Firepower システム ホスト入力 API ガイド

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は当社の
Web サイト
(www.cisco.com/go/offices) をご覧ください。

バージョン 6.0
2016 年 5 月 30 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

ホスト入力について

Firepower Management Center にはネットワーク内の他のソースからデータをインポートし、モニタ対象のホスト情報を増強するためのツールが用意されています。

ホスト入力 API を使用してネットワーク マップ情報を送信するには 2 つの方法があります。1 つは Management Center の nmimport ツールを実行する方法、もう 1 つはリモート クライアントを使用する方法です。いずれの場合も、カンマ区切り値（CSV 形式）のテキスト ファイルでネットワーク マップの詳細を指定します。ホスト入力インポート ツールの使用（2-1 ページ）で、一般的な手順を説明し、CSV ファイル形式を定義し、nmimport ツールの使用方法について説明します。ホスト入力クライアントの設定（3-1 ページ）ではホスト インポート クライアントの使用方法について説明します。

たとえば、新しい FirePOWER システムを設定する場合、資産管理ソフトウェアに記載されたすべてのコンピュータがネットワーク マップに存在することの確認が必要になる場合があります。そのような場合は、資産管理アプリケーションからホストのデータをエクスポートし、結果を適切な形式のテキスト ファイルにして、ホスト入力インポート ツールを使用してデータをインポートできます。資産管理システムに各ホストのオペレーティング システム情報が含まれている場合、資産管理システムについてサードパーティ製品マップを設定し、対応するシスコのラベルにサードパーティのオペレーティング システム ラベルをマッピングできます。インポートを実行する前にそのマップを設定すると、システムは該当するシスコオペレーティング システム定義を各ホストと関連付けます。

Firepower Management Center でホスト入力インポート ツールを使用するには 4 つの主要な手順があります。

1. サードパーティ製ホスト データを使用して影響の関連付けを実行する場合は、サードパーティ製品マップを設定し、Management Center Web インターフェイスを使用してサービス、オペレーティング システム、またはフィックス定義をシスコの製品またはフィックス定義にマップできます。
2. サードパーティの脆弱性をインポートする場合、サードパーティの脆弱性マップを設定し、Management Center Web インターフェイスを使用してサードパーティの脆弱性 ID 文字列をシスコ脆弱性 ID にマップできます。このマッピングはインポート ファイルでも実行できることに注意してください。
3. ホスト入力インポート ツールの使用（2-1 ページ）の説明に従ってサードパーティ アプリケーションからデータをエクスポートし、CSV ファイル形式にします。
4. nmimport ツールまたはホスト入力クライアントを使用して CSV ファイルを送信します。

前提条件

このマニュアルの情報を理解するには、Firepower Management Center の機能と名称、およびそのコンポーネントの機能（特に、ネットワーク マップ）、そしてシステムが生成するさまざまな関連のイベント データに精通する必要があります。これらの機能に関する情報は、なじみのない用語や製品固有の用語の定義と共に、『*Firepower Management Center Configuration Guide*』から参照できます。このマニュアルに記載されているデータ フィールドに関するその他の情報も、この『*Configuration Guide*』から入手できます。

製品バージョンの互換性

次の表に、さまざまなホスト入力機能に必要な製品バージョンを示します。

表 1-1　製品バージョンの互換性

機能	製品バージョン
ホスト入力機能	Firepower Management Center バージョン 4.9+
ホスト入力外部クライアント機能	Firepower Management Center バージョン 5.0+
ホスト入力モバイル デバイス識別機能	Firepower Management Center バージョン 5.1+
IPv6 アドレスのサポート	Firepower Management Center バージョン 5.2+
複数ドメインのサポート	Firepower Management Center バージョン 6.0+

表記法

次の表に、ホスト入力コールで使用されるさまざまなデータ フィールドのフォーマットを説明するために、このマニュアルで使用される名前を示します。

表 1-2　重要な値データ型の規則

データ タイプ	説明
uint	符号なし整数
uint8	符号なし 8 ビット整数
uint32	符号なし 32 ビット整数
string	文字データを格納する可変長のバイト列。

ホスト入力スクリプトのリソース

次に、マニュアルで説明されるトピックの一部と、詳細の検索場所について説明します。

表 1-3　ホスト入力のリソース

内容	検索場所
ホスト入力インポート ツール	ホスト入力インポート ツールの使用（2-1 ページ）
ホスト入力インポート ツールで使用するインポート ファイルの作成に関するガイドライン	ホスト入力インポート ファイルの作成（2-3 ページ）
インポート ファイルに含める特定のホスト入力関数の構文	ホスト入力インポートの構文（2-6 ページ）
ホスト入力インポート ツールの実行	ホスト入力インポートの実行（2-29 ページ）
ホスト入力参照クライアントのインストール、設定、および実行	ホスト入力参照クライアントの使用（3-2 ページ）

ホスト入力インポート ツールの使用

インポート ファイルを作成し、ホスト入力インポート ツールでそれを処理することで、ネットワーク マップにデータをインポートできます。

詳細については、次の項を参照してください。

- ホスト入力インポート ファイルの作成（2-3 ページ）
- ホスト入力インポートの構文（2-6 ページ）
- ホスト入力インポートの実行（2-29 ページ）

ホスト入力インポートを実行する準備

一部のホスト インポート操作は、ユーザが Management Center Web インターフェイスを使用してサードパーティの製品、フィックス、および脆弱性の名前と ID をシスコデータベースにマップするために提供する、製品のマッピング情報によって異なります。インポートを予定しているデータによっては、インポートを実行する前に、以降の各項で説明する設定手順を実行する必要があります。

- サードパーティの脆弱性マップの作成（2-1 ページ）
- サードパーティ製品マップの作成（2-2 ページ）

サードパーティの脆弱性マップの作成

サードパーティの脆弱性を含むデータをインポートし、影響の関連付けにそのデータを使用する場合は、データをインポートする前にサードパーティの脆弱性マップ セットを作成する必要があります。サードパーティ マップ セットにより、システムはサードパーティの脆弱性 ID を、これに対応するシスコ脆弱性 ID に変換できます。インポートする前にサードパーティの脆弱性をマッピングしなかった場合、その脆弱性はシスコ脆弱性 ID にマッピングされず、影響の関連付けに使用できません。マップ セットは、Management Center Web インターフェイスを使用する方法と `AddScanResult` コマンドを使用する方法の 2 とおりの方法で作成できます。このコマンドを使用してスキャン結果をインポートする場合は、必ず、ネットワーク検出ポリシーの入力ソースのソース定義を編集して、スキャナにアイデンティティ ソース タイプを設定してください。

サードパーティ脆弱性マッピングは、任意のドメイン レベルで作成できます。`SetMap` コマンドを使用して、マッピングに使用するマップ名を指定します。マップは、CSV ファイルで使用されるネットマップまたは、そのいずれかの親で定義する必要があります。

Web インターフェイスを介したサードパーティの脆弱性マッピングの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。`SetMap` コマンドおよび `AddScanresult` コマンドの詳細については、インポート ファイルの形式について（2-4 ページ）を参照してください。

サードパーティ製品マップの作成

ホストにオペレーティング システムやサーバのデータをインポートする際に、サードパーティの製品名の詳細をシスコ製品定義にマッピングできます。Management Center Web インターフェイスを介してサードパーティ製品マップを作成できます。

サードパーティ製品マップ セットにより、システムはサードパーティ ベンダー、製品、およびバージョンを対応するシスコ定義に変換できます。サーバ定義またはオペレーティング システム定義を含むサードパーティ製品マップを設定しておけば、API を使用してサードパーティ製サーバまたはオペレーティング システムを追加または設定する際に、同じスクリプト内では、そうしたサーバやオペレーティング システムの表示文字列を定義するだけですみます。

サードパーティ製品マップを使用して、サードパーティ製フィックスをシスコフィックス定義にマップした後に、サードパーティ製フィックスの名前を使用してフィックスをホストに追加した場合、システムは該当するシスコフィックス定義にそのフィックスをマップして、フィックスにより対処された脆弱性を非アクティブ化します。

サードパーティ製品をシスコ製品定義にマッピングする方法:

アクセス: Admin

1. [Policies] > [Application Detectors] を選択し、[User Third-Party Mappings] をクリックします。

   [User Third-Party Mappings] ページが表示されます。

2. 次の 2 つの選択肢があります。

- 既存のマップ セットを編集するには、マップ セットの横にある [Edit] をクリックします。
- 新しいマップ セットを作成するには、[Create Product Map Set] をクリックします。

  [Edit Third-Party Product Mappings] ページが表示されます。

3. [Mapping Set Name] フィールドにマッピング セットの名前を入力します。
4. [Description] フィールドに説明を入力します。
5. 次の 2 つの選択肢があります。

- サードパーティ製品をマッピングするには、[Add Product Map] をクリックします。
- 既存のサードパーティ製品マップを編集するには、マップ セットの横にある [Edit] をクリックします。

  [Add Product Map] ページが表示されます。

6. [Vendor String] フィールドにサードパーティ製品によって使用されるベンダー文字列を入力します。
7. [Product String] フィールドにサードパーティ製品によって使用される製品文字列を入力します。
8. [Version String] フィールドにサードパーティ製品によって使用されるバージョン文字列を入力します。
9. [Product Mappings] セクションで、以下のリストから脆弱性マッピングに使用するオペレーティング システム、製品、およびバージョンを選択します(該当する場合)。

- Vendor
- Product
- Major Version
- Minor Version
- Revision Version

- Build
- Patch
- Extension

  たとえば、名前がサードパーティ文字列で構成される製品を実行するホストで Red Hat Linux 9 の脆弱性を使用する場合、ベンダーとして [Redhat, Inc.]、製品として [Redhat Linux]、バージョンとして [9] を選択します。

10. [Save] をクリックします。

    サードパーティ製品マップを作成した後に、`SetOS`、`SetService`、または `AddService` コマンドを使用してデータをインポートできます。データをインポートする前に、サードパーティ製品の名前の詳細とシスコ製品定義をメモします。

