights-Out 管理ユーザ アクセスの有効化

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

サポートされる防御センター：シリーズ 3

Lights-Out 管理機能を使用するユーザに対して、この機能の権限を明示的に付与する必要があります。各アプライアンスのローカル Web インターフェイスを使用して、アプライアンスごとに LOM と LOM ユーザを設定します。つまり、防御センターを使用して管理対象デバイスで LOM を設定することはできません。同様に、ユーザはアプライアンスごとに個別に管理されるため、防御センターで LOM 対応ユーザを有効化または作成しても、管理対象デバイスのユーザにはその機能が伝達されません。

LOM ユーザには、次のような制約もあります。

- ユーザに Administrator ロールを割り当てる必要があります。
- ユーザ名に使用できるのは英数字 16 文字までです。LOM ユーザに対し、ハイフンやそれより長いユーザ名はサポートされていません。
- 3D7100 ファミリ デバイスを除き、パスワードには最大 20 文字の英数字を使用できます。3D7110、3D7115、3D7120、または 3D7125 デバイスで LOM が有効になっている場合、パスワードには最大 16 文字の英数字を使用できます。20 または 16 文字よりも長いパスワードは、LOM ユーザに対してサポートされません。ユーザの LOM パスワードは、そのユーザのシステム パスワードと同じです。シスコでは辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更することを推奨しています。
- シリーズ 3 防御センターおよび 8000 シリーズ デバイスには、最大 13 人の LOM ユーザを設定できます。7000 シリーズ デバイスには、最大 8 人の LOM ユーザを設定できます。

あるロールを持つユーザのログイン中に LOM でそのロールを非アクティブ化してから再アクティブ化した場合や、ユーザのログイン セッション中にそのユーザまたはユーザ ロールをバックアップから復元した場合、そのユーザは IPMItool コマンドへのアクセスを回復するために Web インターフェイスにログインし直す必要があります。詳細については、事前定義ユーザ ロールの管理（61-53 ページ）を参照してください。

Lights-Out 管理ユーザ アクセスを有効化または表示する方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [ユーザ管理（User Management）] を選択します。

[ユーザ管理（User Management）] ページが表示されます。

手順 2　次の選択肢があります。

- 既存のユーザに LOM ユーザ アクセスを許可するには、リスト内のユーザ名の横にある編集アイコン（  ）をクリックします。
- 新しいユーザに LOM ユーザ アクセスを許可するには、[ユーザの作成（Create User）] をクリックします。

手順 3　[ユーザ設定（User Configuration）] で、Administrator ロールを有効にします。

[管理者のオプション（Administrator Options）] が表示されます。

手順 4　[Lights-Out 管理アクセスを許可（Allow Lights-Out Management Access）] チェックボックスを選択します。

手順 5　[保存（Save）] をクリックします。

このアプライアンスの LOM アクセスがユーザに付与されます。

Serial over LAN 接続の使用

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3

コンピュータ上でサードパーティ製の IPMI ユーティリティを使用して、アプライアンスへの Serial over LAN 接続を確立できます。コンピュータで Linux 系環境または Mac 環境を使用している場合は IPMItool を使用し、Windows 環境の場合は IPMIutil を使用します。

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Linux

多くのディストリビューションで IPMItool が標準となっており、使用可能です。

Mac

Mac では、IPMItool をインストールする必要があります。最初に、Mac に Apple の XCode Apple Developer Tools がインストールされていることを確認します。これにより、コマンドライン開発用のオプション コンポーネント（新しいバージョンでは UNIX Development and System Tools、古いバージョンでは Command Line Support）がインストールされていることを確認できます。次に、MacPorts と IPMItool をインストールします。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows では、IPMIutil をコンパイルする必要があります。コンパイラにアクセスできない場合は、IPMIutil 自体を使用してコンパイルできます。詳細については、好みの検索エンジンを使用するか、次のサイトを参照してください。

```
http://ipmiutil.sourceforge.net/
```

