FireSIGHT システムのコンプライアンス ツールとしての使用

コンプライアンス ホワイト リスト（または*ホワイト リスト*）は、一連の基準で、ユーザはこれを使用して、特定のサブネット上での実行を許可するオペレーティング システム、アプリケーション、およびプロトコルを指定できます。また、サブネット上のホストがホワイト リストに違反した場合、自動的にイベントが生成されます。たとえば、セキュリティ ポリシーで、Web サーバには HTTP の実行を許可するが、ネットワーク上の他のホストには許可しないように指定したとします。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 リストを作成できます。

次の条件でトリガーされるようにルールを設定することによって、この機能を実現する相関ルールを作成できます。

- システムがアプリケーション プロトコルに関する新しい情報を検出する
- アプリケーション プロトコルの名前は http である
- イベントに関係するホストの IP アドレスが Web ファーム内に存在しない

ただし、ネットワーク上のポリシー違反を警告して対処するためのより柔軟な方法を提供する相関ルールは、ホワイト リストよりも設定や保守が複雑です。また、相関ルールの方が対象範囲が広いうえ、複数のイベント タイプのいずれかが指定された条件を満たした段階で相関イベントを生成することができます。一方、ホワイト リストは、ネットワーク上で実行しているオペレーティング システム、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、およびプロトコルが組織のポリシーに違反していないかどうかの評価を支援するためのものです。

特定のニーズを満たすカスタム ホワイト リストを作成することも、オペレーティング システム、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、およびプロトコルを許可する場合の推奨設定を含む、シスコの脆弱性調査チーム（VRT）が作成したデフォルト ホワイト リストを使用することもできます。デフォルト ホワイト リストはネットワーク環境に合わせてカスタマイズすることもできます。

ホワイト リストをアクティブな相関ポリシーに追加すると、ホストがホワイト リストに違反していることをシステムが検出したときに、特別な種類の相関イベントであるホワイト リスト イベントがデータベースに記録されます。また、ホワイト リスト違反の検出時に自動的に応答（修復とアラート）をトリガーするようにシステムを設定できます。

注　NetFlow 対応デバイスによってエクスポートされたデータに基づいてホストとアプリケーション プロトコルをネットワーク マップに追加するようにネットワーク検出ポリシーを設定できますが、これらのホストとアプリケーション プロトコルに関して利用可能な情報が制限されます。たとえば、ホスト入力機能を使用してデータが提供されていない限り、これらのホストに関して利用可能なオペレーティング システム データはありません。これは、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。詳細については、「NetFlow と FireSIGHT データの違い」（P.35-20）を参照してください。

作成されたホワイト リストに準拠しているかどうかを示すホスト属性がホストごとに作成されるため、ネットワークの準拠の概要を把握できます。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、相関機能を使用して、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。

加えて、ホスト プロファイルを使用して、個別のホストが設定されたホワイト リストに違反しているどうかと、ホストがどのようにホワイト リストに違反しているかを特定できます。FireSIGHT システムには、個別のホワイト リスト違反のそれぞれとホストあたりの違反数を表示可能なワークフローも含まれています。

最後に、ダッシュボードを使用して、ホワイト リスト イベントやネットワーク全体のホワイト リスト準拠の概要ビューを含む、最新のシステム規模の準拠活動を監視できます。

コンプライアンス ホワイト リストの作成および管理とホワイト リスト イベントおよび違反の解釈に関する詳細については、以下の項を参照してください。

- 「コンプライアンス ホワイト リストについて」（P.27-3）
- 「コンプライアンス ホワイト リストの作成」（P.27-9）
- 「コンプライアンス ホワイト リストの管理」（P.27-26）
- 「共有ホスト プロファイルの操作」（P.27-28）
- 「ホワイト リスト イベントの操作」（P.27-33）
- 「ホワイト リスト違反の処理」（P.27-38）

加えて、以下の章と項で追加情報を参照してください。

- 「相関ポリシーの作成」（P.39-48）では、コンプライアンス ホワイト リストを含む相関ポリシーの作成方法と設定方法およびホワイト リストへの応答とプライオリティの割り当て方法について説明します。
- 「ホスト プロファイルの使用」（P.37-1）では、ホストのプロファイルを使用してホワイト リストに違反しているかどうかを判断する方法について説明します。
- 「ダッシュボードの使用」（P.3-1）では、ホワイト リスト準拠活動を含む、現在のシステム ステータスの概要を取得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 リストについて

ライセンス：FireSIGHT

*コンプライアンス ホワイト リスト*は、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、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する基準のセットです。特定のニーズを満たすカスタム ホワイト リストを作成することも、推奨設定を含む VRT によって作成されたデフォルト ホワイト リストを使用することもできます。

カスタム ホワイト リストの基準は単純にすることができます。特定のオペレーティング システムを実行しているホストのみを許可するように指定できます。基準は複雑にすることもできます。すべてのオペレーティング システムを許可するが、特定のオペレーティング システムを実行しているホストのみに特定のポート上での特定のアプリケーション プロトコルの実行を許可するように指定できます。

ホワイト リストは*ターゲット*と*ホスト プロファイル*という 2 つの主要部分で構成されます。ターゲットはホワイト リストによって評価される特定のホストであるのに対して、ホスト プロファイルはターゲッ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、およびプロトコルを指定します。

ホワイト リストを作成してアクティブな相関ポリシーに追加すると、システムがホスト プロファイルに照らしてホワイト リストのターゲットを評価し、ホワイト リストに準拠しているかどうかを判断します。この初期評価後に、システムは有効なターゲットがホワイト リストに違反していることを検出した時点で*ホワイト リスト イベント*を生成します。

詳細については、次の項を参照してください。

- 「ホワイト リスト ターゲットについて」（P.27-3）では、ホワイト リストがどのようにして指定されたホストのみを対象とするかを説明します。
- 「ホワイト リスト ホスト プロファイルについて」（P.27-4）では、ネットワーク上での実行を許可するクライアント、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記述したさまざまなプロファイルについて説明します。
- 「ホワイト リストの評価について」（P.27-6）では、システムがどのようにネットワーク上のホストをホワイト リストに照らして評価するかと、準拠しているホストと準拠していないホストの区別方法について説明しています。
- 「ホワイト リスト違反について」（P.27-7）では、システムがどのようにホワイト リスト違反を検出し、通知するかについて説明します。

ホワイト リスト ターゲットについて

ライセンス：FireSIGHT

ホワイト リストを作成する場合は、最初にそれを適用するネットワークの部分を指定します。ホワイト リストを使用してモニタリング対象ネットワーク上のすべてのホストを評価することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ホワイト リストの評価対象となるホストは、*有効なターゲット*（または*ターゲット*）と呼ばれます。有効なターゲットは次のようなものです。

- 指定された IP アドレス ブロックのいずれかに含まれている必要があります。IP アドレスのブロックを除外することもできます。
- 指定されたホスト属性を 1 つ以上持っている必要があります。

  たとえば、ホスト重要度の高いホストのみを評価するようにホワイト リストを設定できます。ホスト重要度を含むホスト属性の詳細については、「ユーザ定義のホスト属性の使用」（P.37-35）と「事前定義のホスト属性の使用」（P.37-35）を参照してください。
- 指定された VLAN のいずれかに属している必要があります。

ホストがこれらの基準のすべてを満たしていない場合は、そのホスト プロファイルがホワイト リストに違反しているかどうかに関係なく、ホワイト リストに照らして評価されません。

ホワイト リストに複数のターゲットが含まれている場合、その中のいずれか 1 つのみで指定された条件を満たしていれば、ホストは有効と見なされます。たとえば、10.10.x.x ネットワークを含むターゲットと 10.10.x.x ネットワークを除外するターゲットを作成した場合、そのネットワークのホストは有効なターゲットと見なされます。ホワイト リストにターゲットが含まれていない場合は、ネットワーク上のどのホストもホワイト リストに照らして評価されないことに注意してください。

ホワイト リストのターゲット ネットワークは、[Create White List] ページの左側に一覧表示されます。デフォルト ホワイト リストではモニタリング対象ネットワークの全体を表す 0.0.0.0/0 と ::/0 のターゲットが使用されることに注意してください。このホワイト リストを使用する場合は、ターゲット ネットワークを現状のままにすることも、使用しているネットワーク環境を反映するように変更することもできます。

ホワイト リスト ターゲットの作成方法については、「コンプライアンス ホワイト リスト ターゲットの設定」（P.27-12）を参照してください。

ホワイト リスト ホスト プロファイルについて

ライセンス：FireSIGHT

ホワイト リストで評価するターゲットを指定したら、次のステップは*ホスト プロファイル*の設定です。ホワイト リスト内のホスト 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、およびプロトコルを指定します。

ホワイト リストで設定可能なホスト プロファイルには 3 つの種類（グローバル ホスト プロファイル、特定のオペレーティング システム用のホスト プロファイル、および共有ホスト プロファイル）があります。ホワイト リストの作成中、それぞれのタイプのホスト プロファイルは異なって表示されます。

次の表に、異なる種類のホスト プロファイルの識別方法とアクセス方法の説明を示します。

表 27-1　　コンプライアンス ホワイト リスト ホスト プロファイルへのアクセス

表示対象	[Allowed Host Profiles] でのクリック対象
ホワイト リストのグローバル ホスト プロファイル	**任意のオペレーティング システム**
特定のオペレーティング システム用のホスト プロファイル	斜体ではなく、プレーン テキストで表記されたホスト プロファイル名
ホワイト リストで使用される共有ホスト プロファイル	斜体で表記されたホスト プロファイル名

詳細については、次の項を参照してください。

- 「グローバル ホスト プロファイルについて」（P.27-5）
- 「特定のオペレーティング システム用のホスト プロファイルについて」（P.27-5）
- 「共有ホスト プロファイルについて」（P.27-6）

グローバル ホスト プロファイルについて

ライセンス：FireSIGHT

すべてのホワイト リストに、ホストのオペレーティング システムに関係なく、ターゲット ホスト上での実行を許可されたアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定するグローバル ホスト プロファイルが含まれています。

