



## コンプライアンス ホワイトリスト

次のトピックでは、関連ポリシーに追加する前にコンプライアンス ホワイトリストを設定する方法について説明します。

- [コンプライアンス ホワイトリストの概要, 1 ページ](#)
- [コンプライアンス ホワイト リストの作成, 7 ページ](#)
- [コンプライアンス ホワイト リストの管理, 15 ページ](#)
- [共有ホスト プロファイルの管理, 18 ページ](#)

## コンプライアンス ホワイトリストの概要

コンプライアンス ホワイトリスト（ホワイトリストと省略されることもある）は、どのオペレーティングシステム、アプリケーション（Web とクライアント）、およびプロトコルがネットワーク上のホストで許可されるかを指定する一連の条件です。システムはホストがホワイトリストに違反するとイベントを生成します。

コンプライアンス ホワイトリストには2つの主要な構成要素があります。

- ターゲットは、ホワイトリスト評価の対象として選択するホストです。サブネット、VLAN、およびホスト属性で制約して、全部または一部のモニタ対象ホストを評価できます。マルチドメイン展開では、ドメインと、ドメイン内またはドメインをまたいだサブネットを対象にすることができます。
- ホスト プロファイルは、ターゲットのコンプライアンス基準を指定します。グローバル ホスト プロファイルはオペレーティングシステムに依存しません。1つのホワイトリスト固有として、またはホワイトリスト間で共有される、オペレーティング システム固有のホスト プロファイルを設定することもできます。

Cisco Talos Security Intelligence and Research Group (Talos) は、推奨設定が指定されたデフォルトのホワイトリストを提供しています。カスタム ホワイトリストを作成することも可能です。単純なカスタム ホワイトリストでは、特定のオペレーティングシステムを実行するホストのみを許可できます。より複雑なホワイトリストでは、すべてのオペレーティングシステムを許可すると

もに、特定のポートで特定のアプリケーションプロトコルを実行する際にホストが使用する必要のあるオペレーティング システムを指定できます。



(注) システムは、ホストをエクスポートされた NetFlow レコードからネットワーク マップに追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い](#)を参照)。この制限は、コンプライアンス ホワイトリストの作成方法に影響する場合があります。

### コンプライアンス ホワイトリストの実装

ホワイトリストを実装するには、アクティブな関連ポリシーにホワイトリストを追加します。システムはターゲットを評価し、対応する属性を各ホストに割り当てます。

- 準拠 (Compliant) : ホストはホワイトリストに違反していません。
- 非準拠 (Non-Compliant) : ホストはホワイトリストに違反しています。
- 評価されていない (Not Evaluated) : ホストがホワイトリストのターゲットではないか、現在評価中であるか、またはシステムに十分な情報がないためホストが準拠しているかどうかを判断できません。



(注) ホスト属性を削除するには、対応するホワイトリストを削除します。1つのホワイトリストを非アクティブ化、削除、または関連ポリシーから削除しても、各ホストのホスト属性は削除されず、属性の値が変更されることもありません。

最初の評価後、モニタ対象ホストがアクティブなホワイトリストに違反するたびにホワイトリスト イベントが生成されます。また、ホワイトリスト違反が記録されます。

ワークフロー、ダッシュボード、およびネットワーク マップを使用して、システム全体のコンプライアンス アクティビティをモニタし、個々のホストがホワイトリストにいつどのように違反したのかを判断できます。修復およびアラートでホワイトリスト違反に自動的に応答することもできます。

#### 例 : Web サーバへの HTTP の制限

セキュリティ ポリシーは、Web サーバのみが HTTP を実行できることを指定しています。HTTP を実行しているホストを特定するために Web ファーム以外のネットワーク全体を評価するホワイトリストを作成します。

ネットワーク マップとダッシュボードを使用して、ネットワークのコンプライアンスの概要を一目で把握できます。数秒で、ポリシーに違反して HTTP を実行している組織内のホストを正確に特定して適切に対処できます。

その後で、関連機能を使用して、Web ファーム内に存在しないホストが HTTP の実行を開始するたびに警告するようにシステムを設定できます。

## コンプライアンス ホワイトリストのターゲット ネットワーク

ターゲットネットワークは、ホワイトリストコンプライアンス評価の対象となるホストを指定します。ホワイトリストには、複数のターゲット ネットワークを含めることができ、いずれかのターゲットの基準を満たすホストが評価されます。

最初は、ターゲットネットワークはIPアドレスまたはアドレス範囲で制約されています。マルチドメイン展開では、初期の制約にドメインも含まれます。

システム提供のデフォルトのホワイトリストでは、すべての監視対象ホスト `0.0.0.0/0` および `::/0` がターゲット設定されています。マルチドメイン展開では、デフォルトのホワイトリストはグローバルドメインに制約されています（グローバルドメインでのみ使用可能です）。