サードパーティ製品とシスコ製品の詳細の場所

アクセス: Admin

1. [Policies] > [Application Detectors] を選択します。

   [Application Detectors] ページが表示されます。

2. [User Third-Party Mappings] を選択します。

   [Third-Party Product Mappings] ページが表示されます。

3. 製品マップ セットの編集アイコン( )をクリックします。

   [Edit Third-Party Product Mappings] ページが表示されます。

4. 製品マップの編集アイコン( )をクリックします。

   [Add Product Map] ポップアップ ウィンドウが表示されます。[Vendor String]、[Product String]、および [Version String] の各値をメモします。

   サードパーティ製品のマッピングの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

ホスト入力インポート ファイルの作成

この章では、ホスト入力インポート ツールのインポート コマンドを使用してデータをインポートする構文の詳細について説明します。インポート ファイルを作成するときには、以降の各項の説明に必ず従ってください。

- インポート ファイルの形式について(2-4 ページ)
- ドメインの設定(2-4 ページ)
- ソース タイプの設定(2-5 ページ)
- ソース ID の設定(2-5 ページ)
- サードパーティ製品マップの設定(2-5 ページ)

インポート ファイルの形式について

一般に、インポート ファイルは 1 行に 1 コマンドを含み、コマンド パラメータをカンマ区切り値（CSV 形式）で指定したテキスト ファイルです。ファイルでの操作の必要に応じて、ファイルの先頭にいくつかの主要コマンドを配置する必要があります。これらの主要コマンドはここで説明しますが、他のすべてのコマンドはホスト入力インポートの構文（2-6 ページ）で後述します。

注意：システムは解釈できないインポート ファイルのデータをすべて破棄します。インポートを実行する前にインポート ファイルをテストするには、Management Center でインポートをテストする（2-28 ページ）を参照してください。

インポートするデータのアプリケーション ソース名を提供し、サードパーティ製品の名前マッピングを設定するには、ホスト入力インポート ファイルを、SetDomain（ドメインを使用する場合）、SetSource、および SetMap コマンドで始める必要があります。詳細については、インポート ファイルの形式について（2-4 ページ）を参照してください。

ファイルの SetDomain、SetSource、および SetMap コマンドの後に、さらにコマンド ラインを追加できます。各コマンド ラインには 1 つのコマンドとそのコマンドに必要なパラメータが含まれ、改行で終了します。一部のフィールドは、ホスト入力が成功して、意味のあるデータをネットワーク マップに追加することを確実にするために、その情報を提供しなければならない場合にのみ必要です。たとえば、システムへのフィックスの追加は、既存の シスコ フィックス定義に一致するフィックスの ID 番号やフィックスの名前を指定せずに、そしてサードパーティのフィックスをシスコのフィックスにマッピングせずに行うことができます。

組み込むことができる個々のコマンドの構文の詳細については、以降の各項を参照してください。

- ホスト コマンド（2-7 ページ）
- サーバ コマンド（2-9 ページ）
- クライアント アプリケーション コマンド（2-13 ページ）
- プロトコル コマンド（2-15 ページ）
- パッケージ フィックス コマンド（2-16 ページ）
- ホスト属性コマンド（2-18 ページ）
- 脆弱性コマンド（2-19 ページ）
- サードパーティ製品マップの設定（2-5 ページ）

完全なインポート ファイルの例とファイルの各セクションの説明を調べるには、ホスト入力インポート ファイルの例（2-23 ページ）を参照してください。

ドメインの設定

システムに複数のドメインが定義されている場合は、インポート ファイルの先頭にターゲット ドメインを指定しなければならないことがあります。クライアント証明書でもインポート ファイルでもリーフ ドメインを指定しない場合、インポートを実行すると失敗し、エラー メッセージが表示されます。

- システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン導入環境では、ネットワーク マップのデータを追加するリーフ ドメインを指定する必要があります。
- ホスト入力クライアントを使用して CSV コマンドを送信する場合は、各リーフ ドメインに別個のクライアント証明書を作成できます。そのような証明書を使用する場合、すべての操作は証明書のドメインを対象とします。その場合、スクリプトで SetDomain コマンドを使用する理由はありません。

- ドメインを持つシステムに nmimport ツールを使用する場合、インポート ファイルは SetDomain コマンドで始まる必要があります。SetDomain コマンドまたは証明書によっていずれのリーフ ドメインも指定されていない場合、どのコマンドも処理されずにインポートは失敗し、エラー メッセージが表示されます。
- ドメイン名は完全修飾され、各ドメイン レベル間はスペース バックスラッシュ スペースで区切られる必要があります。たとえば次のようになります。`Global \ Accounting` または `Global \ Sales \ East` ドメイン名の大文字と小文字は、ドメイン定義と同じである必要があります。

ドメインを設定するには次の手順を実行します。

インポート ファイルの最初の行で、次の構文を使用します。

`SetDomain, DomainName`

ここで、`SetDomain` はコマンド名、*`DomainName`* はインポートするデータを追加するリーフ ドメインの完全修飾名です。

ソース タイプの設定

インポート ファイルの先頭で、インポートするデータのソース タイプを識別する必要があります。このコマンドを使用してスキャン結果をインポートする場合は、必ず、ネットワーク検出ポリシーの入力ソースのソース定義を編集して、スキャナにアイデンティティ ソース タイプを設定してください。

ソース タイプを設定するには次の手順を実行します。

1. 次の構文を使用して、インポート ファイルに行を追加します。

   `SetSourceType, Sourcetype`

   ここで、`SetSourceType` はコマンド名、*`Sourcetype`*はインポートするデータに追加またはインポートするデータで使用するソースのタイプです。有効な値は `2`（スキャナ）または `3`（アプリケーション）です。

   `SetSourceType` を使用しない場合、デフォルトのタイプは `3`（アプリケーション）です。

ソース ID の設定

インポート ファイルの先頭に、インポートするデータのソース ID を設定する必要があります。

ソース アプリケーションの名前を設定するには次の手順を実行します。

1. 次の構文を使用して、インポート ファイルに行を追加します。

   `SetSource, SourceID`

   ここで、`SetSource` はコマンド名、*`SourceID`* はインポートするデータのソース アプリケーションとして表示する ID 文字列です。

   次に、SetSource コマンドの例を示します。

   ```
   # Set the current SOURCE_ID and Product Map to "Custom Utility"
   SetSource, Custom Utility
   ```

   ファイル例のコンテキストでこのコマンドを確認するには、ファイル例の全容（2-27 ページ）を参照してください。

サードパーティ製品マップの設定

サードパーティのオペレーティング システム、サーバ、またはフィックス定義をインポートする場合、サードパーティの名前に対応するユーザ サードパーティ製品マップを作成する必要があります。このコマンドを使用して、現在のセッションに現在のサードパーティ マップを設定できます。それぞれのサードパーティ ベンダー、製品、およびバージョンの組み合わせと、それに対応するシスコ製品定義の間の再利用可能なマップを作成するために、Management Center Web インターフェイスを使用して、サードパーティ マッピングを

作成します。サードパーティ マップを設定し、その後にマップに含まれているサードパーティ アプリケーションの名前を含むホストのオペレーティング システムまたはサーバのデータを追加または設定する場合、システムはマッピングを使用してシスコ製品定義および関連付けられた脆弱性を、入力が発生する各ホストにマップします。

たとえば、•Custom Utility•というマップ セットを作成し、その中で次のようにサードパーティの文字列を定義できます。

- [Vendor String] - Microsoft
- [Product String] - Win7

マップ セットで次のシスコ製品マッピングを選択できます。

- [Vendor] - Microsoft, Corp.
- [Product] - Windows 7
- [Patch] - SP3

SetMap, Custom Utility を呼び出してこの製品マップを設定すると、Microsoft Windows 7 製品の VDB エントリに Microsoft Win7 がマップされます。

サードパーティ製品マップ セットを設定するには次の手順を実行します。

1. 次の構文を使用して、インポート ファイルに行を追加します。

   SetMap, *Third-PartyProductMapName*
   ここで、SetMap はコマンド名、*Third-PartyProductMapName* はインポートに使用するサードパーティ製品マップ セットの名前です。

   たとえば、SetSource コマンドの後ろに次のコード行を配置できます。

   SetMap, Custom Utility
   また、このコマンドを使用して、インポート ファイル内の別のサードパーティ製品マップに変更することもできます。

ホスト入力インポートの構文

ソース ID の設定（2-5 ページ）で説明したように、インポート ファイルでソース ID および製品マップを設定した後に、さまざまなホスト入力コマンドを使用して、ネットワーク マップに追加する特定のデータをインポートするための行を追加できます。インポート コマンドの呼び出しはそれぞれ改行で終了し、1 セットのインポート データをインポートする必要があります。完全なインポート ファイル例については、ホスト入力インポート ファイルの例（2-23 ページ）を参照してください。

使用できる個々のコマンドの詳細については、次の各項を参照してください。

- ホスト コマンド（2-7 ページ）
- サーバ コマンド（2-9 ページ）
- クライアント アプリケーション コマンド（2-13 ページ）
- プロトコル コマンド（2-15 ページ）
- パッケージ フィックス コマンド（2-16 ページ）
- ホスト属性コマンド（2-18 ページ）

- 脆弱性コマンド（2-19 ページ）
- スキャン結果コマンド（2-21 ページ）

ホスト コマンド

ホスト入力 API を使用して、ネットワーク マップへのホストの追加と削除、ホストのオペレーティング システム定義の設定ができます。

ホスト コマンドの詳細については、以降の項を参照してください。

- AddHost（2-7 ページ）
- DeleteHost（2-7 ページ）
- SetOS（2-8 ページ）
- UnsetOS（2-9 ページ）

AddHost

`AddHost` コマンドを使用して、ネットワーク マップにホストを追加できます。IP ホスト（IP アドレスと、オプションで MAC アドレスを持つホスト）または MAC のみホスト（MAC アドレスだけを持つホスト）を追加できます。この方法で追加されたホストは、通常のホスト タイムアウトの対象になりません。

指定した IP アドレスまたはプライマリ MAC アドレスを持つホストがネットワーク マップにすでに含まれている場合、AddHost コマンドは何の影響もありません。ネットワーク マップ内のホストの既存の情報を新しい情報で置き換えることが目的の場合は、AddHost コマンドの前に DeleteHost コマンドを使用する必要があります。