たとえば、Internet Explorer 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、Internet Explorer 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。ARP、IP、TCP、および UDP の各プロトコルは、常に、すべてのホスト上での実行が許可されることに注意してください。これらを禁止することはできません。詳細については、「グローバル ホスト プロファイルの設定」（P.27-15）を参照してください。

特定のオペレーティング システム用のホスト プロファイルについて

ライセンス：FireSIGHT

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する必要があります。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ません。たとえば、ネットワーク上のすべてのホストで Microsoft 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。

特定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するときに、特定のバージョンに限定することもできます。たとえば、準拠ホストが Windows 7 または Windows Server 2008 R2 を実行する必要があると指定できます。

特定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たら、そのオペレーティング システムを実行しているターゲット ホスト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、およびプロトコルを指定できます。たとえば、Linux ホストのポート 22 での SSH の実行を許可することができます。また、特定のベンダーとバージョンを OpenSSH 4.2 に限定することもできます。

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ることに注意してください。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す。

注　未確認ホストと不明ホストは違います。*未確認*ホストは、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です。*不明*ホストは、トラフィックがシステムによって分析されているが、オペレーティング システムが既知のフィンガープリントのいずれとも一致しないホストです。

詳細については、「特定のオペレーティング システム用のホスト プロファイルの作成」（P.27-16）を参照してください。

共有ホスト プロファイルについて

ライセンス：FireSIGHT

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。つまり、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。

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 リストを作成したうえで、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場合に、そのオペレーティング システム用の共有プロファイルを作成して、それをすべてのホワイト リストで使用します。

デフォルト ホワイト リストは、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許可する場合に推奨される「ベスト プラクティス」設定を意味します。このホワイト 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。組み込みホスト プロファイルには組み込みホスト プロファイル アイコン（  ）が付けられることに注意してください。

組み込みホスト プロファイルでは、組み込みアプリケーション プロトコル、プロトコル、およびクライアントが使用されます。これらの要素は、デフォルト ホワイト リストと作成されたカスタム ホワイト リストの両方でそのまま使用することも、必要に応じて変更することもできます。また、これらの要素は、組み込みホスト プロファイルおよびそれらの要素を使用するその他すべてのホスト プロファイル内で斜体で表示されます。

共有ホスト プロファイルと同様に、組み込みホスト プロファイルを変更した場合は、それが使用されているすべてのホワイト リストに影響することに注意してください。同様に、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は、それが使用されているすべてのホワイト リストに影響します。

共有ホスト プロファイルの詳細については、「共有ホスト プロファイルの操作」（P.27-28）を参照してください。

ホワイト リストの評価について

ライセンス：FireSIGHT

ホワイト リスト ホスト プロファイルを作成してホワイト リストを保存したら、相関ルールと同様に、ホワイト リストを相関ポリシーに追加できます。詳細については、「相関ポリシーおよび相関ルールの設定」（P.39-1）を参照してください。

相関ポリシーをアクティブにすると、システムがホワイト リストの条件に照らしてホワイト リストのターゲットを評価します。その後で、ホスト属性ネットワーク マップを使用して、ネットワーク上のホストのホワイト リスト準拠の全体像を把握できます。

ネットワーク上のすべてのホストに、ホワイト リストと同じ名前のホスト属性が割り当てられます。このホスト属性に次のいずれかの値が付与されます。

- [Compliant] ホワイト リストに準拠する有効なターゲットの場合
- [Non-Compliant] ホワイト リストに違反する有効なターゲットの場合
- [Not Evaluated] 何らかの理由で評価されていない無効なターゲットとホストの場合

ネットワークが大規模で、システムがネットワーク マップ内のすべての有効なターゲットをホワイト リストに照らして評価している途中の場合は、まだ評価されていないターゲットが [Not Evaluated] としてマークされることに注意してください。システムが処理を完了すると、さらに多くのホストが [Not Evaluated] から [Not Evaluated] または [Non-Compliant] のいずれかに移行します。システムは 1 秒あたり約 100 ホストを評価できます。

加えて、ホストが準拠しているかどうかを判断するのに十分な情報が収集されていない場合は、ホストが [Not Evaluated] としてマークされます。たとえば、この状態は、新しいホストが検出されたが、そのホスト上で実行されてい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、またはプロトコルに関連した情報が収集されていない場合に発生します。

注　ホストでホスト属性が変更または削除され、その変更または削除がホストが有効なターゲットでなくなったことを意味する場合、そのホストは [Compliant] または [Non-Compliant] から [Not Evaluated] に移行されます。

ホスト属性の詳細については、「ホスト属性のネットワーク マップの使用」（P.36-10）を参照してください。

ホワイト リスト違反について

ライセンス：FireSIGHT

ホワイト リストの初期評価後に、システムは有効なターゲットがホワイト リストに違反していることを検出した時点で*ホワイト リスト イベント*を生成します。ホワイト リスト イベントは、相関イベントの特殊な形態で、防御センター相関イベント データベースに記録されます。ワークフロー内のホワイト リスト イベントを表示したり、特定のホワイト リスト イベントを検索したりできます。詳細については、「ホワイト リスト イベントの操作」（P.27-33）を参照してください。

ホワイト リスト違反は、ホストが準拠していないことを示すイベントが生成されたときに発生します。同様に、検出イベントによって非準拠だったホストが準拠に移行したことが示される場合がありますが、この場合システムではホワイト リスト イベントを**生成しません**。

次のイベントはホストの準拠に影響を与える可能性があります。

- システムがホストのオペレーティング システムの変更を検出
- システムが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 プロトコルのアイデンティティ競合を検出
- システムが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
- システムが、ホスト上で実行中の検出された TCP 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
- システムがホスト上で実行中の新しいクライアントを検出
- システムが非アクティブという理由でデータベースからクライアントをドロップ
- システムがホスト上で実行中の新しい Web アプリケーションを検出
- システムが非アクティブという理由でホスト プロファイルから Web アプリケーションをドロップ

- システムが、ホストが Novell NetWare や IPv6 などの新しいネットワーク プロトコルまたは ICMP や EGP などの新しい転送プロトコルで通信中であることを検出
- システムがジェイルブレイクされた新しいモバイル デバイスを検出
- システムが TCP または UDP ポートがホスト上で閉じられたか、タイムアウトしたことを検出

加えて、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、ホストの準拠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
- ホストのオペレーティング 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

たとえば、ホワイト リストで Microsoft Windows ホストのみをネットワーク上で許可するように指定されている場合は、ホストが現在 Mac OS X を実行していることをシステムが検出したときに、ホワイト リスト イベントが生成されます。加えて、ホワイト リストに関連付けられたホスト属性の値が [Compliant] から [Non-Compliant] に変更されます。

この例のホストが準拠に復帰するには、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 Microsoft Windows に戻ったことをシステムが検出する

いずれの場合も、ホワイト リストに関連付けられたホスト属性の値が [Non-Compliant] から [Compliant] に変更されます。

別の例として、コンプライアンス ホワイト リストで FTP の使用が禁止されている状態で、アプリケーション プロトコル ネットワーク マップまたはイベント ビューから FTP が削除された場合は、FTP を実行中のホストが準拠になります。ただし、システムがアプリケーション プロトコルをもう一度検出すると、ホワイト リスト イベントが生成され、ホストは非準拠になります。

システムがホワイト リストに関する情報が不十分なイベントを生成した場合は、ホワイト リストがトリガーされないことに注意してください。たとえば、ホワイト リストでポート 21 上の TCP FTP トラフィックのみを許可するように指定されているシナリオについて考えてみます。この場合、システムは、TCP プロトコルを使用しているポート 21 がホワイト リスト ターゲットのいずれかでアクティブになっていることを検出しますが、トラフィックが FTP かどうかを判断することはできません。このシナリオでは、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特定するか、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するまで、ホワイト リストがトリガーされません。

注　ホワイト リストの初期評価中は、システムが非準拠ホストに関するホワイト リスト イベントを**生成しません**。すべての非準拠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、防御センター データベースを消去する必要があります。これにより、ネットワークと関連クライアント上のホスト、アプリケーション プロトコル、Web アプリケーション、およびプロトコルが再検出され、ホワイト リスト イベントがトリガーされます。詳細については、「データベースからの検出データの消去」（P.B-1）を参照してください。

最後に、ホワイト リスト違反を検出したときに自動的に応答をトリガーとして使用するようにシステムを設定できます。応答には、修復（Nmap スキャンの実行など）、アラート（電子メール、SNMP、および syslog アラート）、またはアラートと修復の組み合わせが含まれます。詳細については、「ルールとホワイトリストに応答を追加する」（P.39-51）を参照してください。

コンプライアンス ホワイト リストの作成

ライセンス：FireSIGHT

ホワイト リストを作成するときに、ネットワーク全体または特定のネットワーク セグメントを調査できます。ネットワークを調査すると、システムがネットワーク セグメント上で検出したオペレーティング システムごとに 1 つずつのホスト プロファイルでホワイト リストが生成されます。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。

次に、ホワイト リストのターゲットを指定する必要があります。モニタリング対象のネットワーク上のすべてのホストを評価するようにホワイト リストを設定することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ネットワークを調査すると、デフォルトで、調査したネットワーク セグメントがホワイト リスト ターゲットになります。調査したネットワークを編集または削除したり、新しいターゲットを追加したりできます。

その後で、準拠ホストを示すホスト プロファイルを作成します。ホワイト リスト内のホスト 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、およびプロトコルを指定します。グローバル ホスト プロファイルの設定、実施したネットワーク調査によって作成されたホスト プロファイルの編集、新しいホスト プロファイルの追加、および共有ホスト プロファイルの追加と編集を行うことができます。

最後に、ホワイト リストを保存して、それをアクティブな相関ポリシーに追加します。システムは、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびホワイト リスト違反に対して設定された応答のトリガーを開始します。コンプライアンス ホワイト リストの詳細については、「コンプライアンス ホワイト リストについて」（P.27-3）を参照してください。

ヒント　ホストのテーブル ビューからホワイト リストを作成することもできます。詳細については、「選択したホストに基づいたコンプライアンスのホワイト リストの作成」（P.38-26）を参照してください。

コンプライアンス ホワイト リストを作成する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[New White List] をクリックします。