IPMI ユーティリティのコマンドについて

IPMI ユーティリティで使用するコマンドは、次の IPMItool の例に示したセグメントで構成されます。

```
ipmitool -I lanplus -H IP_address -U user_name command
```

引数の説明

- `ipmitool` はユーティリティを起動します
- `-I lanplus` はセッションの暗号化を有効にします
- `-H IP_address` はアクセスするアプライアンスの IP アドレスを示します
- `-U user_name` は権限を持つユーザの名前です
- `-command` は指定するコマンドの名前です

（注） シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

Windows 用の同等のコマンドは次のとおりです。

```
ipmiutil command -V 4 -J 3 -N IP_address -U user_name
```

このコマンドは、アプライアンスのコマンドラインにユーザを接続します。これによって、ユーザは物理的にそのアプライアンスの近くにいるときと同じようにログインできます。場合によっては、パスワードの入力を求められます。

Serial over LAN 接続を作成する方法:

アクセス:LOM アクセスのある Admin

手順 1　次のコマンドを入力します。

IPMItool の場合:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

（注）　シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil の場合:

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

アプライアンスのコマンドライン ログインが表示されます。場合によっては、パスワードの入力を求められます。

Lights-Out 管理の使用

ライセンス:任意（Any）

サポートされるデバイス:シリーズ 3

サポートされる防御センター:シリーズ 3

Lights-Out 管理では、アプライアンスにログインすることなく、デフォルトの管理インターフェイス（eth0）から SOL 接続を介して一連の限定操作を実行できます。SOL 接続を作成するコマンドに続いて、次の表に示すいずれかのコマンドを使用します。コマンドが完了すると、接続は終了します。電源制御コマンドの中には70xx ファミリデバイスに対して有効でないものもあります。

（注）　3D71xx、3D82xx、または 3D83xx デバイスのベースボード管理コントローラ（BMC）は、ホストの電源がオンのときにのみ 1Gbps のリンク速度でアクセスできます。デバイスの電源がオフの場合、BMC は 10/100 Mbps でのみイーサネット リンクを確立できます。したがって、デバイスにリモートから電源供給するために LOM を使用している場合は、10/100 Mbps のリンク速度だけを使用してデバイスをネットワークに接続してください。

注意　稀に、コンピュータがアプライアンスの管理インターフェイスとは異なるサブネットにあり、そのアプライアンスに DHCP が構成されている場合は、シリーズ 3アプライアンスの LOM 機能にアクセスしようとすると失敗することがあります。この場合は、アプライアンスの LOM を無効にして再び有効にするか、または同じサブネット上のコンピュータをアプライアンスとして使用して、その管理インターフェイスを ping することができます。その後、LOM を使用できるようになるはずです。

注意　シスコでは、Intelligent Platform Management Interface（IPMI）標準（CVE20134786）に内在する脆弱性を認識しています。アプライアンスで Lights-Out 管理（LOM）を有効にすると、この脆弱性が顕在化します。この脆弱性を軽減するために、信頼済みユーザだけがアクセス可能なセキュアな管理ネットワークにアプライアンスを展開し、辞書に載っていない複雑な最大長のパスワードをアプライアンスに対して使用し、それを 3 か月ごとに変更してください。この脆弱性のリスクを回避するには、LOM を有効にしないでください。

アプライアンスへのアクセス試行がすべて失敗した場合は、LOM を使用してリモートでアプライアンスを再起動できます。SOL 接続がアクティブなときにシステムが再起動すると、LOM セッションが切断されるか、またはタイムアウトする可能性があります。

注意　アプライアンスが別の再起動の試行に応答している間は、アプライアンスを再起動**しないでください**。リモートでアプライアンスを再起動すると、通常の方法でシステムがリブートしないため、データが失われる可能性があります。