次の構文を使用します。

```
AddHost, ip_address, mac_address
```

表 2-1　AddHost のフィールド

フィールド	説明	必須	値
ip_address	追加するホストの IP アドレスを指定します。	Yes（MAC アドレスが指定されていない場合）	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
mac_address	追加するホストの MAC アドレスを指定します。	Yes（IP アドレスが指定されていない場合）	単一の MAC アドレス。

DeleteHost

`DeleteHost` コマンドを使用して、ネットワーク マップから 1 つ以上のホストを削除できます。ホストの IP アドレスまたは MAC アドレスを指定することによって、IP ホスト（IP アドレスと、オプションで MAC アドレスを持つホスト）を削除できます。MAC のみホスト（MAC アドレスだけを持つホスト）を削除するには、MAC アドレスを入力します。

次の構文を使用します。

```
DeleteHost, ip_address, mac_address
```

表 2-2　DeleteHost のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes（MAC アドレスが指定されていない場合）	単一の IP アドレス。
mac_address	影響を受けるホストの MAC アドレスのリストを示します。	Yes（IP アドレスが指定されていない場合）	単一の MAC アドレス。

SetOS

`SetOS` コマンドを使用して、指定したホストのオペレーティング システムのベンダー、製品、バージョン、およびモバイル デバイスの情報を指定できます。オペレーティング システム情報をインポートすると、ベンダー、製品、バージョン、およびモバイル デバイス情報の表示文字列が設定されます。また、サードパーティ ベンダー、製品およびバージョンの文字列をシスコ製品定義にマッピングできます。詳細については、「サードパーティ製品マップの作成（2-2 ページ）」を参照してください。

サードパーティのオペレーティング システムの名前をシスコ定義にマップする場合は、シスコデータベースにあるそのオペレーティング システムの脆弱性が、サードパーティのデータがインポートされたホストに対応します。Management Center Web インターフェイスを使用して、サードパーティ製品マップ セットをすでに作成している場合、`SetMap` コマンドで使用するサードパーティ アプリケーションの文字列および対応するシスコ定義には、そのマップ セットに指定した値を使用できます（サードパーティ製品マップの設定（2-5 ページ）を参照）。

ホスト プロファイルに表示されるオペレーティング システムの ID は、最も優先度の高いソースによって設定されます。可能なソースには、ユーザ、スキャナおよびアプリケーション（ネットワーク検出ポリシーで設定）、FirePOWER、NetFlow の順の優先度があります。新しい、より優先度の高いオペレーティング システム ID は、現在のアプリケーション ID ほど詳細でない場合は、現在のオペレーティング システムの ID を上書きしないことに注意してください。

ホストのカスタム オペレーティング システムを定義すると、Management Center Web インターフェイスではイベント ビューまたはホスト プロファイルのホスト情報の [Source Type] フィールドに、変更のソースが示されます。

次の構文を使用します。

```
SetOS, ip_address, vendor_str, product_str, version_str, vendor_id,
product_id, major, minor, revision, build, patch, extension, device_string,
mobile, jailbroken
```

またはオペレーティング システムを設定する前に、新しい製品マップを設定するには、次の構文を使用します。

```
SetMap, map_name
SetOS, ip_address, vendor_str, product_str, version_str, vendor_id,
product_id, major, minor, revision, build, patch, extension, device_string,
mobile, jailbroken
```

サードパーティ製品マップの設定の詳細については、サードパーティ製品マップの設定（2-5 ページ）を参照してください。

表 2-3　SetOS のフィールド

フィールド	説明	必須	使用可能な値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
vendor_str	サードパーティ アプリケーションで使用されるオペレーティング システムのベンダーの表示名を入力します。	No	string

表 2-3　SetOS のフィールド（続き）

フィールド	説明	必須	使用可能な値
product_str	サードパーティ アプリケーションで使用されるオペレーティング システム製品の表示名を入力します。	No	string
version_str	サードパーティ アプリケーションで使用されるオペレーティング システムのバージョンの表示名を入力します。	No	string
vendor_id	マップするシスコベンダー定義を入力します。	No	uint32
product_id	マップするシスコ製品定義を入力します。	No	uint32
major	マップするシスコメジャー バージョン定義を入力します。	No	uint32
minor	マップするシスコマイナー バージョン定義を入力します。	No	uint32
revision	マップするシスコリビジョンの文字列を入力します。	No	uint32
build	マップするシスコビルド定義を入力します。	No	string
patch	マップするシスコパッチ定義を入力します。	No	string
extension	マップするシスコ拡張定義を入力します。	No	string
device_string	検出されたモバイル デバイスのハードウェア情報を入力します。	No	string
mobile	オペレーティング システムがモバイル デバイスで動作しているかどうかを示します。	No	uint8
jailbroken	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示します。	No	uint8

UnsetOS

`UnsetOS` コマンドを使用して、指定したホストから以前に設定された OS 定義を削除することができます。これにより OS 定義がリセットされ、今後のオペレーティング システムへの変更をシステムが追跡できるようになります。

次の構文を使用します。

```
UnsetOS, ip_address
```

ここで、*ip_address* は、オペレーティング システムの ID をリセットするホストを表す IP アドレス、CIDR ブロック、および IP アドレスの範囲のカンマ区切りリストです。

サーバ コマンド

サーバ コマンドを使用して、ネットワーク マップ内のホストのサーバ情報を更新できます。

詳細については、次の項を参照してください。

- AddService（2-10 ページ）
- SetService（2-11 ページ）
- UnsetService（2-12 ページ）
- DeleteService（2-13 ページ）
- クライアント アプリケーション コマンド（2-13 ページ）

AddService

AddService コマンドを使用して、ネットワーク マップ内の既存のホストにサーバを追加できます。

ホスト プロファイルに表示されるサーバ ID は、優先度の最も高いソースにより設定されます。可能なソースには、ユーザ、スキャナおよびアプリケーション（ネットワーク検出ポリシーで設定）、FirePOWER、NetFlow の順の優先度があります。新しい、より優先度の高いサーバ ID は、現在の ID ほど詳細でない場合は、現在稼働中のサーバ ID を上書きしないことに注意してください。

次の構文を使用します。

```
AddService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

または、サーバを追加する前に、新しい製品マップを設定するには、次の構文を使用します。

```
SetMap, map_name
AddService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

サードパーティ製品マップの設定の詳細については、サードパーティ製品マップの作成（2-2 ページ）およびサードパーティ製品マップの設定（2-5 ページ）を参照してください。

表 2-4　AddService のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	このフィールドは ip_address および proto フィールドと組み合わせて使用し、ホストに追加するサーバを指定します。	Yes	1 から 65535 の範囲の整数。
proto	このフィールドは ip_address および port フィールドと組み合わせて使用し、ホストに追加するサーバを指定します。	Yes	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。
server	シスコデータベース内のサーバの名前または ID。	No	サーバを識別するには、service_name または service_id の値を含める必要があります。どちらも指定しないと、サーバは unknown としてリストされます。サーバ名を指定すると、システムはサーバ ID を検索します。サーバ名に対する ID が存在しない場合、システムにより ID が作成されます。
vendor_str	サードパーティ アプリケーションで使用されるサーバのベンダーの表示名を入力します。	No	string
product_str	サードパーティ アプリケーションで使用されるサーバ製品の表示名を入力します。	No	string
version_str	サードパーティ アプリケーションで使用されるサーバ バージョンの表示名を入力します。	No	string
vendor_id	シスコベンダー定義を入力します。	No	uint32
product_id	シスコ製品定義を入力します。	No	uint32
major	シスコメジャー バージョン定義を入力します。	No	uint32
minor	シスコマイナー バージョン定義を入力します。	No	uint32
revision	シスコリビジョンの文字列を入力します。	No	uint32
build	マップするシスコビルド定義を入力します。	No	string

表 2-4　AddService のフィールド（続き）

フィールド	説明	必須	値
patch	マップするシスコパッチ定義を入力します。	No	string
extension	マップするシスコ拡張定義を入力します。	No	string

SetService

SetService コマンドを使用して、指定したサーバのサーバ プロトコル、ベンダー、製品、およびバージョンを指定できます。サービス キーを使用してサーバの表示文字列を設定できます。Management Center Web インターフェイスでサードパーティ製品をマッピングするか（サードパーティ製品マップの作成（2-2 ページ）を参照）、または、SetMap コマンドを使用することにより（サードパーティ製品マップの設定（2-5 ページ）を参照）、サードパーティのサーバ データを特定のシスコ製品定義の脆弱性情報と関連付けることができます。

サーバ プロトコルがまだない場合、この呼び出しにより、文字列に対して新しいサーバ ID が作成されます。指定したサーバがこの時点までに存在していなかった場合、システムによってそのサーバが作成されます。

ホスト プロファイルに表示されるサーバ ID は、優先度の最も高いソースにより設定されます。可能なソースには、ユーザ、スキャナおよびアプリケーション（ネットワーク検出ポリシーで設定）、FirePOWER、NetFlow の順の優先度があります。新しい、優先度の高いサーバ ID は、現在の ID ほど詳細でない場合は、現在のサーバ ID を上書きしないことに注意してください。

ホストのサードパーティ サーバ定義を定義すると、Firepower Management Center Web インターフェイスはイベントの [Servers] テーブル ビューまたはホスト プロファイルの [Servers] セクションの [Source Type] フィールドに、変更のソースを示します。

注：特定のホストのネットワーク マップに保存されているサーバの数が 100 を超えると、新しいサーバ情報は、サーバがホストから削除されるまで無視されます。

次の構文を使用します。

```
SetService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

または、サーバを設定する前に、新しい製品マップを設定するには、次の構文を使用します。