[Survey Network] ページが表示されます。

ステップ 3　オプションで、ネットワークを調査します。

- ネットワークを調査するには、「ネットワークの調査」（P.27-10）を参照してください。
- ネットワークを調査せずにホワイト リストを作成するには、[Skip] をクリックして次のステップに進みます。

[Create White List] ページが表示されます。

ステップ 4　[Name] フィールドに、新しいホワイト リストの名前を入力します。

ステップ 5　[Description] フィールドに、ホワイト リストの簡単な説明を入力します。

ステップ 6　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、[Allow Jailbroken Mobile Devices] をオンにします。ジェイルブレイクされたデバイスをホワイト リストで評価することによってホワイト リスト違反を発生させる場合は、このオプションをオフにします。

ステップ 7　ホワイト リストのターゲットを指定します。ネットワーク調査により作成されたターゲットを編集または削除するだけでなく、新しいターゲットを追加することもできます。オプションで、ホスト属性または VLAN ID に基づいてさらにターゲットを制限します。詳細については、「コンプライアンス ホワイト リスト ターゲットの設定」（P.27-12）を参照してください。

ステップ 8　準拠ホストを示すホスト プロファイルを作成します。グローバル ホスト プロファイルの設定、ネットワーク調査によって作成されたホスト プロファイルの編集、新しいホスト プロファイルの追加、および共有ホスト プロファイルの追加と編集を行うことができます。詳細については、「コンプライアンス ホワイト リスト ホスト プロファイルの設定」（P.27-15）を参照してください。

ステップ 9　ホワイト リストを保存するには、[Save White List] をクリックします。

ホワイト リストが保存されます。これで、ホワイト リストをアクティブな相関ポリシーに追加して、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびオプションのホワイト リスト違反に対する応答のトリガーを開始できます。詳細については、「相関ポリシーの作成」（P.39-48）を参照してください。

ネットワークの調査

ライセンス：FireSIGHT

コンプライアンス ホワイト リストの作成を開始するときに、ネットワーク全体または特定のネットワーク セグメントを調査できます。

ネットワークの調査で、検出されたさまざまなオペレーティング システム上で実行中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、およびプロトコルに関するデータがデータベースから収集されます。その後で、システムがホワイト リストに検出したオペレーティング システムごとに 1 つずつのホスト プロファイルを作成します。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。

これにより、ベースライン ホワイト リストが作成されるため、手動で複数のホスト プロファイルを作成して設定する必要がありません。ネットワークを調査したら、調査によりニーズに合わせて作成されたホスト プロファイルを編集または削除できます。必要なその他のホスト プロファイルを追加することもできます。

ホワイト リストの作成プロセス中はいつでもネットワークを調査できることに注意してください。これにより、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。アクティブな相関ポリシーで使用されているホワイト リスト内のネットワークを再調査して、ターゲットとホスト プロファイルのどちらかが変更された場合は、ホワイト リストの保存時にターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ネットワークを調査することによって、コンプライアンス ホワイト リストの作成を開始する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[New White List] をクリックします。

[Survey Network] ページが表示されます。

ステップ 3　ネットワークを調査しますか。

- **はい**の場合は、次のステップに進みます。
- **いいえ**の場合は、[Skip] をクリックします。

  [Create White List] ページが開いて、空白のホワイト リストが表示されます。次の項（基本的なホワイト リスト情報の提供）の手順に進みます。

ステップ 4　[IP Address] フィールドと [Netmask] フィールドに、調査するホストを表す IP アドレスとネットワーク マスクを（CIDR などの特殊な表記で）入力します。

ネットワーク検出ポリシーで監視するようにシステムを設定したネットワークを指定したことを確認します。FireSIGHT システムで使用する IP アドレス表記については、「IP アドレスの表記法」（P.1-19）を参照してください。

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。

ステップ 5　[OK] をクリックします。

[Create White List] ページが表示されます。

ホワイト リストは事前設定されています。そのターゲットは調査したネットワーク上のホストであり、許可されるホスト プロファイルはターゲットのプロファイルです。

ステップ 6　追加のネットワークを調査するには、[Target Network] をクリックし、調査する追加のネットワークごとにステップ 4 と 5 を繰り返します。

追加のネットワークの調査で、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。また、調査したネットワーク セグメント内のホストを表すホワイト リストにターゲットを追加することもできます。このターゲットは、後で、編集または削除することができます。

ステップ 7　次の項基本的なホワイト リスト情報の提供に進みます。

基本的なホワイト リスト情報の提供

ライセンス：FireSIGHT

ホワイト リストごとに名前と簡単な説明（オプション）を入力する必要があります。加えて、ジェイルブレイクされたモバイル デバイスによってホワイト リスト違反が発生するかどうかを選択できます。

基本的なホワイト リスト情報を提供する方法：

アクセス：Admin

ステップ 1　[Name] フィールドに、新しいホワイト リストの名前を入力します。

ステップ 2　[Description] フィールドに、ホワイト リストの簡単な説明を入力します。

ステップ 3　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、[Allow Jailbroken Mobile Devices] をオンにします。ジェイルブレイクされたデバイスをホワイト リストで評価することによってホワイト リスト違反を発生させる場合は、このオプションをオフにします。

ステップ 4　次の項コンプライアンス ホワイト リスト ターゲットの設定に進みます。

コンプライアンス ホワイト リスト ターゲットの設定

ライセンス：FireSIGHT

コンプライアンス ホワイト リストを作成するときに、それを適用するネットワークの部分を指定する必要があります。ホワイト リストを使用してモニタリング対象ネットワーク上のすべてのホストを評価することも、特定のネットワーク セグメントまたは個別のホストのみを評価するようにホワイト リストを制限することもできます。特定のホスト属性を持っている、または、特定の VLAN に属しているホストのみを評価するようにさらにホワイト リストを制限できます。ホワイト リストの評価対象になるホストは、ターゲットと呼ばれます。ホワイト リスト ターゲットの詳細については、「ホワイト リスト ターゲットについて」（P.27-3）を参照してください。

コンプライアンス ホワイト リスト ターゲットの作成が完了したら、「コンプライアンス ホワイト リスト ホスト プロファイルの設定」（P.27-15）に進みます。

注　ホストのホスト属性を変更または削除した結果、ホストが有効なターゲットではなくなった場合、そのホストはホワイト リストに照らして評価されなくなり、準拠でも非準拠でもないと見なされます。

ターゲットの変更方法と削除方法については、以下を参照してください。

- 「既存のターゲットの変更」（P.27-14）
- 「既存のターゲットの削除」（P.27-14）

コンプライアンス ホワイト リストのターゲットを作成するときに、ホストがホワイト リストに照らして評価されるための基準を指定します。有効なターゲットは次のようなものです。

- 指定された IP アドレス ブロックのいずれかに含まれている必要があります。IP アドレスのブロックを除外することもできます。
- 指定されたホスト属性を 1 つ以上持っている必要があります。
- 指定された VLAN のいずれかに属している必要があります。

アクティブな相関ポリシーで使用されているホワイト リストにターゲットを追加した場合は、ホワイト リストの保存後に新しいターゲット ホストの準拠が評価されることに注意してください。ただし、この評価でホワイト リスト イベントは生成されません。

コンプライアンス ホワイト リスト ターゲットを作成する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、[Target Networks] の横にある追加アイコン（  ）をクリックします。

新しいターゲットの設定が表示されます。

ヒント　ネットワーク セグメントを調査することによって新しいターゲットを作成することもできます。[Create White List] ページで、[Target Network] をクリックしてから、「ネットワークの調査」（P.27-10）のステップ 4 と 5 を実行します。新しいターゲットが作成され、指定された IP アドレスに基づいて名前が付けられます。作成したターゲットをクリックし、残りの手順に進んでターゲットの名前を変更したり、新しいネットワークを追加または除外したり、ホスト属性または VLAN 制限を追加したりします。

ステップ 2　[Name] フィールドに、新しいターゲットの名前を入力します。

ステップ 3　[Targeted Networks] の横にある追加アイコン（）をクリックして、特定の IP アドレスのセットをターゲットにします。

ステップ 4　[IP Address] フィールドと [Netmask] フィールドに、ターゲットにするまたはターゲットから除外するホストを表す IP アドレスとネットワーク マスクを（CIDR などの特殊な表記で）入力します。

ネットワーク検出ポリシーで監視するようにシステムを設定したネットワークを指定したことを確認する必要があります。FireSIGHT システムで使用する IP アドレス表記については、「IP アドレスの表記法」（P.1-19） を参照してください。

ヒント　モニタリング対象のネットワーク全体をターゲットにするには、`0.0.0.0/0` と `::/0` を使用します。

ステップ 5　ネットワークをモニタリング対象から除外する場合は、[Exclude] を選択します。

ステップ 6　新しいネットワークを追加するには、ステップ 4 と 5 を繰り返します。

ステップ 7　[Targeted Host Attributes] の横にある [Add] をクリックして、特定のホスト属性を持つホストをターゲットにします。

ステップ 8　[Attribute] と [Value] の各ドロップダウン リストから、ホスト属性を指定します。

ステップ 9　新しいホスト属性を追加するには、ステップ 7 と 8 を繰り返します。

ホストには、ホワイト リストに照らして評価される 1 つ以上のホスト属性を指定する必要があります。

ステップ 10　[Targeted VLANs] の横にある [Add] をクリックして、特定の VLAN に属しているホストをターゲットにします。

ステップ 11　[VLAN ID] フィールドで、ホワイト リストに照らして評価するホストの VLAN ID を指定します。これは、802.1q VLAN 用の 0 ～ 4095 の任意の整数にすることができます。

ステップ 12　新しい VLAN ID を追加するには、ステップ 10 と 11 を繰り返します。

ホストは、ホワイト リストに照らして評価するように指定された VLAN のいずれかのメンバーである必要があります。

ヒント　ネットワーク、ホスト属性制限、または VLAN 制限を削除するには、削除する要素の横にある削除アイコン（  ）をクリックします。

既存のターゲットの変更

ライセンス：FireSIGHT

ターゲットを変更したら、その変更を反映させるためにホワイト リストを保存する必要があります。アクティブな相関ポリシーで使用されているホワイト リスト内のターゲットを変更した場合は、ホワイト リストの保存後に新しいターゲット ホストの準拠が評価されることに注意してください。ただし、この評価でホワイト リスト イベントは生成されません。加えて、システムが有効だったターゲットのホワイト リスト ホスト属性を [Not Evaluated] に変更します。