ホストがホワイトリストに対して有効ではなくなるようにターゲット ネットワークまたはホストを変更すると、ホストはホワイトリストで評価されなくなり、準拠と非準拠のいずれとしてもみなされなくなります。

### ターゲット ネットワークの調査と改善

ホワイトリストにターゲット ネットワークを追加すると、システムにより、準拠ホストの特徴を確認できるようにネットワーク マップを調査するよう求められます。調査により、ターゲットは、調査済みのホストを表すホワイトリストに追加されます。

サブネットまたは個別のホストを調査できます。マルチドメイン展開では、ドメイン全体を調査することも、ドメインをまたいで調査することもできます。先祖ドメインを調査すると、システムによってこのドメインの子孫が調査されます。

追加されたターゲットに加えて、調査では、調査で検出されたオペレーティングシステムごとに1つのホストプロファイルがホワイトリストに入力されます。デフォルトで、これらのホストプロファイルは、システムが該当するオペレーティングシステム上で検出したクライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

ターゲット ネットワークを調査（または調査をスキップ）した後、対象を絞り込みます。IPアドレスを使用してホストを除外するか、ホスト属性またはVLANによりターゲット ネットワークを制約します。

### コンプライアンス ホワイトリストを使用したドメインの対象化

マルチドメイン展開では、ドメインとターゲット ネットワークは密接にリンクされています。

- リーフドメインの管理者は、自分のリーフドメイン内のホストを評価するホワイトリストを作成できます。
- 上位ドメインの管理者は、ドメインをまたいでホストを評価するホワイトリストを作成できます。同じホワイトリストで、ドメインの異なるさまざまなサブネットを対象にすることができます。

グローバルドメインの管理者であり、展開全体のWebサーバに同じコンプライアンス基準を導入する必要があるというシナリオを考えてみます。コンプライアンス基準を定義するグローバルドメインに1つのホワイトリストを作成できます。次に、各リーフドメイン内のWebサーバのIP

スペース（または個別のIPアドレス）を指定するターゲットネットワークを使用して、ホワイトリストを制約します。



- (注) リーフ ドメインの IP アドレスと範囲を対象にすることに加えて、上位のドメインを使用してターゲット ネットワークを制約することもできます。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。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。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

## コンプライアンス ホワイト リストのホスト プロファイル

コンプライアンス ホワイト リストにおいて、ホスト プロファイルは、ターゲット ホスト上で実行を許可するオペレーティングシステム、クライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルを指定します。コンプライアンス ホワイト リストで使用できるホスト プロファイルは3種類あります。3種類のホスト プロファイルはそれぞれ、エディタ上での表示が異なります。

表 1: コンプライアンス ホワイト リストのホスト プロファイル タイプ

ホスト プロファイル タイプ	表示	説明
グローバル	すべてのオペレーティングシステム	オペレーティングシステムに関係なく、ターゲット ホスト上で実行が許可されている内容を指定します。
オペレーティングシステム別	プレーン テキストで表示	特定のオペレーティングシステムを使用するターゲット ホスト上で実行が許可されている内容を指定します。
共有	イタリックで表示	複数のホワイトリストで使用可能なオペレーティングシステム条件を指定します。

### オペレーティング システム固有のホスト プロファイル

コンプライアンス ホワイト リストでは、オペレーティング システム固有のホスト プロファイルで、ネットワーク上での実行を許可するオペレーティング システムだけでなく、それらのオペレーティング システム上での実行を許可するアプリケーションプロトコル、クライアント、Web アプリケーション、およびプロトコルも指定します。

たとえば、準拠ホストではMicrosoft Windows の特定のバージョンを実行することを要件にすることができます。別の例として、SSH の実行を Linux ホストのポート 22 で許可した上で、SSH クライアントのベンダーとバージョンをさらに制限することもできます。

ネットワーク上での実行を許可するオペレーティングシステムごとに1つのホストプロファイルを作成します。ネットワーク上でオペレーティングシステムを禁止する場合は、そのオペレーティングシステム用のホストプロファイルを作成しないでください。たとえば、ネットワーク上のすべてのホストでWindows が実行されるようにするには、そのオペレーティングシステム用のホストプロファイルのみを含めるようにホワイトリストを設定します。



- (注) 未確認ホストは、確認されるまで、すべてのホワイトリストに準拠していると見なされます。ただし、不明ホストのホワイトリストホストプロファイルを作成することはできません。未確認ホストとは、オペレーティングシステムを識別するために十分な情報が収集されていないホストのことです。不明ホストとは、既知のフィンガープリントと一致しないオペレーティングシステムを使用しているホストのことです。

