CHAPTER 13

グローバル相関の設定

（注） IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、グローバル相関の設定について説明します。内容は次のとおりです。

グローバル相関について

センサーが悪意のあるアクティビティのレピュテーションを持つネットワーク デバイスを認識し、それらのアクティビティに対処できるようにグローバル相関を設定できます。シスコの中央脅威データベースである SensorBase ネットワーク に IPS デバイスを加えることにより、グローバル相関更新を受信して取り込むことができます。グローバル相関更新に含まれているレピュテーション データは、ネットワーク トラフィックの分析に組み込まれます。これにより、トラフィックが送信元 IP アドレスのレピュテーションに基づいて拒否または許可されるため、IPS の有効性が高まります。参加している IPS デバイスは、Cisco SensorBase ネットワークにデータを送信して戻します。これにより、最新かつグローバルな更新を維持するフィードバック ループがもたらされます。

センサーを、グローバル相関更新やテレメトリ データの送信に参加するように設定することもできますし、これらのサービスをオフにすることもできます。完全な参加を選択した場合、IBNP がリストを共有しておらず、SensorBase ネットワークへのデータ提供を継続しながらネットワークに関する機密情報を保護できるときには、特定の IP アドレスを除外できます。イベントのレピュテーション スコアを表示したり、攻撃者のレピュテーション スコアを参照したりできます。レピュテーション スコアに基づいてイベントをフィルタし、その結果を基にしてレポートを生成できます。

SensorBase ネットワークへの参加

Cisco IPS には、新しいセキュリティ機能である Cisco グローバル相関が実装されました。この機能では、シスコが長年にわたって蓄積してきた優れたセキュリティ インテリジェンスを駆使しています。Cisco IPS は定期的な間隔で Cisco SensorBase ネットワークから脅威の更新を受信します。これには、インターネット上の既知の脅威（常習的な攻撃者、Botnet ハーベスタ、悪意のあるソフトウェアの大発生、ダーク ネットなど）に関する詳細な情報が含まれています。重要な資産への攻撃の機会をつかまれる前に、IPS はこの情報を使用してフィルタリングによって悪質な攻撃者を除外します。そして、グローバルな脅威データをシステムに組み込み、早期に悪意のあるアクティビティを防止します。

SensorBase ネットワークへの参加に同意した場合は、IPS 宛てに送信されたトラフィックに関する集約された統計情報がシスコによって収集されます。この情報には、Cisco IPS ネットワーク トラフィック プロパティに関する要約データと、このトラフィックがシスコのアプライアンスでどのように処理されたかに関する情報が含まれます。トラフィックのデータ コンテンツおよびその他の企業秘密情報および個人情報の収集は行いません。すべてのデータは集約され、定期的な間隔でセキュリティ保護された HTTP によって Cisco SensorBase ネットワーク サーバに送信されます。シスコで共有されるすべてのデータは匿名とされ、機密情報として扱われます。

表 13-1 に、シスコでのデータの使用法を示します。

表 13-1　シスコによるネットワーク参加データの使用

参加レベル	データのタイプ	目的
Partial	プロトコル属性 (TCP 最大セグメント サイズおよびオプション ストリングなど)	潜在的脅威を追跡し、脅威による影響をシスコが理解するのに役立ちます
	攻撃タイプ (開始されたシグニチャおよびリスク レーティングなど)	現在の攻撃および攻撃の重大度を理解するために使用されます
	接続している IP アドレスおよびポート	攻撃元を特定します
	IPS パフォーマンスの概要 (CPU 使用率、メモリの使用状況、インライン モードと無差別モードなど)	製品の有効性を追跡します
Full	攻撃対象の IP アドレスおよびポート	脅威の動作パターンを検出します

部分的（[Partial]）または完全（[Full]）なネットワーク参加をイネーブルにすると、[Network Participation Disclaimer] が表示されます。参加するには、[Agree] をクリックします。ライセンスをインストールしていない場合は、センサーのライセンスが供与されるまでグローバル相関インスペクションとレピュテーション フィルタリングがディセーブルになることを知らせる警告が表示されます。ライセンスは http://www.cisco.com/go/license で取得できます。

詳細情報

センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。

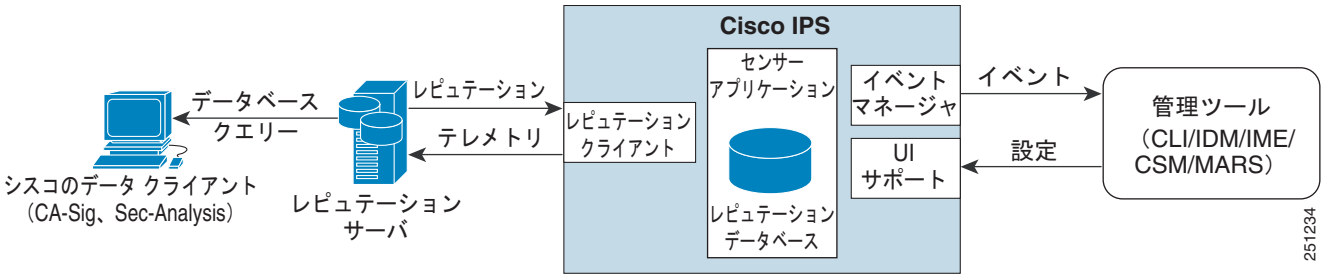
レピュテーションについて

レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。レピュテーションを使用すると、インストール ベースの IPS センサーは、既存のネットワーク インフラストラクチャと協力してコラボレーションを行うことができるようになります。レピュテーションのあるネットワーク デバイスは、ほとんどが悪意のあるネットワーク デバイスまたは感染した可能性があるネットワーク デバイスです。レピュテーション情報と統計情報は IME で表示できます。