既存のターゲットを変更する方法：

アクセス：Admin

ステップ 1　[Create White List] ページの [Targets] で、変更するターゲットをクリックします。

ターゲットの設定が表示されます。

ステップ 2　必要に応じて変更を加えます。

ターゲットの名前を変更したり、新しいネットワークを追加または除外したり、ホスト属性または VLAN 制限を追加したりできます。詳細については、「コンプライアンス ホワイト リスト ターゲットの設定」（P.27-12）を参照してください。

既存のターゲットの削除

ライセンス：FireSIGHT

ターゲットを削除したら、その変更を反映させるためにホワイト リストを保存する必要があります。アクティブな相関ポリシーで使用されているホワイト リストからターゲットを削除した場合は、システムが有効だったターゲットのホワイト リスト ホスト属性を [Not Evaluated] に変更することに注意してください。

ホワイト リスト ターゲットを削除する方法：

アクセス：Admin

ステップ 1　削除するターゲットの横にある削除アイコン（  ）をクリックします。

ステップ 2　プロンプトが表示されたら、ターゲットの削除を確認します。

ターゲットが削除されます。

コンプライアンス ホワイト リスト ホスト プロファイルの設定

ライセンス：FireSIGHT

コンプライアンス ホワイト リスト内のホスト 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、およびプロトコルを指定します。ホワイト リストで設定可能なホスト プロファイルには次の 3 つの種類があります。

- ホストのオペレーティング 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、およびプロトコルを指定するグローバル ホスト プロファイル
- 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する特定のオペレーティング システム用のホスト プロファイル
- 単一のホワイト リストに関連付けられないことを除いて、特定のオペレーティング システム用のホスト プロファイルとまったく同様に機能する共有ホスト プロファイル。これは、複数のホワイト リストで使用できます。

ホワイト リスト ホスト プロファイルの詳細については、「ホワイト リスト ホスト プロファイルについて」（P.27-4）を参照してください。

コンプライアンス ホワイト リスト ホスト プロファイルの作成が完了したら、ホワイト リストをアクティブな相関ポリシーに追加して、ターゲット ホストの準拠の評価、ホストがホワイト リストに違反した場合のホワイト リスト イベントの生成、およびオプションでホワイト リスト違反に基づく応答のトリガーを開始できます。

コンプライアンス ホワイト リスト ホスト プロファイルの作成方法、変更方法、および削除方法については、以下を参照してください。

- 「グローバル ホスト プロファイルの設定」（P.27-15）
- 「特定のオペレーティング システム用のホスト プロファイルの作成」（P.27-16）
- 「コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加」（P.27-22）
- 「既存のホスト プロファイルの変更」（P.27-23）
- 「既存のホスト プロファイルの削除」（P.27-26）

グローバル ホスト プロファイルの設定

ライセンス：FireSIGHT

すべてのホワイト リストに、ホストのオペレーティング システムに関係なく、ターゲット ホスト上での実行を許可されたアプリケーション プロトコル、クライアント、Web アプリケーション、およびプロトコルを指定するグローバル ホスト プロファイルが含まれています。グローバル ホスト プロファイルの詳細については、「グローバル ホスト プロファイルについて」（P.27-5）を参照してください。

グローバル ホスト プロファイルを設定する方法：

アクセス：Admin

ステップ 1　[Create White List] ページの [Allowed Host Profiles] で、[Any Operating System] をクリック します。

グローバル ホスト プロファイルの設定が表示されます。

ステップ 2　許可するアプリケーション プロトコルを指定するには、「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）の指示に従ってください。

ステップ 3　許可するクライアントを指定するには、「ホスト プロファイルへのクライアントの追加」（P.27-19）の指示に従ってください。

ステップ 4　許可する Web アプリケーションを指定するには、「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20）の指示に従ってください。

ステップ 5　許可するプロトコルを指定するには、「ホスト プロファイルへのプロトコルの追加」（P.27-21）の指示に従ってください。

ARP、IP、TCP、および UDP は常に許可されることに注意してください。

特定のオペレーティング システム用のホスト プロファイルの作成

ライセンス：FireSIGHT

特定のオペレーティング システム用のホスト プロファイルは、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。詳細については、「特定のオペレーティング システム用のホスト プロファイルについて」（P.27-5）を参照してください。

特定のオペレーティング システム用の新しいコンプライアンス ホワイト リスト ホスト プロファイルを作成する方法：

アクセス：Admin

ステップ 1　[Allowed Host Profiles] の横にある追加アイコン（  ）をクリックします。

新しいホスト プロファイルの設定が表示されます。

ステップ 2　[Name] フィールドに、ホスト プロファイルの分かりやすい名前を入力します。

ステップ 3　[OS Vendor]、[OS Name]、および [Version] の各ドロップダウン リストから、ホスト プロファイルを作成するオペレーティング システムとバージョンを選択します。

ステップ 4　許可するアプリケーション プロトコルを指定します。次の 3 つのオプションがあります。

- すべてのアプリケーション プロトコルを許可するには、[Allow all Application Protocols] チェック ボックスをオンのままにします。
- どのアプリケーション プロトコルも許可しない場合は、[Allow all Application Protocols] チェック ボックスをオフにします。
- 特定のアプリケーション プロトコルを許可するには、「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）の指示に従ってください。

ステップ 5　許可するクライアントを指定します。次の 3 つのオプションがあります。

- すべてのクライアントを許可するには、[Allow all Clients] チェック ボックスをオンのままにします。
- どのクライアントも許可しない場合は、[Allow all Clients] チェック ボックスをオフにします。
- 特定のクライアントを許可するには、「ホスト プロファイルへのクライアントの追加」（P.27-19）の指示に従ってください。

ステップ 6　許可する Web アプリケーションを指定します。次の 3 つのオプションがあります。

- すべての Web アプリケーションを許可するには、[Allow all Web Applications] チェック ボックスをオンのままにします。
- どの Web アプリケーションも許可しない場合は、[Allow all Web Applications] チェック ボックスをオフにします。
- 特定の Web アプリケーションを許可するには、「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20）の指示に従ってください。

ステップ 7　許可するプロトコルを指定します。

プロトコルを追加するには、[Allowed Protocols] の横で、「ホスト プロファイルへのプロトコルの追加」（P.27-21）の手順に従ってください。ARP、IP、TCP、および UDP は常に許可されることに注意してください。

ホスト プロファイルへのアプリケーション プロトコルの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のアプリケーション プロトコルの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のアプリケーション プロトコルの実行を許可するように設定できます。これは、グローバルに許可されたアプリケーション プロトコルと呼ばれます。

許可するアプリケーション プロトコルに関して、許可するアプリケーション プロトコルのタイプ（FTP と SSH がアプリケーション プロトコル タイプの例）を指定することも、アプリケーション プロトコル タイプに [any] を指定してカスタム アプリケーション プロトコルを許可することもできます。許可するアプリケーション プロトコルで使用されるプロトコル（TCP または UDP）を指定する必要もあります。任意のポートでアプリケーション プロトコルを許可することも、特定のポートに限定することもできます。

オプションで、アプリケーション プロトコル サーバのベンダーまたはバージョンを限定することができます。たとえば、Linux ホストのポート 22 での SSH の実行を許可することができます。また、特定のベンダーとバージョンを OpenSSH 4.2 に限定することもできます。

アプリケーション プロトコルをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

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、[Allowed Application Protocols]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Application Protocols]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるアプリケーション プロトコルは次のとおりです。

- ホワイト リスト内で作成したアプリケーション プロトコル
- 「ネットワークの調査」（P.27-10）の説明に従ってネットワークを調査したときにネットワーク マップ内に存在したアプリケーション プロトコル
- ホワイト リスト内の他のホスト プロファイルによって使用されるアプリケーション プロトコル。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みアプリケーション プロトコルが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するアプリケーション プロトコルを追加するには、それを選択して、[OK] をクリックします。複数のアプリケーション プロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のアプリケーション プロトコルを選択することもできます。

  アプリケーション プロトコルが追加されます。組み込みアプリケーション プロトコルを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、アプリケーション プロトコルの値（ポートやプロトコルなど）を変更するために、追加したアプリケーション プロトコルをクリックしてアプリケーション プロトコル エディタを表示することもできます。

- 新しいアプリケーション プロトコルを追加するには、[<New Application Protocol>] を選択して、[OK] をクリックします。

  アプリケーション プロトコル エディタが表示されます。

ステップ 3　[Type] ドロップダウン リストから、アプリケーション プロトコル タイプを選択します。カスタム アプリケーション プロトコルの場合は、[any] を選択します。

ステップ 4　アプリケーション プロトコル ポートを指定します。次の 2 つのオプションから選択できます。

- 任意のポート上でのアプリケーション プロトコルの実行を許可するには、[Any port] チェック ボックスをオンにします。
- 特定のポート上でのアプリケーション プロトコルの実行を許可するには、[port] フィールドにポート番号を入力します。

ステップ 5　[Protocol] ドロップダウン リストから、プロトコル（[TCP] または [UDP]）を選択します。

ステップ 6　オプションで、[Vendor] フィールドと [Version] フィールドで、アプリケーション プロトコルのベンダーとバージョンを指定します。

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。ベンダーとバージョンを制限する場合は、イベント ビューまたはアプリケーション プロトコル ネットワーク マップに表示されるとおりに正確に指定する必要があります。

ステップ 7　[OK] をクリックします。

アプリケーション プロトコルが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

アプリケーション プロトコルをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへのクライアントの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のクライアント アプリケーションの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のクライアントの実行を許可するように設定できます。これは、グローバルに許可されたクライアントと呼ばれます。

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 8.0 のみに許可することができます。

クライアントをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

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、[Allowed Clients]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Clients]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるクライアントは次のとおりです。