```
SetMap, map_name
SetService, ip_address, port, proto, server, vendor_str, version_str,
vendor_id, product_id, major, minor, revision, build, patch, extension
```

サードパーティ製品マップの設定の詳細については、サードパーティ製品マップの設定（2-5 ページ）を参照してください。

表 2-5　SetService のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	このフィールドは ip_address および proto フィールドと組み合わせて使用し、ホストに設定するサーバを指定します。	Yes	1 から 65535 の範囲の整数。
proto	このフィールドは ip_address および port フィールドと組み合わせて使用し、ホストに設定するサーバを指定します。	Yes	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。

表 2-5　SetService のフィールド（続き）

フィールド	説明	必須	値
server	シスコデータベース内のサーバの名前または ID。	No	サーバを識別するには、service_name または service_id の値を含める必要があります。どちらも指定しないと、サーバは unknown としてリストされます。サーバ名を指定すると、システムはサーバ ID を検索します。サーバ名に対する ID が存在しない場合、システムにより ID が作成されます。
vendor_str	サードパーティ アプリケーションで使用されるサーバのベンダーの表示名を入力します。	No	string
product_str	サードパーティ アプリケーションで使用されるサーバ製品の表示名を入力します。	No	string
version_str	サードパーティ アプリケーションで使用されるサーバ バージョンの表示名を入力します。	No	string
vendor_id	シスコベンダー定義を入力します。	No	uint32
product_id	シスコ製品定義を入力します。	No	uint32
major	シスコメジャー バージョン定義を入力します。	No	uint32
minor	シスコマイナー バージョン定義を入力します。	No	uint32
revision	シスコリビジョンの文字列を入力します。	No	uint32
build	マップするシスコビルド定義を入力します。	No	string
patch	マップするシスコパッチ定義を入力します。	No	string
extension	マップするシスコ拡張定義を入力します。	No	string

UnsetService

UnsetService コマンドを使用してユーザが追加したサーバ定義を指定したホストから削除できます。UnsetService では FirePOWER によって検出されたサーバ定義は削除されません。

注：特定のホストのネットワーク マップに保存されているサーバの数が 100 を超えると、新しいサーバ情報は、サーバがホストから削除されるまで無視されます。

次の構文を使用します。

```
UnsetService, ip_address, port, proto
```

表 2-6　UnsetService のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	このフィールドは ip_address および proto フィールドと組み合わせて使用し、ホストから削除するサーバを指定します。	Yes	1 から 65535 の範囲の整数。
proto	このフィールドは ip_address および port フィールドと組み合わせて使用し、ホストから削除するサーバを指定します。	Yes	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。

DeleteService

`DeleteService` コマンドを使用して、指定したホストからサーバを削除できます。削除するサーバのポートとプロトコルを指定する必要があります。

次の構文を使用します。

```
DeleteService, ip_address, port, proto
```

表 2-7　DeleteService のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	このフィールドは `ip_address` および `proto` フィールドと組み合わせて使用し、ホストで削除するサーバを指定します。	Yes	1 から 65535 の範囲の整数。
proto	このフィールドは `ip_address` および `port` フィールドと組み合わせて使用し、ホストで削除するサーバを指定します。	Yes	文字列 `tcp` または `udp`、または該当するプロトコル ID `6`(tcp)または `17`(udp)。

クライアント アプリケーション コマンド

クライアント アプリケーション コマンドを使用して、ネットワーク マップ内のホストのクライアント アプリケーションのデータを変更することができます。

詳細については、次の項を参照してください。

- AddClientApp（2-13 ページ）
- DeleteClientApp（2-14 ページ）
- DeleteClientAppPayload（2-14 ページ）

AddClientApp

`AddClientApp` コマンドを使用して、ネットワーク マップ内の既存のホストにクライアント アプリケーションを追加できます。クライアント アプリケーションの名前がシスコデータベースに存在しない場合、システムによってそのクライアント アプリケーションの新しいエントリが作成されます。

ホスト プロファイルに表示されるクライアント アプリケーションの ID は、最も優先度の高いソースによって設定されます。可能なソースには、ユーザ、スキャナおよびアプリケーション（ネットワーク検出ポリシーで設定）、FirePOWER、NetFlow の順の優先度があります。新しい優先度の高いクライアント アプリケーション ID は、現在の ID ほど詳細でない場合は、現在のクライアント アプリケーション ID を上書きしないことに注意してください。

次の構文を使用します。

```
AddClientApp, ip_address, app_name, app_type, version
```

表 2-8　AddClientApp のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
app_name	クライアント アプリケーションの名前を示します。	Yes	英数字またはスペース文字で構成される文字列。 既存のアプリケーションでは、データベース内の ID 値に相当します。システムはこの ID を検索し、既存のクライアント アプリケーション ID に一致するかどうかを調べます。一致しない場合は新しい ID が作成されます。
app_type	これは廃止予定のフィールドです。	No	ヌル値。
version	アプリケーションのバージョンを示します。	No	英数字またはスペース文字で構成される文字列。

DeleteClientApp

`DeleteClientApp` コマンドを使用して、指定したホストからクライアント アプリケーションを削除できます。

次の構文を使用します。

```
DeleteClientApp, ip_address, app_name, app_type, version
```

表 2-9　DeleteClientApp のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
app_name	クライアント アプリケーションの名前を示します。	Yes	英数字またはスペース文字で構成される文字列。 既存のアプリケーションでは、データベース内の ID 値に相当します。システムはこの ID を検索し、既存のクライアント アプリケーション ID に一致するかどうかを調べます。一致しない場合は新しい ID が作成されます。
app_type	これは廃止予定のフィールドです。	No	ヌル値。
version	アプリケーションのバージョンを示します。	No	英数字またはスペース文字で構成される文字列。

DeleteClientAppPayload

`DeleteClientAppPayload` コマンドを使用して、指定したホストから Web アプリケーションを削除できます。

次の構文を使用します。

```
DeleteClientAppPayload, ip_address, app_name, app_type, version,
payload_type, payload_id
```

表 2-10　DeleteClientAppPayload のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
app_name	クライアント アプリケーションの名前を示します。	Yes	英数字またはスペース文字で構成される文字列。 既存のアプリケーションでは、データベース内の ID 値に相当します。システムはこの ID を検索し、既存のクライアント アプリケーション ID に一致するかどうかを調べます。一致しない場合は新しい ID が作成されます。
app_type	これは廃止予定のフィールドです。	No	ヌル値。
version	アプリケーションのバージョンを示します。	No	英数字またはスペース文字で構成される文字列。
payload_type	Web アプリケーション カテゴリを示します。	Yes	番号 `0`。 既存のアプリケーションでは、データベース内の ID 値に相当します。システムはこのタイプを検索し、既存の Web アプリケーション タイプに一致するかどうかを調べます。一致しない場合は新しいタイプが作成されます。
payload_id	Web アプリケーションの名前を示します。	Yes	英数字またはスペース文字で構成される文字列。 既存のアプリケーションでは、データベース内の ID 値に相当します。システムはこの ID を検索し、既存の Web アプリケーション ID に一致するかどうかを調べます。一致しない場合は新しい ID が作成されます。

プロトコル コマンド

プロトコル コマンドを使用して、ネットワーク マップ内のホストのプロトコル情報を更新できます。

詳細については、次の項を参照してください。

- DeleteProtocol（2-15 ページ）
- AddProtocol（2-16 ページ）

DeleteProtocol

`DeleteProtocol` コマンドを使用して、指定した IP または MAC ホストからプロトコルを削除できます。

次の構文を使用します。

```
DeleteProtocol, ip_address, mac_address, proto, type
```

表 2-11　DeleteProtocol のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes（MAC アドレスが指定されていない場合）	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
mac_address	影響を受けるホストの MAC アドレスのリストを示します。	Yes（IP アドレスが指定されていない場合）	区切り文字のコロン付き、またはコロンなしの、MAC アドレス文字列のリスト。

表 2-11　DeleteProtocol のフィールド（続き）

フィールド	説明	必須	値
proto	削除する ID 文字列またはプロトコル名を示します。	Yes	英数字またはスペース文字で構成される有効なプロトコル名。トランスポート プロトコル（「xport」）の場合、/etc/protocols ファイルにリストされているプロトコルを使用できます。ネットワーク プロトコル（「net」）については、ネットワーク プロトコル値（A-1 ページ）を参照してください。
type	削除するプロトコルのタイプを示します。	Yes	「xport」または「net」

AddProtocol

AddProtocol コマンドを使用して、ネットワーク プロトコルまたはトランスポート プロトコルをネットワーク マップ内の既存のホストに追加できます。プロトコル ID、Management Center の /etc/protocols ファイルに存在するトランスポート プロトコル名、または、ネットワーク プロトコル値（A-1 ページ）のネットワーク プロトコル名のいずれかを指定できます。

注：MAC のみホストへはトランスポート プロトコルを追加できません。

次の構文を使用します。

```
AddProtocol, ip_address, mac_address, proto, type
```

表 2-12　AddProtocol のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes（MAC アドレスが指定されていない場合）	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
mac_address	影響を受けるホストの MAC アドレスのリストを示します。	Yes（IP アドレスが指定されていない場合）	区切り文字のコロン付き、またはコロンなしの、MAC アドレス文字列のリスト。
proto	追加する ID 文字列またはプロトコル名を示します。	Yes	英数字またはスペース文字で構成される有効なプロトコル名。トランスポート プロトコル（「xport」）の場合、/etc/protocols ファイルにリストされているプロトコルを使用できます。ネットワーク プロトコル（「net」）については、ネットワーク プロトコル値（A-1 ページ）を参照してください。
type	追加するプロトコルのタイプを示します。	Yes	「xport」または「net」

パッケージ フィックス コマンド

パッケージ フィックス コマンドを使用して、インポートを実行するリーフ ドメインのネットワーク マップ内のホストに対してフィックスの適用または削除ができます。

詳細については、次の項を参照してください。

- AddFix（2-17 ページ）
- RemoveFix（2-17 ページ）

AddFix

AddFix コマンドを使用して、指定したホストまたはサーバにフィックスをマップできます。シスコ脆弱性データベース（VDB）のフィックス ID、または、Management Center Web インターフェイスを使用して VDB のフィックスにマップするサードパーティのフィックスを使用して、フィックスをマップできます。

ホストまたはサーバにフィックスを適用すると、システムの脆弱性マッピングが調整され、フィックスが適用された脆弱性は Web インターフェイスで無効とマークされて、影響の評価に使用されません。ただし、適用されるフィックスを OS またはサーバ ID に適用できない場合、そのフィックスの影響はありません。

次の構文を使用します。