## 共有ホスト プロファイル

コンプライアンス ホワイトリストでは、共有ホストプロファイルが特定のオペレーティングシステムに関連付けられますが、それぞれの共有ホストプロファイルを複数のホワイトリスト内で使用できます。

たとえば、世界中にオフィスがあり、拠点ごとに別々のホワイトリストを使用する一方、Apple Mac OS X を実行しているすべてのホストに対しては常に同じプロファイルを使用するとします。その場合、該当するオペレーティングシステム用の共有プロファイルを作成し、そのプロファイルをすべてのホワイトリストで使用するという方法があります。

デフォルトホワイトリストでは、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルが使用されます。これらのプロファイルは、組み込みのアプリケーションプロトコル、Web アプリケーション、プロトコル、クライアントを使用します。コンプライアンス ホワイトリストエディタでは、システムはこれらのプロファイルを組み込みホストプロファイルアイコン (📁) で示します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。このプロファイルは編集できます。また、先祖ドメインからの共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。



- (注) 共有ホストプロファイル (組み込みを含む) を変更した場合や、組み込みアプリケーションプロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイトリストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

## ホワイトリスト違反のトリガー

ホストのホワイトリストコンプライアンスは、システムで次のことが発生すると変化する場合があります。

- ホストのオペレーティング システムの変更を検出
- ホストのオペレーティング システムまたはホスト上のアプリケーション プロトコルに関するアイデンティティの競合を検出
- ホスト上でアクティブになっている新しい TCP サーバ ポート（SMTP または Web サーバによって使用されるポートなど）、または、ホスト上で実行中の新しい UDP サーバを検出
- ホスト上で実行中の検出された TCP サーバまたは UDP サーバで、アップグレードのためのバージョン変更などの変更を検出
- ホスト上で実行中の新しいクライアント アプリケーションまたは Web アプリケーションを検出
- クライアント アプリケーションまたは Web アプリケーションを非アクティブを理由にそのデータベースからドロップ
- ホストが新しいネットワークまたはトランスポート プロトコルと通信していることを検出
- 新しいジェイルブレイクされたモバイル デバイスを検出
- ホスト上で TCP ポートまたは UDP ポートが閉じられたか、タイムアウトしたことを検出

さらに、ホスト入力機能またはホスト プロファイルを使用して次の操作を実行することによって、ホストのコンプライアンスの変化をトリガーできます。

- ホストにクライアント、プロトコル、またはサーバを追加する
- ホストからクライアント、プロトコル、またはサーバを削除する
- ホストにオペレーティング システム定義を設定する
- ホストが有効なターゲットでなくなるようにホストのホスト属性を変更する



(注) 非常に多数のイベントが発生しないように、システムでは、その最初の評価に基づいて非標準のホストにホワイトリスト イベントを生成せず、またユーザがアクティブなホワイトリストまたは共有ホスト プロファイルを変更した結果としてホストを非標準にしません。ただし、違反は記録されます。すべての非標準ターゲットに対してホワイトリスト イベントを生成する場合は、検出データを消去してください。ネットワーク アセットを再検出すると、ホワイトリスト イベントをトリガーすることがあります。

### 例：オペレーティング システムのコンプライアンス

ホワイトリストで Microsoft Windows ホストのみがネットワーク上で許可されるように指定されている場合、システムでは、Mac OS X を実行中のホストを検出するとホワイトリスト イベントを生成します。さらに、ホワイトリストに関連付けられているホスト属性が、そのホストに関して [準拠 (Compliant)] から [非準拠 (Non-Compliant)] に変更されます。

この例のホストが [準拠 (Compliant)] に復帰するには、次のいずれかが行われる必要があります。

- Mac OS X オペレーティング システムを許可するようにホワイト リストを編集する
- ホストのオペレーティング システム定義を手動で Microsoft Windows に変更する
- オペレーティング システムが変更されて Microsoft Windows に戻ったことをシステムが検出する

### 例：非準拠のアセットをネットワーク マップから削除する

ホワイトリストで FTP の使用が許可されていない場合に、アプリケーション プロトコルのネットワーク マップ、またはイベント ビューから FTP を削除すると、FTP を実行中のホストは準拠になります。ただし、システムがこのアプリケーション プロトコルを再度検出すると、システムによってホワイトリスト イベントが生成され、そのホストは非準拠になります。

### 例：完全な情報に基づいてのみトリガーを実行

ホワイトリストでポート 21 で TCP FTP トラフィックだけを許可していた場合、システムでポート 21/TCP で不明なアクティビティを検出すると、ホワイト リストはトリガーを実行しません。ホワイトリストがトリガーを実行するのは、システムがトラフィックを FTP 以外のトラフィックとして識別するか、またはユーザがホスト入力機能を使用してトラフィックを非 FTP トラフィックとして指定した場合だけです。システムは、部分的な情報のみを使用して違反を記録することはありません。