- ホワイト リスト内で作成したクライアント
- 「ネットワークの調査」（P.27-10）の説明に従ってネットワークを調査したときにネットワーク マップ内のホスト上で実行されていたクライアント
- ホワイト リスト内の他のホスト プロファイルによって使用されるクライアント。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みクライアントが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するクライアントを追加するには、それを選択して、[OK] をクリックします。複数のクライアントを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のクライアントを選択することもできます。

  クライアントが追加されます。組み込みクライアントを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、クライアントの値（バージョンなど）を変更するために、追加したクライアントをクリックしてクライアント エディタを表示することもできます。
- 新しいクライアントを追加するには、[<New Client>] を選択して、[OK] をクリックします。

  クライアント エディタが表示されます。

ステップ 3　[Client] ドロップダウン リストから、クライアントを選択します。

ステップ 4　オプションで、[Version] フィールドで、クライアントのバージョンを指定します。

バージョンを指定しなかった場合は、名前が一致している限り、ホワイト リストではすべてのバージョンが許可されます。バージョンを制限する場合は、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に正確に指定する必要があることに注意してください。

ステップ 5　[OK] をクリックします。

クライアントが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

クライアントをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへの Web アプリケーションの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または、単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定の Web アプリケーションの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定の Web アプリケーションの実行を許可するように設定できます。これは、グローバルに許可された Web アプリケーションと呼ばれます。

Web アプリケーションをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

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、[Allowed Web Applications]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Web Applications]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示され、システムで検出されたすべての Web アプリケーションが一覧表示されます。

ステップ 2　Web アプリケーションを選択して、[OK] をクリックします。複数の Web アプリケーションを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数の Web アプリケーションを選択することもできます。

Web アプリケーションが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

Web アプリケーションをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

ホスト プロファイルへのプロトコルの追加

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは、共有ホスト プロファイル、または単一のホワイト リストに属しているホスト プロファイルのいずれかを使用して、特定のオペレーティング システム上での特定のプロトコルの実行を許可するように設定できます。また、ホワイト リストは、有効な任意のターゲット上での特定のプロトコルの実行を許可するように設定できます。これは、グローバルに許可されたプロトコルと呼ばれます。ARP、IP、TCP、および UDP は、常にすべてのホスト上での実行が許可されることに注意してください。これらを禁止することはできません。

許可するプロトコルに関して、そのタイプ（ネットワークまたはトランスポート）と番号を指定する必要があります。

プロトコルをコンプライアンス ホワイト リスト ホスト プロファイルに追加する方法：

アクセス：Admin

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、[Allowed Protocols]（または [Any Operating System] ホスト プロファイルを変更している場合は [Globally Allowed Protocols]）の横にある追加アイコン（  ）をクリックします。

ポップアップ ウィンドウが表示されます。一覧表示されるプロトコルは次のとおりです。

- ホワイト リスト内で作成したプロトコル
- 「ネットワークの調査」（P.27-10）の説明に従ってネットワークを調査したときにネットワーク マップ内のホスト上で実行されていたプロトコル
- ホワイト リスト内の他のホスト プロファイルによって使用されるプロトコル。これには、デフォルト ホワイト リストで使用するために VRT によって作成された組み込みプロトコルが含まれる場合があります。

ステップ 2　次の 2 つのオプションから選択できます。

- リスト内にすでに存在するプロトコルを追加するには、それを選択して、[OK] をクリックします。複数のプロトコルを選択する場合は、Ctrl または Shift キーを押しながらクリックします。また、クリックしてドラッグすることによって、隣接する複数のプロトコルを選択することもできます。

  プロトコルが追加されます。組み込みプロトコルを追加した場合は、その名前が斜体で表示されることに注意してください。残りの手順を省略することも、オプションで、プロトコルの値（タイプや番号など）を変更するために、追加したプロトコルをクリックしてプロトコル エディタを表示することもできます。

- 新しいプロトコルを追加するには、[<New Protocol>] を選択して、[OK] をクリックします。

  プロトコル エディタが表示されます。

ステップ 3　[Type] ドロップダウン リストから、プロトコル タイプ（[Network] または [Transport]）を選択します。

ステップ 4　プロトコルを指定します。次の 2 つのオプションから選択できます。

- ドロップダウン リストからプロトコルを選択します。
- リスト内に存在しないプロトコルを指定するには、[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 5　[OK] をクリックします。

プロトコルが追加されます。変更を反映するためにはホワイト リストを保存する必要があることに注意してください。

プロトコルをアクティブな相関ポリシーで使用されているホワイト リストに追加した場合は、ホワイト リストの保存後に、ターゲット ホストが再評価されます。この再評価で一部のホストが準拠に移行したとしても、ホワイト リスト イベントは生成されません。

コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加

ライセンス：FireSIGHT

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、ホワイト リスト全体で使用できます。つまり、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。

組み込み共有ホスト プロファイルをコンプライアンス ホワイト リストに追加することも、作成した共有ホスト プロファイルを追加することもできます。詳細については、「共有ホスト プロファイルについて」（P.27-6）および「共有ホスト プロファイルの作成」（P.27-28）を参照してください。

共有ホスト プロファイルをコンプライアンス ホワイト リストに追加する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、[Add Shared Host Profile] をクリックします。

[Add Shared Host Profile] ページが表示されます。

ステップ 2　[Name] ドロップダウン リストから、ホワイト リストに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 プロファイルがホワイト リストに追加され、[Create White List] ページが再び表示されます。共有ホスト プロファイルの名前が [Allowed Host Profiles] の下に斜体で表示されます。

ヒント　[Allowed Host Profiles] でプロファイル名をクリックすることによって、それを使用するホワイト リストから共有ホスト プロファイルを編集できます。詳細については、「既存のホスト プロファイルの変更」（P.27-23）を参照してください。

既存のホスト プロファイルの変更

ライセンス：FireSIGHT

コンプライアンス ホワイト リスト内のホスト プロファイルを変更したら、その変更を反映させるためにホワイト リストを保存する必要があります。

変更するホスト プロファイルがアクティブな相関ポリシーで使用されているホワイト リストに属している場合は、プロファイルを変更すると、ホストが準拠または非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。また、共有ホスト プロファイルを変更すると、それを使用しているすべてのホワイト リストに影響します。これにより、操作しているホワイト リストだけでなく、その他のホワイト リストでもホストが準拠または非準拠に移行する場合があります。

ヒント　他の共有ホスト プロファイルと同様に、デフォルト ホワイト リストで使用されている組み込みホスト プロファイルを編集できます。それらを出荷時の初期状態にリセットすることもできます。詳細については、「組み込みホスト プロファイルの出荷時の初期状態へのリセット」（P.27-32）を参照してください。

既存のホスト プロファイルを変更する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、変更するホスト プロファイルの名前をクリックします。

ホスト プロファイルの設定が表示されます。共有ホスト プロファイルを編集している場合は、[Edit] リンクがホスト プロファイルの名前の横に表示されることに注意してください。組み込みホスト プロファイルを編集している場合は、組み込みホスト プロファイル アイコン（  ）も表示されます。

ステップ 2　次の 2 つのオプションから選択できます。

- 共有ホスト プロファイルを変更している場合は、[Edit] をクリックします。

  ポップアップ ウィンドウが表示されます。次の表に従って、必要に応じて変更を加えます。[Save All Profiles] をクリックしてプロファイルを保存してから、[Done] をクリックしてポップアップ ウィンドウを閉じます。

  共有ホスト プロファイルの編集方法については、「共有ホスト プロファイルの変更」（P.27-30）を参照してください。

- ホワイト リストのグローバル ホスト プロファイルまたは特定のオペレーティング システム用のホスト プロファイルを変更している場合は、次の手順に記載されているいずれかの操作を実行します。

ホスト プロファイルの名前を変更する方法：

アクセス：Admin

ステップ 1　[Name] フィールドに新しい名前を記入します。

ホスト プロファイルのオペレーティング システムを変更する方法：

アクセス：Admin

ステップ 1　[OS Vendor]、[OS Name]、[Version] の各ドロップダウン リストから、新しいオペレーティング システムとバージョンを選択します。

これらの値を変更するときに、ホスト プロファイルの名前を変更することもできます。ホワイト リストのグローバル ホスト プロファイルにはオペレーティング システムが関連付けられていないため、変更できないことに注意してください。

アプリケーション プロトコルを追加する方法：

アクセス：Admin

ステップ 1　「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）の指示に従ってください。

クライアントを追加する方法：

アクセス：Admin

ステップ 1　「ホスト プロファイルへのクライアントの追加」（P.27-19）の指示に従ってください。

Web アプリケーションを追加する方法：

アクセス：Admin

ステップ 1　「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20）の指示に従ってください。

プロトコルを追加する方法：

アクセス：Admin

ステップ 1　「ホスト プロファイルへのプロトコルの追加」（P.27-21）の指示に従ってください。

すべてのアプリケーション プロトコルを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Application Protocols] で、[Allow all Application Protocols] チェック ボックスをオンにします。

過去に許可したアプリケーション プロトコルを削除するまで、チェック ボックスが表示されないことに注意してください。

すべてのクライアントを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Clients] で、[Allow all Clients] チェック ボックスをオンにします。

過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。

すべての Web アプリケーションを許可する方法：

アクセス：Admin

ステップ 1　[Allowed Web Applications] で、[Allow all Web Applications] チェック ボックスをオンにします。

過去に許可した Web アプリケーションを削除するまで、チェック ボックスが表示されないことに注意してください。

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、またはプロトコルを変更する方法：

アクセス：Admin

ステップ 1　変更する要素をクリックします。

変更可能なプロパティの詳細については、以下を参照してください。

- 「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）
- 「ホスト プロファイルへのクライアントの追加」（P.27-19）
- 「ホスト プロファイルへのプロトコルの追加」（P.27-21）

注　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、またはプロトコルに加えた変更は、その要素を使用しているすべてのホスト プロファイルに反映されます。

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、またはプロトコルを削除する方法：

アクセス：Admin

ステップ 1　削除する要素の横にある削除アイコン（ ）をクリックします。

ネットワークを調査する方法：

アクセス：Admin

ステップ 1　[Survey Network] をクリックします。ネットワークを調査することで、新しく許可したクライアント、アプリケーション プロトコル、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。詳細については、「ネットワークの調査」（P.27-10）を参照してください。