```
AddFix, ip_address, port, proto, fix_id
```

表 2-13　AddFix のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	proto フィールドと共に、インポートを実行するホストの変更の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	1 から 65535 の範囲の整数。
proto	port フィールドと共に、インポートを実行するホストの変更の影響を受けるサーバを指定します。	No	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。
fix_id	フィックスの ID 文字列を示します。	Yes	シスコフィックスの ID 番号、または、AddFix コマンドを呼び出す前に SetMap コマンドを呼び出して使用するサードパーティ製品マップで定義されたフィックス名。詳細については、サードパーティ製品マップの設定（2-5 ページ）を参照してください。

RemoveFix

RemoveFix コマンドを使用して、指定したホストまたはサーバからフィックス マッピングを削除できます。フィックスを削除すると、脆弱性マッピングが適宜更新されます。

次の構文を使用します。

```
RemoveFix, ip_address, port, proto, fix_id
```

表 2-14　RemoveFix のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	proto フィールドと共に、インポートを実行するホストの変更の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	1 から 65535 の範囲の整数。

表 2-14　RemoveFix のフィールド（続き）

フィールド	説明	必須	値
proto	port フィールドと共に、インポートを実行するホストの変更の影響を受けるサーバを指定します。	No	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。
fix	フィックスの ID 文字列を示します。	Yes	シスコフィックス名、または、AddFix コマンドを呼び出す前に SetMap コマンドを呼び出して使用する、サードパーティ製品マップで定義されたフィックス名。詳細については、サードパーティ製品マップの設定（2-5 ページ）を参照してください。

ホスト属性コマンド

ホスト入力インポート ツールを使用して、インポートするリーフ ドメインのネットワーク マップの属性値を設定できます。詳細については、次の項を参照してください。

- AddHostAttribute（2-18 ページ）
- DeleteHostAttribute（2-18 ページ）
- SetAttributeValue（2-18 ページ）
- DeleteAttributeValue（2-19 ページ）

AddHostAttribute

AddHostAttribute コマンドを使用して、テキスト属性または URL 属性を追加できます。ホスト属性の追加により、属性の値が追加されることはありません。属性値の設定の詳細については、次のSetAttributeValue（2-18 ページ）を参照してください。

次の構文を使用します。

```
AddHostAttribute, attributename, attributetype
```

ここで、*attributename* は属性の名前（英数字とスペース文字で構成されます）で、*attributetype* は属性のタイプ（「text」または「URL」）。

DeleteHostAttribute

DeleteHostAttribute コマンドを使用して属性を削除できます。

次の構文を使用します。

```
DeleteHostAttribute, attributename
```

ここで、*attributename* は属性の名前です（有効な名前は英数字とスペース文字で構成されます）。

SetAttributeValue

SetAttributeValue コマンドを使用して、指定したホストの既存の属性の値を、指定した値に設定することができます。このコマンドは、ユーザ定義のホスト属性および Criticality 属性の値を設定できます。属性 ID として「criticality」を使用することにより、このコマンドを使用してホストの重要度を設定できます。

次の構文を使用します。

```
SetAttributeValue, ip_address, attribute, value
```

表 2-15　SetAttributeValue のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
attribute	ホストの属性名を示します。	Yes	英数字またはスペース文字で構成される有効な属性名。
value	ホスト属性値を示します。	Yes	英数字またはスペース文字で構成される、名前付き属性の有効な属性値。リスト属性に値が渡される場合、その値はリスト属性の既存の名前付き値である必要があります。

DeleteAttributeValue

`DeleteAttributeValue` コマンドを使用して、ホストの属性値を削除できます。

次の構文を使用します。

```
DeleteAttributeValue, ip_address, attribute, value
```

表 2-16　DeleteAttributeValue のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
id	ホストの属性名を示します。	Yes	英数字またはスペース文字で構成される有効な属性名。
value	ホスト属性値を示します。	Yes	英数字またはスペース文字で構成される、名前付き属性の有効な属性値。リスト属性に値が渡される場合、その値はリスト属性の既存の名前付き値である必要があります。

脆弱性コマンド

脆弱性コマンドを使用して、ホストの脆弱性状態を更新できます。

詳細については、次の項を参照してください。

- SetInvalidVulns（2-19 ページ）
- SetValidVulns（2-20 ページ）

SetInvalidVulns

`SetInvalidVulns` コマンドを使用して、あるホストまたは一連のホストで脆弱性を非アクティブ化できます。このコマンドの呼び出しが有効になるには、脆弱性がホストに存在し、有効に設定されている必要があります。

次の構文を使用します。

```
SetInvalidVulns, ip_address, port, proto, type, vuln_id
```

表 2-17　SetInvalidVulns のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	`proto` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	1 から 65535 の範囲の整数。
proto	`port` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	文字列 `tcp` または `udp`、または該当するプロトコル ID `6`（tcp）または `17`（udp）。
vuln_id	脆弱性の脆弱性 ID を示します。	Yes	有効なシスコ脆弱性 ID、またはマッピングされたサードパーティの脆弱性 ID。 サードパーティの脆弱性では、サードパーティの脆弱性 ID をマップし、設定された脆弱性マップを `vuln_type` フィールドで参照する必要があります。詳細については、サードパーティの脆弱性マップの作成（2-1 ページ）を参照してください。

SetValidVulns

`SetValidVulns` コマンドを使用して、あるホストまたは一連のホストで脆弱性をアクティブ化できます。あるホストの脆弱性を有効に設定すると、有効な脆弱性にイベントの SID がマップされた場合に、Management Center によってそのイベントに赤色の影響が割り当てられます。このコマンドの呼び出しが有効になるには、脆弱性がホストに存在し、無効に設定されている必要があります。

次の構文を使用します。

```
SetValidVulns, ip_address, port, proto, type, vuln_id
```

表 2-18　SetValidVulns のフィールド

フィールド	説明	必須	値
ip_address	影響を受けるホストの IP アドレスを含む文字列を示します。	Yes	IP アドレス、CIDR マスク範囲、IP-IP 範囲、またはそれらの値の引用符付きカンマ区切りリスト。
port	`proto` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	1 から 65535 の範囲の整数。
proto	`port` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（フィックスをサーバに適用する場合）	文字列 `tcp` または `udp`、または該当するプロトコル ID `6`（tcp）または `17`（udp）。
vuln_id	脆弱性の脆弱性 ID を示します。	Yes	有効なシスコ脆弱性 ID、またはマッピングされたサードパーティの脆弱性 ID。 サードパーティの脆弱性では、サードパーティの脆弱性 ID をマップし、設定された脆弱性マップを `vuln_type` フィールドで参照する必要があります。詳細については、サードパーティの脆弱性マップの作成（2-1 ページ）を参照してください。

スキャン結果コマンド

ホスト入力インポート ツールを使用して、スキャン結果を Management Center に追加し、追加した結果をデータベースにフラッシュできます。スキャン結果を追加する際に、結果のサードパーティの脆弱性を CVE または BugTraq の脆弱性にマッピングできます。

詳細については、次の項を参照してください。

- AddScanResult コマンド（2-21 ページ）
- ScanFlush コマンド（2-22 ページ）
- ScanUpdate コマンド（2-22 ページ）
- DeleteScanResult コマンド（2-23 ページ）

AddScanResult コマンド

`AddScanResult` コマンドを使用して、サードパーティの脆弱性スキャナのスキャン結果を追加し、それぞれの脆弱性を BugTraq または CVE ID にマッピングできます。このコマンドを使用してスキャン結果をインポートする場合は、必ず、ネットワーク検出ポリシーの入力ソースのソース定義を編集して、スキャナにアイデンティティ ソース タイプを設定してください。

次の構文を使用します。

```
AddScanResult, ipaddr, scanner_id, vuln_id, port, protocol, name,
description, cve_ids, bugtraq_ids
```

注：ScanUpdate コマンドと ScanFlush コマンドのどちらを使用するかによって、結果がどのように追加されるかが異なります。詳細については、ScanFlush コマンド（2-22 ページ）およびScanUpdate コマンド（2-22 ページ）を参照してください。

表 2-19　AddScanResult のフィールド

フィールド	説明	必須	使用可能な値
ipaddr	スキャンされたホストの IP アドレスを示します。	Yes	単一の IP アドレス。
scanner_id	スキャン結果を取得したスキャナのスキャナ ID を示します。	Yes	'scanner_id' ここで `scanner_id` は、追加する脆弱性データのソースであるスキャナの名前を示す文字列です。 以前に使用したスキャナのスキャン結果を追加するには、結果を追加した Management Center のシステム ポリシーにリストされている特定のスキャナの名前を指定します。 新しいスキャナ ID の結果を追加すると、そのスキャナがシステム ポリシーに追加されます。デフォルトでは、新しいスキャナは最も低い優先度で追加されます。スキャナの優先度を変更する場合は、システム ポリシーで変更できます。詳細については、『*Firepower Management Center Deployment Guide*』を参照してください。
vuln_id	脆弱性の脆弱性 ID を示します。	Yes	有効なシスコ脆弱性 ID、またはマッピングされたサードパーティの脆弱性 ID。 このフィールド、port、protocol、bugtraq_ids、および cve_ids が空の場合、全体的なスキャン結果になります。

表 2-19　AddScanResult のフィールド（続き）

フィールド	説明	必須	使用可能な値
port	`proto` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（脆弱性をサーバに適用する場合）	1 から 65535 の範囲の整数。
proto	`port` フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	Yes（脆弱性をサーバに適用する場合）	文字列 `tcp` または `udp`、または該当するプロトコル ID `6`（tcp）または `17`（udp）。
name	インポートされる脆弱性の名前。	No	単一引用符で囲まれた文字列。次に例を示します。 `'Using NetBIOS to retrieve info from a Windows host'`
description	インポートされる脆弱性の説明。	No	単一引用符で囲まれた文字列。次に例を示します。 `'The following 2 NetBIOS names have been gathered...'`
cve_ids	CVE 脆弱性 ID のスペース区切りリスト	No	有効な CVE 脆弱性 ID。たとえば、`'cve_ids: CVE2003-0988'`。 このフィールド、port、protocol、vuln_id、および bugtraq_ids が空の場合、全体的なスキャン結果になります。
bugtraq_ids	BugTraq 脆弱性 ID のスペース区切りリスト	No	有効な BugTraq 脆弱性 ID。たとえば、`'bugtraq_ids: 9506'`。 このフィールド、port、protocol、vuln_id、および cve_ids が空の場合、全体的なスキャン結果になります。

ScanFlush コマンド

`AddScanResult` を使用してスキャン結果を Management Center に追加した後に、`ScanUpdate` コマンドまたは `ScanFlush` コマンドのいずれかを使用して、Management Center で `AddScanResult` コマンドを実行し、スキャン結果をデータベースにアップロードできるようにする必要があります。

`ScanFlush` コマンドは引数を必要とせず、データをデータベースにアップロードするインポート ファイルのどの部分でも使用できます。

`ScanFlush` コマンドを使用すると、ホストから既存のスキャン結果がすべて削除され、新しい結果だけが追加されます。

ScanUpdate コマンド

`AddScanResult` を使用してスキャン結果を Management Center に追加した後に、`ScanUpdate` コマンドまたは `ScanFlush` コマンドのいずれかを使用して、Management Center で `AddScanResult` コマンドを実行し、スキャン結果をデータベースにアップロードできるようにする必要があります。

`ScanUpdate` コマンドは引数を必要とせず、データをデータベースにアップロードするインポート ファイルのどの部分でも使用できます。

`ScanUpdate` コマンドを使用すると、既存のスキャン結果はホストから削除されません。新しいスキャン結果は既存のスキャン結果とマージされます。

`ScanUpdate` コマンドを `DeleteScanResult` コマンドと共に使用すると、特定の結果が削除されます。

`ScanUpdate` は、インポート ファイルに明示的に含まれていない場合にも、インポートの終了時に自動的に発生するので注意してください。これは、クライアント接続が終了するからです。

DeleteScanResult コマンド

DeleteScanResult コマンドを ScanUpdate コマンドと共に使用して、特定のスキャン結果を特定のホストから削除できます。

オプション パラメータの値を指定した場合は、結果はパラメータと一致するものに制限されます。オプション パラメータの値を指定しない場合は、指定した IP アドレスのすべての結果が削除されます。

次の構文を使用します。