## コンプライアンス ホワイト リストの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリストを作成する際には、ネットワークを調べて最初のターゲットを作成するよう求めるプロンプトが表示されます。これは、コンプライアンスに準拠するホストの特徴を指定するのに役立ちます。

## 手順

- ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択し、[ホワイトリスト (White List)] タブをクリックします。
- ステップ 2** [新規ホワイトリスト (New White List)] をクリックします。
- ステップ 3** 必要に応じて、最初のターゲット ネットワークの [IP アドレス (IP Address)] および [ネットマスク (Netmask)] を入力します。マルチドメイン導入では、ターゲット ネットワークが存在する [ドメイン (Domain)] を選択します。
- ヒント** モニタリング対象のネットワーク全体を調査するには、デフォルト値の 0.0.0.0/0 と ::/0 を使用します。
- (注) ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。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。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。
- ステップ 4** ターゲット ネットワークを追加します。
- [追加 (Add)] : 調査せずにターゲット ネットワークを追加する場合は、[追加 (Add)] をクリックします。
  - [ネットワークの追加および調査 (Add and Survey Network)] : ターゲット ネットワークを追加して調査する場合は、[ネットワークの追加および調査 (Add and Survey Network)] をクリックします。
  - [スキップ (Skip)] : ネットワークを調査せずにホワイトリストを作成する場合は、[スキップ (Skip)] をクリックします。
- ステップ 5** 必要に応じて、ホワイトリストの新しい [名前 (Name)] および [説明 (Description)] を入力します。
- ステップ 6** 必要に応じて、[脱獄モバイル デバイスを許可 (Allow Jailbroken Mobile Devices)] を選択して、ネットワークで脱獄モバイル デバイスを許可します。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
- ステップ 7** [コンプライアンス ホワイトリストのターゲット ネットワークの設定](#)、(9 ページ) の説明に従って、1 つ以上の [ターゲット ネットワーク (Target Network)] をホワイトリストに追加します。
- ステップ 8** [許可されるホスト プロファイル (Allowed Host Profiles)] を使用して、準拠ホストの特徴を指定します。
- グローバル ホスト プロファイル : ホワイトリストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム (Any Operating System)] をクリックし、[ホワイトリスト ホスト プロファイルの作成](#)、(10 ページ) の説明に従います。
  - 調査済みプロファイルの編集 : ネットワーク調査によって作成された既存のオペレーティング システム固有のホスト プロファイルを編集するには、その名前をクリックし、[ホワイトリスト ホスト プロファイルの作成](#)、(10 ページ) の説明に従います。

- 新規プロファイルの作成：このホワイトリストに新しいオペレーティングシステム固有のホストプロファイルを作成するには、[許可されるホストプロファイル (Allowed Host Profiles)] の隣にある追加アイコン (+) をクリックし、[ホワイトリストホストプロファイルの作成](#)、(10 ページ) の説明に従います。
- 共有ホストプロファイルの追加：ホワイトリストに既存の共有ホストプロファイルを追加するには、[共有ホストプロファイルの追加 (Add Shared Host Profile)] をクリックし、追加する共有ホストプロファイルを選択して、[OK] をクリックします。共有ホストプロファイルは斜体で表示されます。

**ステップ 9** [ホワイトリストの保存 (Save White List)] をクリックします。

**次の作業**

- [関連ポリシーの設定](#)の説明に従って、アクティブな関連ポリシーにホワイトリストを追加します。システムはすぐにホワイトリストの評価および違反の生成を開始します。

## コンプライアンス ホワイトリストのターゲットネットワークの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ターゲットネットワークを追加するときには、ターゲットネットワークを調査して、準拠しているホストを特定することができます。この調査によって、調査で検出された各オペレーティングシステムの1つのホストプロファイルがホワイトリストに追加されます。これらのホストプロファイルは、システムが該当するオペレーティングシステム上で検出したクライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルのすべてを許可します。

**手順**

- ステップ 1** コンプライアンス ホワイトリスト エディタで、[ターゲットネットワークの追加 (Add Target Network)] をクリックします。
- ステップ 2** ターゲットネットワークの [IP アドレス (IP Address)] と [ネットマスク (Netmask)] を入力します。
- ステップ 3** マルチドメイン展開では、ターゲットネットワークが存在する [ドメイン (Domain)] を選択します。

- (注) ターゲット ネットワークのドメインを選択した後は、ドメインを変更できません。より高いレベルのドメインのサブネットをターゲットにすると、各子孫リーフ ドメイン内の同じサブネットがターゲットになります。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。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