既存のホスト プロファイルの削除

ライセンス：FireSIGHT

コンプライアンス ホワイト リストからホスト プロファイルを削除したら、その変更を反映させるためにホワイト リストを保存する必要があります。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ないことに注意してください。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。

削除するホスト プロファイルがアクティブな相関ポリシーで使用されている 1 つ以上のホワイト リストに属している場合は、プロファイルを削除すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

コンプライアンス ホワイト リスト ホスト プロファイルを削除する方法：

アクセス：Admin

ステップ 1　[Create White List] ページで、削除するホスト プロファイルの横にある削除アイコン（）をクリックします。

ステップ 2　プロンプトが表示されたら、ホスト プロファイルの削除を確認します。

ホスト プロファイルが削除されます。

コンプライアンス ホワイト リストの管理

ライセンス：FireSIGHT

コンプライアンス ホワイト リストは [White List] ページを使用して管理します。デフォルト ホワイト リストを含め、ホワイト リストを作成、変更、および削除することができます。作成した共有ホスト プロファイルだけでなく、組み込み共有ホスト プロファイルを編集したり、新しい共有ホスト プロファイルを追加したりすることもできます。詳細については、以下を参照してください。

- 「コンプライアンス ホワイト リストの作成」（P.27-9）
- 「コンプライアンス ホワイト リストの変更」（P.27-27）
- 「コンプライアンス ホワイト リストの削除」（P.27-27）
- 「共有ホスト プロファイルの操作」（P.27-28）

コンプライアンス ホワイト リストの変更

ライセンス：FireSIGHT

アクティブな相関ポリシーに含まれているコンプライアンス ホワイト リストを変更すると、システムがターゲット ホストを再評価します。この再評価中は、ホワイト リストがアクティブな相関ポリシーに含まれており、準拠していたホストが更新されたホワイト リストによって非準拠になった場合でも、システムがホワイト リスト イベントを**生成せず**、したがってホワイト リストに関連付けられた応答もトリガーされないことに注意してください。

既存のコンプライアンス ホワイト リストを変更する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

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。

[Create White List] ページが表示されます。

ステップ 3　必要に応じて変更を加えて、[Save White List] をクリックします。

ホワイト リストが更新されます。

コンプライアンス ホワイト リストの削除

ライセンス：FireSIGHT

1 つ以上の相関ポリシーで使用しているコンプライアンス ホワイト リストは削除できません。その前に、それが使用されているすべてのポリシーからホワイト リストを削除する必要があります。ポリシーからホワイト リストを削除する方法については、「相関ポリシーの編集」（P.39-54）を参照してください。

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ホワイト リストに関連付けられたホスト属性も削除されます。

既存のコンプライアンス ホワイト リストを削除する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　削除するホワイト リストの横にある削除アイコン（  ）をクリックします。

ホワイト リストが削除されます。

共有ホスト プロファイルの操作

ライセンス：FireSIGHT

共有ホスト プロファイルは、複数のホワイト リストに渡りターゲット 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、およびプロトコルを指定します。つまり、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。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ることに注意してください。

共有ホスト プロファイルの詳細については、「共有ホスト プロファイルについて」（P.27-6）を参照してください。

共有ホスト プロファイルは作成、変更、および削除できます。加えて、組み込み共有ホスト プロファイルを変更または削除した場合、あるいは、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または削除した場合は、それらを出荷時の初期状態にリセットできます。詳細については、以下を参照してください。

- 「共有ホスト プロファイルの作成」（P.27-28）
- 「共有ホスト プロファイルの変更」（P.27-30）
- 「共有ホスト プロファイルの削除」（P.27-32）
- 「組み込みホスト プロファイルの出荷時の初期状態へのリセット」（P.27-32）

共有ホスト プロファイルを作成したら、それを複数のホワイト リストに追加できます。詳細については、「コンプライアンス ホワイト リストへの共有ホスト プロファイルの追加」（P.27-22）を参照してください。

共有ホスト プロファイルの作成

ライセンス：FireSIGHT

1 つのホスト プロファイルを使用して、複数のホワイト リストに渡り特定のオペレーティング システムを実行しているホストを評価する場合は、共有ホスト プロファイルを作成します。

ヒント　特定のホストのホスト プロファイルを使用して、コンプライアンス ホワイト リストの共有ホスト プロファイルを作成することもできます。詳細については、「ホスト プロファイルからのホワイト リスト ホスト プロファイルの作成」（P.37-28）を参照してください。

共有ホスト プロファイルを作成する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　オプションで、ネットワークを調査します。

ネットワークを調査すると、システムがネットワークについて収集したデータに基づいていくつかのベースライン共有ホワイト リストが作成されます。これにより、複数の共有ホスト プロファイルを手動で作成して設定する手間が省けます。次の 2 つのオプションから選択できます。

- ネットワークを調査するには、[Survey Network] をクリックします。詳細については、「ネットワークの調査」（P.27-10）を参照してください。

  システムは 1 つ以上のベースライン共有ホスト プロファイルを作成します。これらの共有ホスト プロファイルは、「共有ホスト プロファイルの変更」（P.27-30）と「共有ホスト プロファイルの削除」（P.27-32）の説明に従って編集または削除できます。他に必要な共有ホスト プロファイルを追加するには、次のステップに進みます。
- ネットワークの調査を省略するには、次のステップに進みます。

ステップ 4　[Shared Host Profiles] の横にある追加アイコン（  ）をクリックします。

新しい共有ホスト プロファイルの設定が表示されます。

ステップ 5　[Name] フィールドに、共有ホスト プロファイルの分かりやすい名前を入力します。

ステップ 6　[OS Vendor]、[OS Name]、および [Version] の各ドロップダウン リストから、共有ホスト プロファイルを作成するオペレーティング システムとバージョンを選択します。

ステップ 7　許可するアプリケーション プロトコルを指定します。次の 3 つのオプションがあります。

- すべてのアプリケーション プロトコルを許可するには、[Allow all Application Protocols] チェック ボックスをオンにします。
- どのアプリケーション プロトコルも許可しない場合は、[Allow all Application Protocols] チェック ボックスをオフのままにします。
- 特定のアプリケーション プロトコルを許可するには、[Allowed Application Protocols] の横で、「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）の手順に従ってください。

ステップ 8　許可するクライアントを指定します。次の 3 つのオプションがあります。

- すべてのクライアントを許可するには、[Allow all Clients] チェック ボックスをオンにします。
- どのクライアントも許可しない場合は、[Allow all Clients] チェック ボックスをオフのままにします。
- 特定のクライアントを許可するには、「ホスト プロファイルへのクライアントの追加」（P.27-19）の指示に従ってください。

ステップ 9　許可する Web アプリケーションを指定します。次の 3 つのオプションがあります。

- すべての Web アプリケーションを許可するには、[Allow all Web Applications] チェック ボックスをオンにします。
- どの Web アプリケーションも許可しない場合は、[Allow all Web Applications] チェック ボックスをオフのままにします。
- 特定の Web アプリケーションを許可するには、「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20）の指示に従ってください。

ステップ 10　許可するプロトコルを指定します。

プロトコルを追加するには、[Allowed Protocols] の横で、「ホスト プロファイルへのプロトコルの追加」（P.27-21）の手順に従ってください。ARP、IP、TCP、および UDP は常に許可されることに注意してください。

ステップ 11　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが作成されます。これで、共有ホスト プロファイルを任意のコンプライアンス ホワイト リストに追加できるようになりました。

共有ホスト プロファイルの変更

ライセンス：FireSIGHT

共有ホスト プロファイル変更すると、それが属しているすべてのホワイト リストのプロファイルが変更されます。共有ホスト プロファイルを使用し、アクティブな相関ポリシーでも使用されているホワイト リストの場合は、共有ホスト プロファイルを変更すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

次の表に、共有ホスト プロファイルを変更するための操作の説明を示します。

表 27-2　　共有ホスト プロファイルの操作

目的	操作
ホスト プロファイルの名前を変更する	[Name] フィールドに新しい名前を記入します。
オペレーティング システムを変更する	[OS Vendor]、[OS Name]、[Version] の各ドロップダウン リストから、新しいオペレーティング システムとバージョンを選択します。これらの値を変更するときに、ホスト プロファイルの名前を変更することもできます。
アプリケーション プロトコルを追加する	「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17）の指示に従ってください。
クライアントを追加する	「ホスト プロファイルへのクライアントの追加」（P.27-19）の指示に従ってください。
Web アプリケーションを追加する	「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20）の指示に従ってください。
プロトコルを追加する	「ホスト プロファイルへのプロトコルの追加」（P.27-21）の指示に従ってください。
すべてのアプリケーション プロトコルを許可する	[Allowed Application Protocols] で、[Allow all Application Protocols] チェック ボックスをオンにします。過去に許可したアプリケーション プロトコルを削除するまで、チェック ボックスが表示されないことに注意してください。
すべてのクライアントを許可する	[Allowed Clients] で、[Allow all Clients] チェック ボックスをオンにします。過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。
すべての Web アプリケーションを許可する	[Allowed Web Applications] で、[Allow all Web Applications] チェック ボックスをオンにします。過去に許可したクライアントを削除するまで、チェック ボックスが表示されないことに注意してください。

表 27-2　共有ホスト プロファイルの操作（続き）

目的	操作
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、またはプロトコルを変更する	変更する要素をクリックします。変更可能なプロパティの詳細については、以下を参照してください。 • 「ホスト プロファイルへのアプリケーション プロトコルの追加」（P.27-17） • 「ホスト プロファイルへのクライアントの追加」（P.27-19） • 「ホスト プロファイルへの Web アプリケーションの追加」（P.27-20） • 「ホスト プロファイルへのプロトコルの追加」（P.27-21） （注）　アプリケーション プロトコル、クライアント、またはプロトコルに加えた変更は、その要素を使用しているすべてのホスト プロファイルに反映されます。
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、またはプロトコルを削除する	削除する要素の横にある削除アイコン（ ）をクリックします。
ネットワークを調査する	[Survey Network] をクリックします。ネットワークを調査すると、新しく許可したクライアント、アプリケーション プロトコル、Web アプリケーション、およびプロトコルを既存のホスト プロファイルに追加したり、初期調査で検出されなかったオペレーティング システムを実行中のホストが今回の調査で検出された場合に追加のホスト プロファイルを作成したりできます。詳細については、「ネットワークの調査」（P.27-10）を参照してください。