```
DeleteScanResult, ipaddr, 'scanner_id', vuln_id, port, protocol
```

表 2-20　DeleteScanResult のフィールド

フィールド	説明	必須	使用可能な値
ipaddr	スキャンされたホストの IP アドレスを示します。	Yes	単一の IP アドレス。
scanner_id	スキャン結果を取得したスキャナのスキャナ ID を示します。	No	'scanner_id' ここで scanner_id は、追加する脆弱性データのソースであるスキャナの名前を示す文字列です。 以前に使用したスキャナのスキャン結果を追加するには、結果を追加した Management Center のシステム ポリシーにリストされている特定のスキャナの名前を指定します。 新しいスキャナ ID の結果を追加すると、そのスキャナがシステム ポリシーに追加されます。デフォルトでは、新しいスキャナは最も低い優先度で追加されます。スキャナの優先度を変更する場合は、システム ポリシーで変更できます。詳細については、『*Firepower Management Center Deployment Guide*』を参照してください。
vuln_id	脆弱性の脆弱性 ID を示します。	No	有効なサードパーティの脆弱性 ID。
port	proto フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	No	1 から 65535 の範囲の整数。
proto	port フィールドと共に、インポートを実行するホストの脆弱性の影響を受けるサーバを指定します。	No	文字列 tcp または udp、または該当するプロトコル ID 6（tcp）または 17（udp）。

ホスト入力インポート ファイルの例

次の各項では、ホスト入力インポート ツールを使用してデータをインポートするためのインポート ファイルを作成する方法の概要を説明します。

次の各項では、ファイルの各部分を順番に説明します。

- 例：ソース ドメイン、ソース ID、および製品マップの設定（2-24 ページ）
- 例：ホストの追加（2-24 ページ）
- 例：ホストへのプロトコルの追加（2-25 ページ）
- 例：ホストへのサーバの追加（2-25 ページ）

- 例:オペレーティング システムの設定(2-25 ページ)
- 例:サードパーティの脆弱性の追加(2-26 ページ)
- 例:ホストの重要度の設定(2-26 ページ)
- 例:スキャン結果の追加(2-26 ページ)
- 例:Management Center でのコマンドの実行(2-27 ページ)
- 例:ホストにクライアント アプリケーションを追加する(2-27 ページ)
- 例:MAC のみホストの追加(2-27 ページ)
- ファイル例の全容(2-27 ページ)

例:ソース ドメイン、ソース ID、および製品マップの設定

このスクリプト例は、インポートで使用されるドメイン、ソース アプリケーションの名前、および製品マップを設定する呼び出しで開始されます。

```
# Set the current DOMAIN to Global \ Sales \ East
#
SetDomain, Global \ Sales \ East
# Set the current SOURCE_ID and Product Map to "Asset Management App"
SetSource, Asset Management App
SetMap, Asset Management App
```

このソース ドメインには追加するホスト情報のホストを含むドメインを指定します。ソース ID 値には、このインポートの結果のホスト入力イベントで使用される、システムのアプリケーション名を指定します。このインポートを使用して変更されたホストのホスト入力イベントまたはホスト プロファイルを表示すると、ソース タイプの値は `Application: Asset Management App` になります。

SetMap コマンドによって参照される「Asset Management App」という製品マップは、Management Center Web インターフェイスを使用して作成されていることに注意してください。

サードパーティの製品マップは資産管理アプリケーションのマップ セットであるため、システムはインポート ファイルに含まれるコマンド内のすべてのサードパーティのオペレーティング システム名またはサーバ名を、そのマップ セットで定義された製品マップまたはフィックス マップを使用してシスコ定義にマップします(例:オペレーティング システムの設定(2-25 ページ)を参照)。

例:ホストの追加

ファイルでソース アプリケーションの名前およびサードパーティ製品マップを設定した後に、データをインポートするコマンドが続きます。SetDomain コマンドまたは証明書のいずれかで指定されたリーフ ドメインのネットワーク マップに、データが追加されます。最初のインポート コマンドは `AddHost` コマンドです。

```
# Add an IP host with no Primary MAC
#
AddHost,1.2.3.4
```

追加されたホストの IP アドレスは `1.2.3.4` であり、ホストのプライマリ MAC アドレスは設定されないことに注意してください。

例:ホストへのプロトコルの追加

インポート ファイルの次のコマンドにより、ospf プロトコルが 1.2.3.4 ホストに追加されます。

```
# Add the ospf protocol to the host
#
AddProtocol, 1.2.3.4,,ospf,xport
```

このプロトコルのプロトコル タイプは xport であることに注目してください。

例:ホストへのサーバの追加

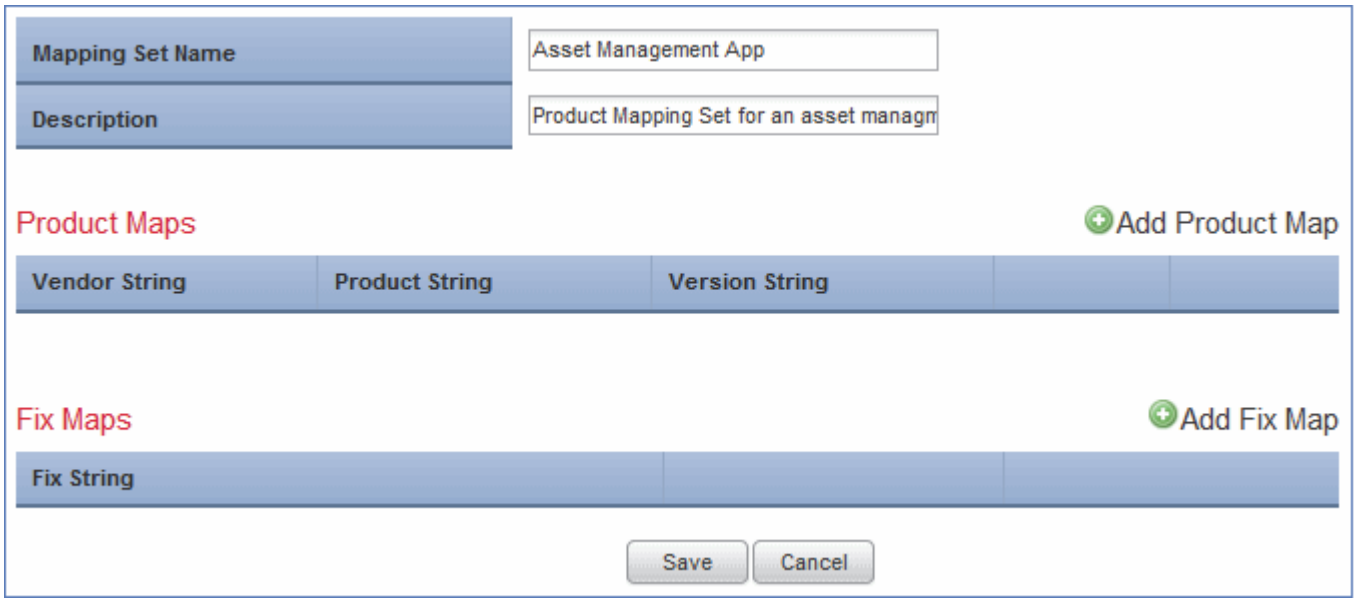
インポート ファイルの次のコマンドは AddService コマンドを使用して OpenSSH サーバを 1.2.3.4 ホストに追加します。