**ステップ 4** ターゲット ネットワークを追加します。

- 追加 (Add) : 調査なしでターゲット ネットワークを追加するには、[追加 (Add)] をクリックします。
- ネットワークの追加と調査 (Add and Survey Network) : ターゲット ネットワークを追加および調査するには、[ネットワークの追加と調査 (Add and Survey Network)] をクリックします。

**ステップ 5** 必要に応じて、新しいターゲットをクリックしてさらに構成します。

- 名前 (Name) : 新しい [名前 (Name)] を入力します。
- ネットワークの追加 (Add Networks) : 追加のホストをターゲットにするには、追加アイコン (+) をクリックして、[IP アドレス (IP Address)] と [ネットマスク (Netmask)] を入力します。ネットワークをホワイト リスト コンプライアンスから除外するには、[除外 (Exclude)] を選択します。
- ホスト属性の追加 (Add Host Attributes) : 特定のホスト属性を持つホストをターゲットにするには、追加アイコン (+) をクリックして、[属性 (Attribute)] とその [値 (Value)] を指定します。
- VLAN の追加 (Add VLANs) : VLAN をターゲットにするには、追加アイコン (+) をクリックして VLAN 番号を入力します (802.1q VLAN の場合)。
- 削除 (Delete) : ターゲット制限を削除するには、削除アイコン (🗑️) をクリックします。

**ステップ 6** 最後に保存した後で行ったすべての変更をすぐに実装するには、[ホワイト リストの保存 (Save White List)] をクリックします。

## ホワイト リスト ホスト プロファイルの作成

スマートライセン ス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホストプロファイルは、ターゲット ホスト上での実行を許可するオペレーティング システム、クライアント、アプリケーションプロトコル、Web アプリケーション、およびプロトコルといった、ホワイトリストの適合基準を指定します。

すべてのホワイト リストには、オペレーティング システムに依存しないグローバル ホストプロファイルがあります。たとえば、Mozilla Firefox を許可するように複数の Microsoft Windows ホストプロファイルと Linux ホストプロファイルを編集する代わりに、検出されたオペレーティング システムに関係なく、Firefox を許可するようにグローバルホストプロファイルを設定できます。

また、各オペレーティングシステム専用のホストプロファイルを設定できます。これは、単一のホワイトリスト専用としても、複数のホワイトリストの共有プロファイルとしても設定できます。



- (注) 共有ホストプロファイル（ビルトインを含む）を変更した場合、またはビルトインアプリケーションプロトコル、プロトコル、クライアントを変更した場合、これらのプロファイルを使用するすべてのホワイトリストに影響します。これらのビルトイン要素に意図しない変更や削除を行った場合は、出荷時のデフォルトにリセットできます。

## はじめる前に

- [コンプライアンス ホワイトリストの編集](#)、(16 ページ) の説明に従い、ホワイトリスト内でホストプロファイルを作成または編集します。または、[共有ホストプロファイルの管理](#)、(18 ページ) の説明に従い、共有ホストプロファイルを作成または編集します。

## 手順

**ステップ 1** ホワイトリスト適合ホストプロファイルエディタで、以下のホストプロファイルを設定します。

- 名前：[名前 (Name) ]を入力します。
- オペレーティング システム：ホスト プロファイルを特定のオペレーティング システム専用にするには、[OS ベンダ (OS Vendor) ]、[OS 名 (OS Name) ]、[バージョン (Version) ] ドロップダウンリストを使用します。グローバルホストプロファイルはすべてのオペレーティングシステムを実行するホストへ適用されることを目的としたプロファイルであるため、これに制限を設定することはできません。
- アプリケーションプロトコル：アプリケーション プロトコルを許可するには、追加アイコン (+) をクリックし、[アプリケーションプロトコルのホワイトリスト](#)、(12 ページ) の説明に従います。
- クライアント：クライアントを許可するには、追加アイコン (+) をクリックし、[クライアントのホワイトリスト](#)、(13 ページ) の説明に従います。
- Web アプリケーション：Web アプリケーションを許可するには、追加アイコン (+) をクリックし、[Web アプリケーションのホワイトリスト](#)、(14 ページ) の説明に従います。
- プロトコル：プロトコルを許可するには、追加アイコン (+) をクリックし、[プロトコルのホワイトリスト](#)、(14 ページ) の説明に従います。

- 削除：一度許可した項目への許可を解除するには、削除アイコン (🗑️) をクリックします。
- プロパティの編集：許可されているアプリケーションプロトコルのプロパティ、クライアント、プロトコルを編集するには、その名前をクリックします。変更は、変更した要素を使用する各ホストプロファイルに反映されます。