共有ホスト プロファイルを変更する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　組み込み共有ホスト プロファイルのいずれかを編集しますか。

- はいの場合は、[Built-in Host Profiles] を展開してそれらのホスト プロファイルを表示します。
- いいえの場合は、次のステップに進みます。

ステップ 4　変更する共有ホスト プロファイルの名前をクリックします。

ホスト プロファイルが表示されます。

ステップ 5　「共有ホスト プロファイルの操作」の表に記載されている操作のいずれかを実行します。

ステップ 6　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが保存されます。

共有ホスト プロファイルの削除

ライセンス：FireSIGHT

削除する共有ホスト プロファイルがアクティブな相関ポリシーで使用されている 1 つ以上のホワイト リストに属している場合は、プロファイルを削除すると、ホストが非準拠に移行する場合がありますが、ホワイト リスト イベントは**生成されません**。

ヒント　デフォルト ホワイト リストで使用されている組み込み共有ホスト プロファイルを削除した場合は、組み込みプロファイルを出荷時の初期状態にリセットすることによって、それを復元できます。詳細については、「組み込みホスト プロファイルの出荷時の初期状態へのリセット」（P.27-32）を参照してください。

共有ホスト プロファイルを削除する方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　組み込み共有ホスト プロファイルのいずれかを削除しますか。

- はいの場合は、[Built-in Host Profiles] を展開してそれらのホスト プロファイルを表示します。
- いいえの場合は、次のステップに進みます。

ステップ 4　削除する共有ホスト プロファイルの横にある削除アイコン（ ）をクリックします。

共有ホスト プロファイルの削除を確認します。

ステップ 5　[Save all Profiles] をクリックして変更を保存します。

共有ホスト プロファイルが削除され、それを使用しているすべてのコンプライアンス ホワイト リストから除外されます。

組み込みホスト プロファイルの出荷時の初期状態へのリセット

ライセンス：FireSIGHT

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。組み込みホスト プロファイルでは、組み込みアプリケーション プロトコル、プロトコル、およびクライアントが使用されます。これらの要素は、デフォルト ホワイト リストおよびユーザが作成したカスタム ホワイト リストの両方でそのまま使用することも、ニーズに合わせて変更することもできます。詳細については、共有ホスト プロファイルについてを参照してください。

組み込みプロファイル、アプリケーション プロトコル、プロトコル、Web アプリケーション、またはクライアント加えた変更を元に戻す必要がある場合は、出荷時の初期状態にリセットすることができます。出荷時の初期状態にリセットすると、次の現象が発生します。

- 変更した組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントの**すべて**が出荷時の初期状態にリセットされます。
- 削除した組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントの**すべて**が復元されます。
- アクティブな相関ポリシーで使用されているホワイト リスト（デフォルト ホワイト リストを含む）と、リセットした組み込みホスト プロファイル、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のいずれかを使用していたホワイト リストの**すべて**が再評価されます。この再評価で一部のホストが準拠に移行される場合がありますが、ホワイト リスト イベントは生成されません。

組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントをリセットする方法：

アクセス：Admin

ステップ 1　[Policies] > [Correlation] の順に選択してから、[White List] をクリックします。

[White List] ページが表示されます。

ステップ 2　[Edit Shared Profiles] をクリックします。

[Edit Shared Profiles] ページが表示されます。

ステップ 3　[Built-in Host Profiles] をクリックします。

[Built-in Host Profiles] ページが表示されます。

ステップ 4　[Reset to Factory Defaults] をクリックします。

ステップ 5　[OK] をクリックすることによって、出荷時の初期状態へのリセットを確認します。

組み込みホスト プロファイル、アプリケーション プロトコル、プロトコル、およびクライアントのすべてが出荷時の初期状態にリセットされます。アクティブな相関ポリシーで使用されているホワイト リストと、リセットした組み込みホスト プロファイル、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使用していたホワイト リストがすべて再評価されます。

ホワイト リスト イベントの操作

ライセンス：FireSIGHT

ホストがアクティブな相関ポリシーに含まれているホワイト リストに準拠していないことを示す検出イベントをシステムが生成すると、ホワイト リスト イベントが生成されます。ホワイト リスト イベントは、相関イベントの特殊な形態で、相関イベント データベースに記録されます。ホワイト リスト イベントは検索、表示、および削除することができます。

ヒント　データベースに保存されるイベント数の設定方法については、「データベース イベント制限の設定」（P.50-15）を参照してください。ホワイト リスト イベントは相関イベント データベースに保存されることに注意してください。

詳細については、次の項を参照してください。

- 「ホワイト リスト イベントの表示」（P.27-34）
- 「ホワイト リスト イベント テーブルについて」（P.27-36）
- 「コンプライアンス ホワイト リスト イベントの検索」（P.27-37）

ホワイト リスト イベントの表示

ライセンス：FireSIGHT

防御センターを使用して、コンプライアンス ホワイト リスト イベントのテーブルを表示できます。その後で、探している情報に合わせてイベント ビューを操作できます。

ホワイト リスト イベントにアクセスしたときに表示されるページは使用しているワークフローによって異なります。ホワイト リスト イベントのテーブル ビューを含む事前定義のワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、「カスタム ワークフローの作成」（P.47-45）を参照してください。

次の表に、ホワイト リスト イベント ワークフロー ページで実行可能な特定の操作の説明を示します。

表 27-3　コンプライアンス ホワイト リスト イベントの操作

目的	操作
ホストのホスト プロファイルを表示する	IP アドレスの横に表示されたホスト プロファイル アイコン（  ）をクリックします。
ユーザ プロファイル情報を表示する	ユーザ ID の横に表示されたユーザ アイコン（  ）をクリックします。詳細については、「ユーザの詳細とホストの履歴について」（P.38-65）を参照してください。
現在のワークフロー ページでイベントをソートしたり、制限したりする	「ドリルダウン ワークフロー ページのソート」（P.47-39）で詳細を参照してください。
現在のワークフロー ページ内で移動する	「ワークフロー内の他のページへのナビゲート」（P.47-40）で詳細を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、「ワークフローのページの使用」（P.47-21）を参照してください。
表示された列の詳細を表示する	「ホワイト リスト イベント テーブルについて」（P.27-36）で詳細を参照してください。
表示されたイベントの時刻と日付の範囲を変更する	「イベント時間の制約の設定」（P.47-27）で詳細を参照してください。

表 27-3　コンプライアンス ホワイト リスト イベントの操作（続き）

目的	操作
特定の値に制限して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。 • 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェック ボックスをオンにしてから、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
システムからホワイト リスト イベントを削除する	次のいずれかの方法を使用します。 • 特定のイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにしてから、[Delete] をクリックします。 • 現在の制限ビュー内のすべてのイベントを削除するには、[Delete All] をクリックしてから、すべてのイベントを削除することを確認します。
他のイベント ビューに移動して関連イベントを表示する	「ワークフロー間のナビゲート」（P.47-41）で詳細を参照してください。

コンプライアンス ホワイト リスト イベントを表示する方法：

アクセス：Admin/Any Security Analyst/Discovery Admin

ステップ 1　[Analysis] > [Correlation] > [White List Events] の順に選択します。

デフォルト ホワイト リスト イベント ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。「イベント時間の制約の設定」（P.47-27）を参照してください。

ホワイト リスト イベント テーブルについて

ライセンス：FireSIGHT

相関ポリシー機能を使用して*相関ポリシー*を作成し、システムがネットワーク上の脅威にリアルタイムに対処するように設定できます。相関ポリシーには、コンプライアンス ホワイト リスト違反を含む、ポリシー違反を構成する活動の種類が記載されます。相関ポリシーの詳細については、「相関ポリシーおよび相関ルールの設定」（P.39-1）を参照してください。

コンプライアンス ホワイト リストの違反があると、ホワイト リスト イベントが生成されます。ホワイト リスト イベント テーブル内のフィールドの説明を次の表に示します。

表 27-4　コンプライアンス ホワイト リスト イベントのフィールド

フィールド	説明
Time	ホワイト リスト イベントが生成された日時。
IP Address	非準拠ホストの IP アドレス。
User	非準拠ホストにログインしている既知のユーザの ID。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたポート（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

Description	ホワイト リスト違反の説明。次に例を示します。
	`Client "AOL Instant Messenger" is not allowed.`
	アプリケーション プロトコルに関係する違反は、アプリケーション プロトコルの名前とバージョンだけでなく、それが使用しているポートとプロトコル（TCP または UDP）も示します。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。
	`Server "ssh / 22 TCP ( OpenSSH 3.6.1p2 )" is not allowed on Operating System "Linux Linux 2.4 or 2.6".`

Policy	違反した相関ポリシー、つまりホワイト リストを含む相関ポリシーの名前。
White List	ホワイト リストの名前。
Priority	ポリシーまたはポリシー違反をトリガーしたホワイト リストで指定された優先度。相関ルールとポリシーの優先度の設定方法については、「ポリシーの基本情報の指定」（P.39-49）と「ルールおよびホワイトリストのプライオリティの設定」（P.39-50）を参照してください。
Host Criticality	ホワイト リストに準拠していないホストに対してユーザが割り当てたホスト重要度（[None]、[Low]、[Medium]、または [High]）。 ホスト重要度の詳細については、「事前定義のホスト属性の使用」（P.37-35）を参照してください。
Device	ホワイト リスト違反を検出した管理対象デバイスの名前。
Count	各行に表示された情報と一致するイベントの数。[Count] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

コンプライアンス ホワイト リスト イベントの検索

ライセンス：FireSIGHT

特定のコンプライアンス ホワイト リスト イベントを検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成して保存しておけば、後で再利用することができます。次の表に、使用可能な検索基準の説明を示します。