```
# Add a server for the host
#
AddService,1.2.3.4, 22, tcp, ssh, OpenSSH, 4.1
```

このコマンドにより、ポートが 22 に、プロトコルが tcp に、サーバ タイプが ssh に、ベンダーの表示文字列が OpenSSH に、バージョンの表示文字列が 4.1 に設定されます。

例:オペレーティング システムの設定

インポート ファイルでは次に、SetOS コマンドを使用して、ホストのオペレーティング システムの値を設定します。Asset Management App マップ セットには、サードパーティ製品名 Microsoft Win2K を Microsoft Windows 2000 SP3 のシスコ製品定義にマッピングする製品マップが含まれています。



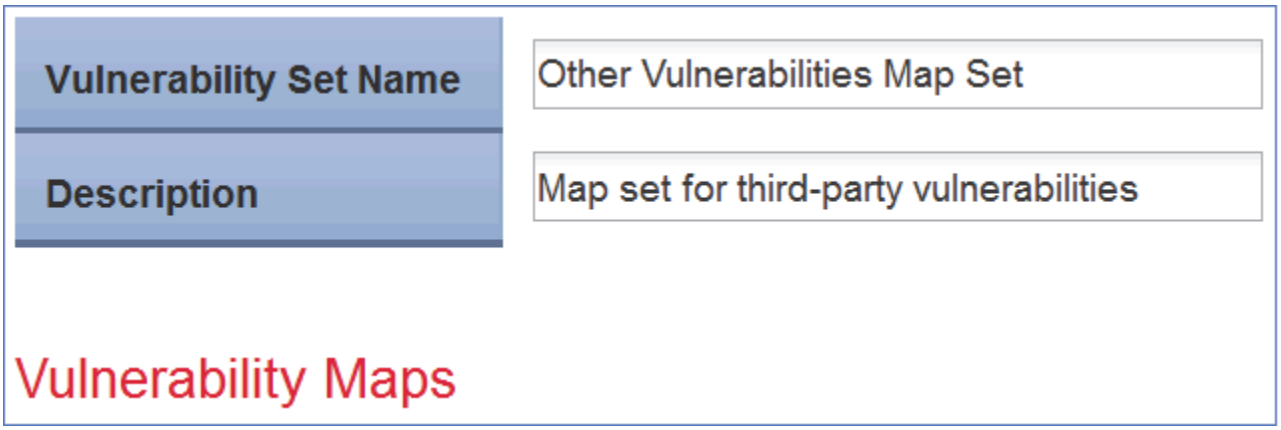
インポート ファイルのコマンドは次のようになります。

```
# Set the OS.Because the Map is set to "Asset Management App" these values
resolve to the Windows 2000 SP3 definition
#
SetOS, 1.2.3.4, Microsoft, Win2k
```

SetOS コマンド ラインにはオペレーティング システムの表示名を Microsoft Win2K に設定するための vendor_str フィールドと product_str フィールドが含まれていることに注目してください。それらは Asset Management App 製品マップ セットで定義された **Vendor String** 設定と **Product String** 設定に一致するため、システムはそのサードパーティのオペレーティング システム名をシスコ Microsoft Windows 2000 SP3 製品定義にマップします。

例：サードパーティの脆弱性の追加

インポート ファイルでは次に、サードパーティの脆弱性を 1.2.3.4 ホストにインポートします。この例では Management Center Web インターフェイスを使用して作成されたサードパーティの脆弱性マップセットが使用されています。



インポート ファイルの次のコマンドで Vuln003 という脆弱性を有効に設定します。

```
# Add a third-party vulnerability (from third-party vulnerability map "Other
Vulnerabilities Map Set") to the host
#
SetValidVuln, 1.2.3.4,,, Other Vulnerabilities Map Set, Vuln0003
```

例：ホストの重要度の設定

インポート ファイルの次のコマンドは SetAttributeValue コマンドを使用して 1.2.3.4 ホストの重要度を「High」に設定します。

```
# Set the criticality of the host to "High"
#
SetAttributeValue, 1.2.3.4,criticality,high
```

属性名が criticality に設定され、属性値が「high」に設定されます。

例：スキャン結果の追加

インポート ファイルの次のコマンド セットでは、AddHost コマンドを使用してホストを追加し、その後に AddScanResult コマンドを使用して、サードパーティ スキャナからそのホストのデータを追加します。

```
# Add IP host for scan results to follow
#
AddHost,1.2.3.5
#
# Add the scan result from a Qualys scanner to the network map
#
```

```
AddScanResult,1.2.3.5,"Qualys",82003,,,"ICMP Timestamp Request","ICMP
(Internet Control and Error Message Protocol) is a protocol encapsulated in
IP packets.Its principal purpose is to provide a protocol layer able to
inform gateways of the inter-connectivity and accessibility of other
gateways or hosts. ping is a well-known program for determining if a host is
up or down.It uses ICMP echo packets.ICMP timestamp packets are used to
synchronize clocks between hosts.","cve_ids: CVE-1999-0524","bugtraq_ids:"
```

例：Management Center でのコマンドの実行

`ScanFlush` コマンドは Management Center に対し、キューに入れられた ScanFlush 行よりも上のコマンドを実行できることを示します。

ScanFlush

例：ホストにクライアント アプリケーションを追加する

インポート ファイルは次に `AddClientApp` コマンドを使用して `BMC Remedy` という名前のクライアント アプリケーションを `1.2.3.4` ホストに追加します。

```
# Add a Client App
#
AddClientApp, 1.2.3.4, “BMC Remedy”, "Asset Manager", "0.0"
```

クライアント アプリケーション ID が `BMC Remedy` に設定され、クライアント アプリケーション タイプが `Asset Manager` に設定され、バージョンが `0.0` に設定されます。

例：MAC のみホストの追加

最後に、インポート ファイルは `AddHost` コマンドを使用して MAC のみホストを追加します。

```
# Add a MAC-only host
#
AddHost,,01:02:03:04:05:06
```

`ip_address` フィールドが空白のままで、代わりに MAC アドレスが指定されていることに注目してください。

さらに、ファイルの最後に `ScanFlush` コマンドが設定されていないにもかかわらず、インポート ファイルが終了すると、セッションが切断されるために、スクリプトの残りのデータがネットワーク マップに送信されることに注意してください。

ファイル例の全容

前述の各項で説明したインポート ファイルの全容は次のようになります。

```
# Example import file for Host Input Import Tool
#
# Set the DOMAIN to “Global \ Sales \ East”
#
# Set the current SOURCE_ID and Product Map to "Asset Management App"
#
SetDomain, Global \ Sales \ East
SetSource, Asset Management App
SetMap, Asset Management App
#
# Add an IP host with no Primary MAC
#
AddHost,1.2.3.4
#
```