表 64-7　Lights-Out 管理のコマンド

IPMItool	IPMIutil	説明
(適用なし)	`-V 4`	IPMI セッションの管理者権限を有効にします
`-I lanplus`	`-J 3`	IPMI セッションの暗号化を有効にします
`-H`	`-N`	リモート アプライアンスの IP アドレスを指定します
`-U`	`-U`	認可された LOM アカウントのユーザ名を指定します
`sol activate`	`sol -a`	SOL セッションを開始します
`sol deactivate`	`sol -d`	SOL セッションを終了します
`chassis power cycle`	`power -c`	アプライアンスを再起動します（70xx ファミリ デバイスでは無効）
`chassis power on`	`power -u`	アプライアンスの電源を投入します
`chassis power off`	`power -d`	アプライアンスの電源を切断します（70xx ファミリ デバイスでは無効）
`sdr`	センサー	アプライアンスの情報（ファン速度や温度など）を表示します

たとえば、アプライアンスの情報のリストを表示する IPMItool のコマンドは、次のとおりです。

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

（注）　シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil ユーティリティの同等のコマンドは次のとおりです。

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

Lights-Out 管理を使用する方法:

アクセス:LOM アクセスのある Admin

手順 1　次のコマンドを入力します。

IPMItool の場合:

```
ipmitool -I lanplus -H IP_address -U user_name command
```

（注）　シスコでは、IPMItool バージョン 1.8.12 以降の使用を推奨しています。

IPMIutil の場合:

```
ipmiutil -J 3 -H IP_address -U username command
```

command は、Lights-Out 管理のコマンドの表に示されたいずれかのコマンドです。

この表に示された対応するアクションが実行されます。場合によっては、パスワードの入力を求められます。

クラウド通信の有効化

ライセンス:URL Filtering または Malware

サポートされる防御センター:任意（DC500 を除く）

FireSIGHT システム は、シスコ の Collective Security Intelligence クラウド に接続してさまざまなタイプの情報を取得します。

- 組織に FireAMP サブスクリプションがある場合は、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（FireAMP 用のクラウド接続の操作（37-29 ページ）を参照）。
- アクセス コントロール ルールに関連付けられたファイル ポリシーにより、管理対象デバイスによるネットワーク トラフィック内で送信されるファイルの検出が許可されます。防御センター は、シスコ クラウドからのデータを使用して、ファイルがマルウェアに相当するかどうかを判定します。ファイル ポリシーの概要と作成（37-11 ページ）を参照してください。
- URL フィルタリングを有効にすると、防御センター は、一般的にアクセスされる多数の URL のカテゴリとレピュテーション データを取得し、さらに未分類 URL の検索も実行します。その後、アクセス コントロール ルールの URL 条件をすばやく作成できます。レピュテーション ベースの URL ブロッキングの実行（16-12 ページ）を参照してください。

ファイルおよびマルウェアに関するクラウドベースの機能については、組織が追加のセキュリティを必要とする場合や外部接続を制限したい場合に、標準のクラウド接続の代わりに FireAMP プライベート クラウドを使用できます。すべてのファイルおよびマルウェアのクラウド ルックアップ、および FireAMPエンドポイントからのイベント データの収集とリレーは、プライベート クラウドを介して処理されます。プライベート クラウドは、シスコのパブリック クラウドに接続したときに、匿名化されたプロキシ接続を介してこれらの処理を行います。プライベート クラウドは、動的分析や FireAMP 以外のクラウド機能（セキュリティ インテリジェンスや URL フィルタリングなど）をサポートしていませんが、ユーザの観点からは標準のパブリック クラウド接続とほぼ同じように機能します。プライベート クラウドの構成方法の詳細については、FireAMP プライベート クラウドの操作（37-33 ページ）を参照してください。

防御センター のローカル構成を使用して、次のオプションを指定します。

URL フィルタリングを有効にする（Enable URL Filtering）

カテゴリおよびレピュテーションベースの URL フィルタリングを実行するには、このオプションを有効にする必要があります。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親ドメインのサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親サイトのデータが使用されます。これらのデバイスには、7100 ファミリと、以下の ASA FirePOWER モデルが含まれます。ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X。