表 27-5　コンプライアンス ホワイト リスト イベントの検索基準

フィールド	検索基準ルール
Policy	相関ポリシーに含まれるホワイト リストの違反によって引き起こされたすべてのイベントを返す相関ポリシーの名前を入力します。
White List	ホワイト リストの違反によって引き起こされたすべてのイベントを返すホワイト リストの名前を入力します。
Description	ホワイト リスト イベントの説明を入力します。
Priority	相関ポリシー内のホワイト リストの優先度または相関ポリシー自体の優先度によって決定されるホワイト リスト イベントの優先度を指定します。ホワイト リストの優先度のほうがそのポリシーの優先度より優先されることに注意してください。優先度がない場合は、「none」と入力します。 相関ルールとポリシーの優先度の設定方法については、「ポリシーの基本情報の指定」（P.39-49）と「ルールおよびホワイトリストのプライオリティの設定」（P.39-50）を参照してください。
IP Address	ホワイト リストに非準拠になったホストの IP アドレスを指定します。
User	ホワイト リストに非準拠になったホストにログインしていたユーザの ID を指定します。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたポート（存在する場合）を指定します。
Host Criticality	ホワイト リスト イベントに関係するソース ホストのホスト重要度（[None]、[Low]、[Medium]、または [High]）を指定します。ホスト重要度の詳細については、「事前定義のホスト属性の使用」（P.37-35）を参照してください。
Device	ホワイト リスト違反を検出したデバイスまたはデバイス グループの名前を入力します。

コンプライアンス ホワイト リスト イベントを検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] の順に選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[White List Events] を選択します。

ページが適切な制約を使用してリロードされます。

ステップ 3　オプションで、検索を保存する場合は、[Name] フィールドに検索の名前を入力します。

名前を入力しなかった場合は、検索を保存するときに自動的に名前が付けられます。

ステップ 4　「コンプライアンス ホワイト リスト イベントの検索基準」の表の説明に従って、該当するフィールドに検索基準を入力します。このとき、次の点に留意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドでカンマ区切りの列挙を使用できます。複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 検索基準としてオブジェクトを使用する場合は、検索フィールドの横に表示されたオブジェクト追加アイコン（  ）をクリックします。

検索でのオブジェクトの使用を含む検索構文の詳細については、「イベントの検索」（P.45-1）を参照してください。

ステップ 5　検索を保存して他のユーザがアクセスできるようにするには、[Save As Private] チェック ボックスをオフにします。そうではなく、検索をプライベートとして保存するには、このチェック ボックスをオンのままにします。

カスタム ユーザ ロールに対するデータ制限として検索を使用する場合は、プライベート検索として保存する**必要があります**。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[Search] ボタンをクリックします。

  デフォルト ホワイト リスト イベント ワークフローに、現在の時刻範囲に制限された検索結果が表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。
- 既存の検索を変更して、その変更を保存する場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できます。

ホワイト リスト違反の処理

ライセンス：FireSIGHT

システムは、ネットワーク上のホストがアクティブな相関ポリシー内のコンプライアンス ホワイト リストにどのように違反しているかを追跡します。これらのレコードを検索して表示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。

- 「ホワイト リスト違反の表示」（P.27-39）
- 「ホワイト リスト違反テーブルについて」（P.27-40）
- 「ホワイト リスト違反の検索」（P.27-42）

ホワイト リスト違反の表示

ライセンス：FireSIGHT

防御センターを使用して、ホワイト リスト違反のテーブルを表示できます。その後で、探している情報に合わせてイベント ビューを操作できます。ホワイト リスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。次の 2 つの事前定義ワークフローが用意されています。

- ホスト違反カウント ワークフローには、1 つ以上のホワイト リストに違反したすべてのホストが一覧表示された一連のページが示されます。最初のページでは、ホストがホストあたりの違反数に基づいてソートされ、違反数が最大のホストがリストの先頭に表示されます。ホストが複数のホワイト リストに違反している場合は、違反しているホワイト リストごとに別の行が表示されます。ワークフローには、最近検出された違反を先頭に、すべての違反を一覧表示するホワイト リスト違反のテーブル ビューも含まれています。テーブル内の各行に 1 つずつ検出された違反が示されます。
- ホワイト リスト違反ワークフローには、最近検出された違反を先頭に、すべての違反を一覧表示するホワイト リスト違反のテーブル ビューが含まれています。テーブル内の各行に 1 つずつ検出された違反が示されます。

両方の事前定義ワークフローが、制限を満たすすべてのホストのホスト プロファイルを含むホスト ビューで終わります。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。詳細については、「カスタム ワークフローの作成」（P.47-45）を参照してください。

次の表に、ホワイト リスト違反ワークフロー ページで実行可能な特定の操作の説明を示します。

表 27-6　コンプライアンス ホワイト リスト違反の操作

目的	操作
ホストのホスト プロファイルを表示する	IP アドレスの横に表示されたホスト プロファイル アイコン（  ）をクリックします。
現在のワークフロー ページでイベントをソートしたり、制限したりする	「ドリルダウン ワークフロー ページのソート」（P.47-39）で詳細を参照してください。
現在のワークフロー ページ内で移動する	「ワークフロー内の他のページへのナビゲート」（P.47-40）で詳細を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、「ワークフローのページの使用」（P.47-21）を参照してください。
表示された列の詳細を表示する	「ホワイト リスト違反テーブルについて」（P.27-40）で詳細を参照してください。

表 27-6　コンプライアンス ホワイト リスト違反の操作（続き）

目的	操作
ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。ドリルダウンされません。 • いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示させるイベントの横のチェック ボックスを選択し、[View] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[View All] をクリックします。 ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、「イベントの制約」（P.47-36）を参照してください。
他のイベント ビューに移動して関連イベントを表示する	「ワークフロー間のナビゲート」（P.47-41）で詳細を参照してください。

コンプライアンス ホワイト リスト違反を表示する方法：

アクセス：Admin/Any Security Analyst/Discovery Admin

ステップ 1　[Analysis] > [Correlation] > [White List Violations] の順に選択します。

デフォルト ホワイト リスト違反ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。

ホワイト リスト違反テーブルについて

ライセンス：FireSIGHT

相関ポリシー機能を使用して*相関ポリシー*を作成し、システムがネットワーク上の脅威にリアルタイムに対処するように設定できます。相関ポリシーには、コンプライアンス ホワイト リスト違反を含む、ポリシー違反を構成する活動の種類が記載されます。相関ポリシーの詳細については、「相関ポリシーおよび相関ルールの設定」（P.39-1）を参照してください。

コンプライアンス ホワイト リストに違反すると、その違反が記録されます。テーブル ビューにはネットワーク上の現在のホスト違反しか表示されないため、イベント時間制限をテーブル ビューに設定できないことに注意してください。ホワイト リスト違反テーブル内のフィールドの説明を次の表に示します。

表 27-7　コンプライアンス ホワイト リスト違反のフィールド

フィールド	説明
Time	ホワイト リスト違反が検出された日時。
IP Address	非準拠ホストの関連 IP アドレス。
Type	ホワイト リスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。 • オペレーティング システム（os） • アプリケーション プロトコル（server） • クライアント（client） • プロトコル（protocol） • Web アプリケーション（web）
Information	ホワイト リスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。 たとえば、Microsoft Windows ホストのみを許可するホワイト リストを使用している場合は、[Information] フィールドに、Microsoft Windows を実行していないホストのオペレーティング システムが示されます。 ホワイト リストに違反するプロトコルの場合は、[Information] フィールドに、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらなのかも示されます。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたポート（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。
Protocol	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられたプロトコル（存在する場合）他のタイプのホワイト リスト違反の場合、このフィールドは空白です。
White List	違反されたホワイト リストの名前。
Count	各行に表示された情報と一致するイベントの数。[Count] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

ホワイト リスト違反の検索

ライセンス：FireSIGHT

特定のコンプライアンス ホワイト リスト違反を検索できます。ネットワーク環境に合わせてカスタマイズした検索を作成して保存しておけば、後で再利用することができます。次の表に、使用可能な検索基準の説明を示します。

表 27-8　コンプライアンス ホワイト リスト違反の検索基準

フィールド	検索基準ルール
Time	ホワイト リストが違反された日時を指定します。
IP Address	ホワイト リストに非準拠になったホストの IP アドレスを指定します。
White List	そのホワイト リストのすべての違反を返すホワイト リストの名前を入力します。
Type	ホワイト リスト違反のタイプを入力します。 • オペレーティング システムに基づいて違反を検索する場合は、「os」（または「operating system」）と入力します。 • アプリケーション プロトコルに基づいて違反を検索する場合は、「server」と入力します。 • クライアントに基づいて違反を検索する場合は、「client」と入力します。 • プロトコルに基づいて違反を検索する場合は、「protocol」と入力します。 • Web アプリケーションに基づいて違反を検索する場合は、「web application」と入力します。
Information	ホワイト リスト違反情報を入力します。
Port	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたポート（存在する場合）を指定します。
Protocol	アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられたプロトコル（存在する場合）を指定します。

コンプライアンス ホワイト リスト違反を検索する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　[Analysis] > [Search] の順に選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[White List Violations] を選択します。

ページが適切な制約を使用してリロードされます。

ステップ 3　オプションで、検索を保存する場合は、[Name] フィールドに検索の名前を入力します。

名前を入力しなかった場合は、検索を保存するときに自動的に名前が付けられます。

ステップ 4　「コンプライアンス ホワイト リスト イベントの検索基準」の表の説明に従って、該当するフィールドに検索基準を入力します。このとき、次の点に留意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドでカンマ区切りの列挙を使用できます。複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 検索基準としてオブジェクトを使用する場合は、検索フィールドの横に表示されたオブジェクト追加アイコン（  ）をクリックします。

検索でのオブジェクトの使用を含む検索構文の詳細については、「イベントの検索」（P.45-1）を参照してください。

ステップ 5　検索を保存して他のユーザがアクセスできるようにするには、[Save As Private] チェック ボックスをオフにします。そうではなく、検索をプライベートとして保存するには、このチェック ボックスをオンのままにします。

カスタム ユーザ ロールに対するデータ制限として検索を使用する場合は、プライベート検索として保存する**必要があります**。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[Search] ボタンをクリックします。

  検索結果がデフォルト ホワイト リスト違反ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、ワークフロー タイトルのそばにある [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。
- 既存の検索を変更して、その変更を保存する場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できます。