```
# Add the ospf protocol to the host
#
AddProtocol, 1.2.3.4,,ospf,xport
#
# Add a server for the host
#
AddService,1.2.3.4, 22, tcp, ssh, OpenSSH, 4.1
#
# Set the OS.Because the Map is set to "Asset Management App" these values
resolve to the Windows 2000 SP3 definition
#
SetOS, 1.2.3.4, Microsoft, Win2k
#
# Add a third-party vulnerability (from third-party map "Other
Vulnerabilities Set") to the host
#
SetValidVuln, 1.2.3.4,,, Other Vulnerabilities Set, Vuln0003
#
# Set the criticality of the host to "High"
#
SetAttributeValue, 1.2.3.4,criticality,high
#
# Add IP host for scan results to follow
#
AddHost,1.2.3.5
#
# Add the scan result from a Qualys scanner to the network map
#
AddScanResult,1.2.3.5,"Qualys",82003,,,"ICMP Timestamp Request","ICMP
(Internet Control and Error Message Protocol) is a protocol encapsulated in
IP packets.Its principal purpose is to provide a protocol layer able to
inform gateways of the inter-connectivity and accessibility of other
gateways or hosts. ping is a well-known program for determining if a host is
up or down.It uses ICMP echo packets.ICMP timestamp packets are used to
synchronize clocks between hosts.","cve_ids: CVE-1999-0524","bugtraq_ids:"
#
#Send the commands above to the host input service for processing
#
ScanFlush
#
# Add a Client App
#
AddClientApp, 1.2.3.4, "BMC Remedy", "Asset Manager", "0.0"
#
# Add a MAC only host
#
AddHost,,01:02:03:04:05:06
```

Management Center でインポートをテストする

インポート ファイルが期待どおりに動作することを確認するために、インポートをシミュレートできます。多くのコマンドでは重複したデータをネットワーク マップにインポートできるため、同じインポートを複数回実行することを回避する必要があります。テスト インポートを実行すると、この問題を回避できます。また、インポート ファイルのデータでシステムが解釈できないデータは破棄されるため、インポート ファイルによりインポートが完全に実行されることを確認する必要があります。テストの結果が画面に表示される（またはファイルにリダイレクトすることもできます）ので、実際のインポートを実行する前にファイルの問題を修正できます。

インポート ファイルをテストするには、次の手順を実行します。

1. 作成したインポート ファイルを、インポートを実行する Management Center にコピーします。
2. `admin` アカウントで Management Center にログインします。
3. コマンド ラインで `nmimport.pl -t` *`filename`* を入力します。

   ログファイルにテスト インポートの結果をリダイレクトするには、コマンドの末尾に `>` *`logfilename`* を追加します。

   システムは、インポートしたデータをネットワーク マップに追加し、結果メッセージを画面に表示するか、または、指定したファイルに結果をリダイレクトします。

ホスト入力インポートの実行

コマンド ラインからホスト入力インポート ツールを実行し、作成したインポート ファイルを処理できます。

注意：システムは解釈できないインポート ファイルのデータをすべて破棄します。また、同じインポートを複数回実行すると、ネットワーク マップに一部の項目の重複データが見つかる可能性があります。これらの問題を回避するために、実際のインポートを実行する前にインポート ファイルのインポートをテストする必要があります。詳細については、Management Center でインポートをテストする（2-28 ページ）を参照してください。

Management Center にアクセスできるリモート ホストにホスト入力の参照クライアントをセットアップした場合は、`sf_host_input_agent.pl` スクリプトを使用してクライアントからのインポート ファイルを処理できます。参照クライアントのセットアップに関する詳細については、ホスト入力参照クライアントの実行（3-4 ページ）を参照してください。

インポートを実行するには、次の手順を実行します。

1. 作成したインポート ファイルを、インポートを実行する Management Center にコピーします。
2. `root` アカウントで Management Center にログインします。
3. コマンド ラインで `nmimport.pl` *`filename`* を入力します。

   ログファイルにテスト インポートの結果をリダイレクトするには、コマンドの末尾に `>` *`logfilename`* を追加します。

   システムは、インポートしたデータをネットワーク マップに追加し、結果メッセージを画面に表示するか、または、指定したファイルに結果をリダイレクトします。

ホスト入力クライアントの設定

Management Center のホスト入力サービスは、Management Center のユーザからホスト入力コマンドを受け入れるほかに、外部ホストの認証されたホスト入力クライアントからのバッチ インポート ファイルも受け入れます。ホスト入力クライアントを使用して、ホスト入力インポート ツールのために作成されたインポート ファイルを処理し、その後にデータを Management Center に送信してその情報をネットワーク マップに追加できます。

提供されているホスト入力 API の参照クライアントを使用して CSV データを処理して送信したり、Management Center へのホスト入力クライアント接続をテストすることができます。

Management Center と入力クライアントのインタラクションを管理するには、次のタスクを実行します。

1. Management Center への認証接続を確立します。

   Management Center への認証接続を確立するための認証クレデンシャル生成の詳細については、Management Center へのホスト入力クライアントの登録（3-1 ページ）を参照してください。

2. 参照を実行するコンピュータに参照クライアントをセットアップします。詳細については、ホスト入力参照クライアントの使用（3-2 ページ）を参照してください。

   参照クライアントを使用して処理するインポート ファイル（コマンド ファイルとも呼ぶ）の作成に関する詳細については、ホスト入力インポート ファイルの作成（2-3 ページ）を参照してください。

Management Center へのホスト入力クライアントの登録

ライセンス: すべて

ホスト入力クライアントを使用する前に、クライアントが動作するコンピュータを Management Center に登録する必要があります。Management Center はその後に認証証明書を生成し、ユーザは使用するクライアント コンピュータにそれをダウンロードします。

ホスト入力クライアントを追加する方法:

アクセス: Admin

1. システムでドメインが作成されていた場合は、ドメイン スイッチャで目的のドメインを選択します。グローバル ドメインまたは別の親ドメイン用に作成された証明書を使用するクライアントは、その範囲のすべてのリーフ ドメインに対する変更権限を持ちますが、インポート ファイルではいずれかのドメインを指定する必要があります。リーフ ドメイン用に作成された証明書を使用するクライアントは、そのリーフ ドメインに対する変更権限しか持ちません。

2. [System] > [Integration] > [Host Input Client] を選択します。

   [Host Input Client] ページが表示されます。

3. [Create Client] をクリックします。

   [Create Client] ページが表示されます。

4. [Hostname] フィールドに、ホスト入力クライアントを実行しているホストのホスト名または IP アドレスを入力します。

注：ホスト名を使用する場合、ホスト入力サーバはホストを IP アドレスに解決できる**必要**があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

5. 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。
6. [Save] をクリックします。

   ホスト入力サービスは、クライアント コンピュータから Management Center 上のポート 8307 へのアクセスを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [Host Input Clients] の下に表示された状態で、[Host Input Client] ページが再表示されます。
7. 証明書ファイルの横にあるダウンロード アイコン（  ）をクリックします。
8. SSL 認証のためにクライアント コンピュータが使用するディレクトリに証明書ファイルを保存します。

   これで、クライアントは Management Center に接続できるようになりました。

注：クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（  ）をクリックします。Management Center でホスト入力サービスを再起動する必要はありません。アクセスは直ちに取り消されます。

Management Center へのクライアントの接続

Management Center のホスト入力サービスは、クライアントの接続時にクライアントからバージョンを読み取ります。クライアントがサーバのバージョンよりも新しいバージョンを送信した場合、サービスは接続を拒否します。

また、最初の交換時に、ホスト入力サービスはトランザクションごとに許容される最大データ サイズを、クライアントへ伝えます。クライアントが最大サイズより大きいデータ ブロックを送信すると、サーバは接続を終了します。

ホスト入力参照クライアントの使用

ホスト入力 SDK に付属の参照クライアントは、ホスト入力 API の使用法を説明する一連のサンプル クライアント スクリプトと Perl モジュールです。これらを実行してホスト入力インポートに慣れることができます。また、カスタム クライアントのインストールに関する問題のデバッグにも使用できます。さらに、スクリプトの 1 つを使用して、クライアントからのホスト入力コマンド ファイルを処理できます。

参照クライアントのセットアップの詳細については、以降の各項を参照してください。

- ホスト入力参照クライアントのセットアップ（3-2 ページ）
- ホスト入力参照クライアントの実行（3-4 ページ）

ホスト入力参照クライアントのセットアップ

ホスト入力参照クライアントを使用するには、まずサンプル スクリプトをインストールし、スクリプトの要件に適合するようにクライアントを設定する必要があります。

詳細については、次の項を参照してください。

- ホスト入力参照クライアントについて（3-3 ページ）
- ホスト入力参照クライアントの通信の設定（3-3 ページ）

- ホスト入力参照クライアントの一般的な前提条件を読み込む（3-3 ページ）
- ホスト入力参照クライアントのダウンロードと展開（3-4 ページ）
- ホスト入力参照クライアントの証明書の作成（3-4 ページ）

ホスト入力参照クライアントについて

ホスト入力参照クライアントが含まれた `HostInputClientSDK.zip` パッケージを シスコサポート サイトからダウンロードできます。表 3-1 ホスト入力参照クライアントのファイル（3-3 ページ）に、`HostInputClientSDK.zip` パッケージに含まれるファイルの一覧を示します。

表 3-1　　ホスト入力参照クライアントのファイル

ファイル名	説明
SFHIClient.pm	この Perl モジュールには Perl クライアントが呼び出すコマンドが含まれています。
SFPkcs12.pm	この Perl モジュールはクライアント証明書を解析し、クライアントが Management Center に接続できるようにします。
sf_host_input_agent.pl	この Perl スクリプトを使用して、適切な入力プラグインおよびコマンド ファイルを指定して、CSV データをインポートできます。
InputPlugins/csv.pm	この Perl モジュールを呼び出して、CSV データをインポートするコマンド ファイルを実行できます。

ホスト入力参照クライアントの通信の設定

参照クライアントは、データ通信にセキュア ソケット レイヤ（SSL）プロトコルを使用します。クライアントとして使用する予定のコンピュータに OpenSSL をインストールし、環境に合わせて適切に設定する必要があります。

クライアントで SSL を設定するには、次の手順を実行します。

1. OpenSSL を `http://openssl.org/source/` からダウンロードします。
2. `/Usr/local/src` にソースを展開します。
3. Configure スクリプトを実行して、ソースを設定します。
4. コンパイル対象のソースに Make を実行し、インストールします。

ホスト入力参照クライアントの一般的な前提条件を読み込む

ホスト入力参照クライアントを実行する前に、クライアント コンピュータに `IO::Socket::SSL` Perl モジュールをインストールする必要があります。モジュールは手動でインストールすることも、`cpan` を使用してインストールすることもできます。

注：クライアント コンピュータに `Net::SSLeay` モジュールがインストールされていない場合は、そのモジュールも同様にインストールします。`Net::SSLeay` は OpenSSL の通信に必要です。

Management Center への SSL 接続をサポートするために、OpenSSL もインストールし、設定する必要があります。詳細については、ホスト入力参照クライアントの通信の設定（3-3 ページ）を参照してください。

また、ホスト入力クライアントで Qualys プラグインを使用する場合は、`XML::Smart` Perl モジュールおよびその前提条件をインストールする必要があります。クライアントと Management Center との間で IPv6 を使って通信する場合は、`IO::Socket::INET6` Perl モジュールもインストールする必要があります。

ホスト入力参照クライアントのダウンロードと展開

ホスト入力参照クライアントが含まれた `HostInputClientSDK.zip` ファイルをサポート サイトからダウンロードできます。

クライアントを実行する予定の Linux オペレーティング システムを実行しているコンピュータで zip ファイルを展開します。

ホスト入力参照クライアントの証明書の作成

ライセンス: すべて

ホスト入力参照クライアントを使用する前に、Management Center へのホスト入力クライアントの登録（3-1 ページ）の説明に従って、クライアント証明書を作成する必要があります。参照クライアントを置くディレクトリに、その証明書ファイルを保存します。

参照クライアントの証明書を作成するには次の手順を実行します。

アクセス: Admin

1. Management Center へのホスト入力クライアントの登録（3-1 ページ）の説明に従ってクライアントを作成します。
2. 参照クライアントを置くディレクトリにその証明書ファイルを保存します。

ホスト入力参照クライアントの実行

ホスト入力 Perl 参照クライアント スクリプトは Linux カーネルを持つオペレーティング システムで使用するよう設計されていますが、クライアント マシンがホスト入力参照クライアントのセットアップ（3-2 ページ）で定義されている前提条件を満たしていれば、任意の POSIX ベースのオペレーティング システムでも機能します。

参照クライアントを使用して、リモート クライアントから Management Center のネットワーク マップに CSV データをインポートできます。

次の構文を使用して `sf_host_input_agent.pl` スクリプトを実行します。

```
./sf_host_input_agent.pl -server=ManagementCenterIPAddress -level=DebugLevel
-logfile=LogFile -pluginfo=CSVCommandFile.csv
```

たとえば、`csv_file.txt` という名前の CSV ファイルを使用して IP アドレスが 10.10.0.4 で、HostInput.log ログ ファイルへのデバッグ ロギングを実行する Management Center にインポートするには、次のスクリプトを実行します。

```
./sf_host_input_agent.pl -server=10.10.0.4 -level=3 -logfile=HostInput.log
-pluginfo=cvs_file.txt csv
```

ネットワーク プロトコル値

`AddProtocol` および `DeleteProtocol` コマンドを使用して、ホストへのプロトコルの追加、またはホストからのプロトコルの削除ができます。次の表に、利用可能なネットワーク プロトコル値を示します。

表 A-1　　ネットワーク プロトコル値

値	説明
IP	インターネット プロトコル バージョン 4
ARP	アドレス解決プロトコル
BPDU（STP）	ブリッジ プロトコル データ ユニット（スパニング ツリー プロトコル）
RARP	Reverse Address Resolution Protocol
OldIPX	Internetwork Packet Exchange、旧バージョン
IP Version 6	インターネット プロトコル バージョン 6
Loopback	ループバック
SNAP	Subnetwork Access Protocol
Novell NetWare	Novell NetWare
NetBIOS	Network Basic Input/Output System
NetBIOS (Response)	Network Basic Input/Output System の応答
IPX	Internetwork Packet Exchange
Intel ANS	Intel Advanced Network Services
DEC MOP Dump/Load Assistance	Digital Equipment Corporation メンテナンス オペレーション プロトコル ダンプ/ロード補助
DEC MOP Remote Console	Digital Equipment Corporation メンテナンス オペレーション プロトコル リモート コンソール
PPPoE Discovery	PPPoE ディスカバリ ステージ
PPPoE Session	PPPoE セッション ステージ