**ヒント** プロファイルに一致するホストにすべてのアプリケーションプロトコル、クライアント、webアプリケーションを許可するには、該当する[すべて許可 (Allow all...)] チェックボックスを選択します。

**ステップ 2** 最後の保存以降に施した変更をすぐに適用するには、[ホワイトリストを保存 (Save White List)] (または、共有ホストプロファイルを編集している場合は[すべてのプロファイルを保存 (Save All Profiles)] ) をクリックします。

## アプリケーション プロトコルのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、アプリケーションプロトコルのホワイトリストを作成できます。オプションで、ポート、ベンダー、バージョンによって、アプリケーションプロトコルを制限できます。たとえば、ポート 22/TCP で、Linux ホスト上で実行する OpenSSH の特定のバージョンを許可することができます。

### 手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるアプリケーションプロトコル (Allowed Application Protocols)] (またはグローバルホストプロファイルを変更している場合は[グローバルに許可されるアプリケーションプロトコル (Globally Allowed Application Protocols)] ) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 次の 2 つの対処法があります。

- 許可するアプリケーションプロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたアプリケーションプロトコル、または今許可しようとしているアプリケーションプロトコルが表示されます。
- リストにないアプリケーションプロトコルを許可するには、[<新規アプリケーションプロトコル> (<New Application Protocol>)] を選択し、[OK] をクリックしてアプリケーションプロトコルエディタを表示します。許可するアプリケーションプロトコル[タイプ (Type)] と [プロトコル (Protocol)] を選択します。オプションで、[ポート (port)]、[ベンダー

(Vendor) ]、[バージョン (Version) ]によって、アプリケーションプロトコルを制限します。

(注) アプリケーションのテーブルビューに表示されているとおり正確にベンダーやバージョンを入力する必要があります。ベンダーまたはバージョンを指定しなかった場合は、タイプとプロトコルが一致している限り、ホワイトリストではすべてのベンダーとバージョンが許可されます。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List) ] をクリックします。

## クライアントのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、クライアントのホワイトリストを作成できます。オプションで、クライアントを特定のバージョンに限定することができます。たとえば、Microsoft Windows ホスト上での実行を Microsoft Internet Explorer 10 のみに許可することができます。

### 手順

**ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるクライアント (Allowed Clients) ] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるクライアント (Globally Allowed Clients) ]) の横にある追加アイコン (+) をクリックします。

**ステップ 2** 次の 2 つの対処法があります。

- 許可するクライアントが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたクライアント、または今許可しようとしているクライアントが表示されます。
- リストにないクライアントを許可するには、[<新規クライアント> (<New Client>)] を選択し、[OK] をクリックしてクライアント エディタを表示します。ドロップダウンリストから許可する [クライアント (Client) ] を選択し、オプションで許可するクライアントの [バージョン (Version) ] を制限します。

- (注) クライアントのテーブル ビューに表示されているとおり正確にバージョンを入力する必要があります。バージョンを指定しない場合、ホワイトリストはすべてのバージョンを許可します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List) ] をクリックします。

## Web アプリケーションのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、Web アプリケーションのホワイトリストを作成できます。

### 手順

- ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可される Web アプリケーション (Allowed Web Applications) ] (またはグローバル ホスト プロファイルを変更している場合は[グローバルに許可される Web アプリケーション (Globally Allowed Web Applications) ]) の横にある追加アイコン (⊕) をクリックします。
- ステップ 2** 許可する Web アプリケーションを選択します。
- ステップ 3** [OK] をクリックして、
- ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List) ] をクリックします。

## プロトコルのホワイトリスト

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

ホワイトリスト ホスト プロファイルを使用して、グローバルにまたは特定のオペレーティングシステムに対して、プロトコルのホワイトリストを作成できます。ARP、IP、TCP、UDP は、常にすべてのホスト上での実行が許可されます。これらを禁止することはできません。

手順

- ステップ 1** ホワイトリスト ホスト プロファイルを作成または変更しているときに、[許可されるプロトコル (Allowed Protocols)] (またはグローバル ホスト プロファイルを変更している場合は [グローバルに許可されるプロトコル (Globally Allowed Protocols)] ) の横にある追加アイコン (➕) をクリックします。
- ステップ 2** 次の 2 つの対処法があります。
- 許可するプロトコルが表示されたら、これらを選択します。Web インターフェイスには、ホワイトリストによって、過去に許可されたプロトコル、または今許可しようとしているプロトコルが表示されます。
  - リストにないプロトコルを許可するには、[<新規プロトコル> (<New Protocol>)] を選択し、[OK] をクリックしてプロトコル エディタを表示します。[タイプ (Type)] ドロップダウンリストから、プロトコル タイプ ([ネットワーク (Network)] や [トランスポート (Transport)] ) を選択し、ドロップダウンリストから [プロトコル (Protocol)] を選択します。
- ヒント** リスト内に存在しないプロトコルを指定するには、[その他(手動入力) (Other(manual entry))] を選択します。ネットワーク プロトコルの場合は、<http://www.iana.org/assignments/ethernet-numbers/> に記載されている適切な番号を入力します。トランスポート プロトコルの場合は、<http://www.iana.org/assignments/protocol-numbers/> に記載されている適切な番号を入力します。
- ステップ 3** [OK] をクリックします。
- ステップ 4** 最後に保存した後に加えられたすべての変更をすぐに実施するには、[ホワイトリストの保存 (Save White List)] をクリックします。