仮想デバイスの場合は、インストール ガイドを参照して、カテゴリとレピュテーション ベースの URL フィルタリングを実行するための適切なメモリ量の割り当てを確認してください。

不明 URL のクエリ クラウド（Query Cloud for Unknown URL）

監視対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムがクラウドを照会できるようにします。

クラウドが URL のカテゴリまたはレピュテーションを識別できない場合や、防御センターがクラウドに接続できない場合、その URL は、カテゴリまたはレピュテーション ベースの URL 条件を含むアクセス コントロール ルールと一致**しません**。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

プライバシー上の理由などで、未分類の URL を シスコ クラウドでカタログ化したくない場合は、このオプションを無効にします。

自動アップデートを有効にする（Enable Automatic Updates）

システムが定期的にクラウドに接続して、アプライアンスのローカル データ セットに含まれる URL データの更新を取得できるようにします。クラウドはそのデータを通常 1 日に 1 回更新しますが、自動更新を有効にすると 防御センター によるチェックが 30 分ごとに強制的に行われ、常に最新の情報が保持されるようになります。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムがクラウドに接続するタイミングを厳密に制御する必要がある場合は、URL フィルタリング更新の自動化（62-20 ページ）で説明しているように、自動更新を無効にして、代わりにスケジューラを使用できます。

（注） シスコ では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。手動でオンデマンド更新を実行することもできますが、定期的にクラウドに接続するようにシステムを自動化することで、最も関連性の高い最新の URL データを取得できます。

シスコ とのマルウェアイベントの URI 情報の共有

必要に応じて、ネットワーク トラフィックで検出されたファイルに関する情報を防御センターからクラウドに送信できます。この情報には、検出されたファイルに関連する URL 情報およびファイルの SHA256 ハッシュ値が含まれます。共有はオプトインですが、この情報をシスコに送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

ネットワーク AMP ルックアップでのレガシーポート 32137 の使用

このチェックボックスを選択すると、システムがネットワーク クラウド ルックアップでポート 443/tcp の代わりにポート 32137/tcp（以前のデフォルト ポート）を使用できるようになります。アプライアンスをFireSIGHT システムの以前のバージョンから更新した場合は、デフォルトでこのチェックボックスが選択されています。

ライセンス

カテゴリおよびレピュテーションベースの URL フィルタリングとデバイスベースのマルウェア検出を実行するには、管理対象デバイスで適切なライセンスを有効にする必要があります（FireSIGHT システム のライセンス（65-1 ページ）を参照）。

防御センターに URL Filtering または Malware ライセンスがない場合は、クラウド接続オプションを構成**できません**。どちらかのライセンスがあってもう一方がない場合は、[クラウドサービス（Cloud Services）] ローカル構成ページに、ライセンスがあるオプションのみが表示されます。ライセンスが期限切れになっている 防御センター では、クラウドに接続できません。

防御センターに URL Filtering ライセンスを追加すると、URL フィルタリングの設定オプションが表示されることに加えて、[URL フィルタリングを有効にする（Enable URL Filtering）] と [自動アップデートを有効にする（Enable Automatic Updates）] が自動的に有効になります。必要な場合は、手動でこれらのオプションを無効にすることができます。

FireAMP サブスクリプションを使用してエンドポイントベースのマルウェア イベントを受信する場合は、ライセンスは不要であり、許可またはブロックする個々の URL や URL のグループを指定する必要もありません。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）および手動による URL ブロッキングの実行（16-15 ページ）を参照してください。

インターネット アクセスとハイ アベイラビリティ

システムはシスコクラウドへの接続にポート 80/HTTP および 443/HTTPS を使用し、プロキシの使用もサポートします。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。