## コンプライアンス ホワイト リストの管理

スマートライセン ス	従来のライセンス	サポートされるデ バイス	サポートされるド メイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

[ホワイト リスト (White List)] ページは、コンプライアンス ホワイトリストと共有ホストプロファイルの管理に使用できます。デフォルトホワイトリストは、推奨設定を表すものであり、組み込みホストプロファイルと呼ばれる特殊なカテゴリの共有ホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成されたコンプライアンスホワイトリストが表示されます。これは、編集が可能なリストです。また、先祖ドメインからの選択したホワイトリストも表示されますが、これは編集できません。下位のドメインで作成されたホワイトリストを表示および編集するには、そのドメインに切り替えます。



- (注) 設定に無関係なドメイン（名前、管理対象デバイスなど）に関する情報が公開されている場合、システムは先祖ドメインからの設定を表示しません。デフォルトホワイトリストは、グローバルドメインでのみ使用できます。

## 手順

- ステップ1** [ポリシー (Policies)] > [相関 (Correlation)] を選択して、[ホワイトリスト (White List)] タブをクリックします。
- ステップ2** コンプライアンス ホワイトリストを管理します。
- 作成：新しいホワイトリストを作成するには、[新規ホワイトリスト (New White List)] をクリックして、[コンプライアンス ホワイトリストの作成, \(7 ページ\)](#) で説明する手順を実行します。
  - 削除：使用していないホワイトリストを削除するには、削除アイコン (🗑️) をクリックして、ホワイトリストの削除を確認します。また、ホワイトリストを削除すると、ネットワーク上のすべてのホストから、そのリストに関連付けられたホスト属性も削除されます。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
  - 編集：既存のホワイトリストを変更するには、編集アイコン (✏️) をクリックし、[コンプライアンス ホワイトリストの編集, \(16 ページ\)](#) で説明する手順を実行します。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
  - 共有ホストプロファイル：ホワイトリストの共有ホストプロファイルを管理するには、[共有プロファイルの編集 (Edit Shared Profiles)] をクリックして、[共有ホストプロファイルの管理, \(18 ページ\)](#) で説明する手順を実行します。

## コンプライアンス ホワイトリストの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

アクティブな関連ポリシーに含まれるコンプライアンス ホワイトリストを修正して保存すると、システムは、ホワイトリストのターゲットネットワークのホストのコンプライアンスを再評価します。この再評価で一部のホストがコンプライアンス準拠または違反とされた場合でも、ホワイトリスト イベントは生成されません。

## 手順

- ステップ 1** [ポリシー (Policies)] > [関連 (Correlation)] を選択し、[ホワイトリスト (White List)] タブをクリックします。
- ステップ 2** 変更するホワイトリストの横にある編集アイコン (✎) をクリックします。  
代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** コンプライアンス ホワイト リストを編集します。
- 名前と説明：名前または説明を変更するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、新しい情報を入力します。
  - ジェイルブレイクされたデバイスの許可：ネットワーク上でジェイルブレイクされたモバイルデバイスを許可するには、左側のパネルでホワイトリストの名前をクリックしてホワイトリストの基本情報を表示し、[ジェイルブレイクされたモバイル デバイスを許可 (Allow Jailbroken Mobile Devices)] を有効にします。このオプションを無効にすると、ジェイルブレイクされたデバイスによってホワイトリスト違反が生成されます。
  - 許可されるホスト プロファイルの追加：このホワイトリストに対してオペレーティングシステム固有のホスト プロファイルを作成するには、[許可されているホスト プロファイル (Allowed Host Profiles)] の横にある追加アイコン (+) をクリックし、[ホワイト リスト ホスト プロファイルの作成, \(10 ページ\)](#) の説明に従って続行します。
  - 共有ホスト プロファイルの追加：ホワイトリストに既存の共有ホスト プロファイルを追加するには、[共有ホスト プロファイルの追加 (Add Shared Host Profile)] をクリックし、追加する共有ホスト プロファイルを選択して [OK] をクリックします。共有ホスト プロファイルは斜体で表示されます。
  - ターゲット ネットワークの追加：ホストを調査することなく新しいターゲット ネットワークを追加するには、ターゲット ネットワークの横にある追加アイコン (+) をクリックし、[コンプライアンス ホワイト リストのターゲット ネットワークの設定, \(9 ページ\)](#) の説明に従って続行します。
  - ホスト プロファイルの削除：ホワイトリストから共有またはオペレーティング システム固有のホスト プロファイルを削除するには、ホスト プロファイルの横にある削除アイコン (🗑️) をクリックし、選択内容を確認します。共有ホスト プロファイルを削除すると、それがホワイトリストから除外されますが、プロファイルは削除されず、それを使用する他のホワイトリストからも除外されません。ホワイトリストのグローバル ホスト プロファイルは削除できません。