ハイ アベイラビリティの導入では、防御センター間ですべての URL フィルタリング構成と情報が同期されますが、URL フィルタリング データをダウンロードするのはプライマリ防御センターだけです。プライマリ防御センターに障害が発生した場合は、セカンダリ防御センターがインターネットに直接アクセスできることを確認し、セカンダリ防御センターの Web インターフェイスを使用して [アクティブ（Active）] に昇格させる必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

一方、ハイ アベイラビリティ ペアの防御センターは、ファイル ポリシーと関連する構成を共有しますが、クラウド接続やマルウェア処理は共有しません。運用の継続性を確保し、検出されたファイルのマルウェア性質が両方の防御センターで同じであるようにするためには、プライマリとセカンダリ両方の防御センターがクラウドにアクセスできなければなりません。

ヘルス モニタリング

デフォルトのヘルス ポリシーには、防御センターのクラウド接続の状態と安定性を追跡する次のモジュールが含まれています。

- URL フィルタリング モニタ。これは、防御センターがその管理対象デバイスにカテゴリとレピュテーションの更新をプッシュできない場合にも、ユーザに対して警告を表示します。
- Advanced Malware Protection

ヒント　もう 1 つのモジュールである FireAMP ステータス モニタは、FireAMP サブスクリプションの保有者のために、防御センターからシスコ クラウドへの接続を追跡します。ヘルス モニタリングの詳細については、ヘルス モニタの使用（68-46 ページ）を参照してください。

次の手順は、シスコ クラウドとの通信を有効にする方法、および URL データのオンデマンド更新を実行する方法を示しています。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

クラウドとの通信を有効にするには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[クラウド サービス（Cloud Services）] をクリックします。

[クラウド サービス（Cloud Services）] ページが表示されます。URL Filtering ライセンスがある場合は、このページに URL データの最終更新時間が表示されます。

手順 3　上記の説明に従って、クラウド接続のオプションを構成します。

[自動アップデートを有効にする（Enable Automatic Updates）] または [不明 URL のクエリ クラウド（Query Cloud for Unknown URL）] を有効にするには、あらかじめ [URL フィルタリングを有効にする（Enable URL Filtering）] を有効にする必要があります。

手順 4　[保存（Save）] をクリックします。

設定が保存されます。URL フィルタリングを有効にした場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にしたかどうかによって、防御センターがクラウドから URL フィルタリング データを取得します。

システムの URL データのオンデマンド更新を実行するには、次の手順を実行します。

アクセス：管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[URL フィルタリング（URL Filtering）] をクリックします。

[URL フィルタリング（URL Filtering）] ページが表示されます。

手順 3　[今すぐ更新（Update Now）] をクリックします。

防御センター がクラウドに接続し、更新が使用可能な場合はその URL フィルタリング データを更新します。

VMware ツールの有効化

ライセンス: 任意（Any）

サポートされる防御センター: 仮想

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- スナップショット
- timeSync
- vmbackup

サポート対象のすべての ESXi バージョンで VMware Tools を有効化できます。サポートされているバージョンのリストについては、『*FireSIGHT システム Virtual Installation Guide*』を参照してください。VMwareツールのすべての機能については、VMware の Web サイト（http://www.vmware.com/）を参照してください。

次の手順では、仮想防御センター上で Web インターフェイスの構成メニューを使用して VMware Tools を有効にする方法について説明します。仮想デバイスには Web インターフェイスがないため、仮想デバイスではコマンドライン インターフェイスを使用して VMwareツールを有効にする必要があります。『*FireSIGHT システム Virtual Installation Guide*』を参照してください。

仮想防御センターで VMware ツールを有効にする方法:

アクセス: 管理

手順 1　[システム（System）] > [ローカル（Local）] > [構成（Configuration）] の順に選択します。

[情報（Information）] ページが表示されます。

手順 2　[VMware ツール（VMware Tools）] をクリックします。

[VMware ツール（VMware Tools）] ページが表示されます。

手順 3　[VMware ツールを有効化（Enable VMware Tools）] をクリックしてから、[保存（Save）] をクリックします。

変更が保存されます。