- ターゲット ネットワークの削除：ホワイトリストからターゲット ネットワークを削除するには、ネットワークの横にある削除アイコン (🗑️) をクリックし、選択内容を確認します。
- グローバル ホスト プロファイルの編集：ホワイトリストのグローバル ホスト プロファイルを編集するには、[任意のオペレーティング システム (Any Operating System)] をクリックし、[ホワイトリストホストプロファイルの作成, \(10 ページ\)](#) の説明に従って続行します。
- 他のホスト プロファイルの編集：共有またはオペレーティング システム固有のホスト プロファイルを編集するには、ホスト プロファイルの名前をクリックし、[ホワイトリストホストプロファイルの作成, \(10 ページ\)](#) の説明に従って続行します。
- ターゲット ネットワークの編集：ターゲット ネットワークを編集するには、ネットワークの名前をクリックし、[コンプライアンス ホワイトリストのターゲット ネットワークの設定, \(9 ページ\)](#) の指示に従って続行します。

**ステップ 4** 前回の保存以降に行ったすべての変更をすぐに実装するには、[ホワイトリストの保存 (Save White List)] をクリックします。

## 共有ホスト プロファイルの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

コンプライアンス ホワイトリストでは、共有ホストプロファイルは特定のオペレーティング システムに関連付けられますが、それぞれの共有ホストプロファイルを複数のホワイトリスト内で使用できます。複数のホワイトリストを作成するが、同じホストプロファイルを使用して複数のホワイトリストで特定のオペレーティングシステムを実行するホストを評価する場合は、共有のホストプロファイルを使用します。

マルチドメイン展開では、現在のドメインで作成された共有ホストプロファイルが表示されます。これは、編集が可能なプロファイルです。また、先祖ドメインからの共有ホストプロファイルも表示されますが、これは編集できません。下位のドメインで作成された共有ホストプロファイルを表示および編集するには、そのドメインに切り替えます。



(注) 共有ホストプロファイル (組み込みを含む) を変更した場合や、組み込みアプリケーションプロトコル、プロトコル、またはクライアントを変更した場合、それを使用するすべてのホワイトリストに変更が影響します。意図しない変更を加えた場合や、該当する組み込みの要素を削除した場合は、工場出荷時の初期状態にリセットできます。

## 手順

- 
- ステップ 1** [ポリシー (Policies)] > [相関 (Correlation)] を選択して、[ホワイトリスト (White List)] タブ をクリックします。
- ステップ 2** [共有プロファイルの編集 (Edit Shared Profiles)] をクリックします。
- ステップ 3** 共有ホスト プロファイルを管理します。
- 共有ホストプロファイルの作成：ホストの調査なしで新しい共有ホスト プロファイルを作成するには、[共有ホストプロファイル (Shared Host Profiles)] の横にある追加アイコン (⊕) をクリックし、[ホワイトリスト ホスト プロファイルの作成, \(10 ページ\)](#) で説明する手順を実行します。
  - 調査によるホストプロファイルの作成：ネットワークの調査によって複数の新しい共有ホスト プロファイルを作成するには、[ターゲット ネットワークの追加 (Add Target Network)] をクリックして、[コンプライアンス ホワイトリストのターゲット ネットワークの設定, \(9 ページ\)](#) で説明する手順を実行します。
  - 削除：共有ホストプロファイルを削除するには、削除アイコン (🗑️) をクリックして、選択内容を確認します。
  - 編集：既存の共有ホストプロファイル (組み込み共有ホストプロファイルを含む) を変更するには、そのプロファイルの名前をクリックして、[ホワイトリスト ホスト プロファイルの作成, \(10 ページ\)](#) で説明する手順を実行します。
  - 組み込みのホストプロファイルのリセット：すべての組み込みホストプロファイルを工場出荷時の初期状態にリセットするには、[組み込みホストプロファイル (Built-in Host Profiles)] をクリックして、[工場出荷時の初期状態にリセット (Reset to Factory Defaults)] をクリックしてから、選択内容を確認します。
- ステップ 4** 最後の保存以降に行われたすべての変更をすぐに実装するには、[すべてのプロファイルの保存 (Save All Profiles)] をクリックします。
-