IPS センサーはグローバル相関サーバ（別名レピュテーション サーバ）とのコラボレーションを行い、センサーの有効性を高めます。

図 13-1 に、センサーのロールとグローバル相関サーバを示します。

図 13-1　IPS 管理およびグローバル相関サーバとのやり取り



グローバル相関サーバは悪意のあるホストまたは感染したホストを特定できる可能性のある IP アドレスについて、センサーに情報を提供します。センサーはこの情報を使用して、実行するアクションを決定し（該当する場合）、既知のレピュテーションのあるホストから潜在的に有害なトラフィックを受け取るとそれを実行します。グローバル相関データベースは急速に変化するため、センサーはグローバル相関サーバから定期的にグローバル相関更新をダウンロードする必要があります。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

詳細情報

- グローバル相関の統計情報表示の詳細については、「統計情報の表示」（P.19-31）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

ネットワーク参加について

ネットワーク参加によって、ほぼリアルタイムのデータを世界中のセンターから収集できます。カスタマー サイトにインストールされているセンサーは、SensorBase ネットワークにデータを送信できます。これらのデータは、グローバル相関データベースに提供されるため、レピュテーションの忠実度が高まります。センサーと SensorBase ネットワーク間の通信には、TCP/IP を介した HTTPS 要求および応答が含まれます。

ネットワーク参加により、次のデータが収集されます。

- シグニチャ ID
- 攻撃者の IP アドレス
- 攻撃者のポート
- 最大セグメント サイズ

- 攻撃対象者の IP アドレス
- 攻撃対象者のポート
- シグニチャのバージョン
- TCP オプション ストリング
- レピュテーション スコア
- リスク レーティング

ネットワーク参加の統計情報には、警告のヒットとミス、レピュテーション アクション、拒否されたパケットのカウンタが示されます。

ネットワーク参加には、3 つのモードがあります。

- オフ：ネットワーク参加サーバは、データの収集、統計情報の追跡、または Cisco SensorBase ネットワークへの接続試行は行いません。
- 部分的な参加：ネットワーク参加サーバは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。
- 完全参加：ネットワーク参加サーバは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。ネットワーク参加データから除外した IP アドレスを除き、収集されたすべてのデータが送信されます。

ネットワーク参加を行うには、インターネットへのネットワーク接続が必要です。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

詳細情報

- グローバル相関の詳細については、「ネットワーク参加の設定」（P.13-11）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

有効性について

IPS クライアントの参加により取得したデータと脅威に関する既知の資料を併用することで、IPS の有効性が高まります。シスコでは、次の使用に基づいて有効性を評価します。

- 実行可能なイベントの偽陽性（パーセンテージ）
- 実行可能なイベントにはならない脅威の偽陰性（パーセンテージ）
- すべてのイベントの実行可能なイベント（パーセンテージ）

IPS シグニチャ チームは、このデータを使用してシグニチャの忠実度を改善します。IPS エンジニアリング チームは、このデータを使用してさまざまなタイプのセンサーの配置について理解を深めます。

詳細情報

レピュテーションとリスク レーティングの詳細については、「レピュテーションとリスク レーティング」（P.13-6）を参照してください。

レピュテーションとリスク レーティング

リスク レーティングは、ネットワーク イベントに悪意があるかどうかの蓋然性の概念を示します。ネットワーク上で特定のイベントに関連するリスクの数値定量化を割り当てます。デフォルトでは、リスク レーティングが極端に高い警告が表示されると、トラフィックはシャットダウンされます。レピュテーションは、既知のアクティビティに基づいて、特定の攻撃者の IP アドレスから悪意のある動作が開始される可能性を示します。このレピュテーションについてのスコアがアラーム チャネルによって算出され、リスク レーティングに加算されます。このようにして、IPS の有効性が改善されていきます。悪いレピュテーション スコアを持つ攻撃者が認識されると、リスクがリスク レーティングに増分的に加算され、アグレッシブにされます。

アラーム チャネルは、データ パスからのシグニチャ イベントを処理します。このアラート処理装置は、各種集約技術、アクション オーバーライド、アクション フィルタ、攻撃者のレピュテーション、アクションごとのカスタム処理方法を備えています。ピュテーション参加クライアントから得た大量のレピュテーション データを使用して、アラーム チャネルで攻撃者のスコアを設定し、このスコアを使用してリスク レーティングとアラートのアクションを決定します。

詳細情報

- リスク レーティングの詳細については、「リスク レーティングの計算」（P.11-3）を参照してください。
- 脅威レーティングの詳細については、「脅威レーティングの概要」（P.11-4）を参照してください。
- イベント アクション フィルタの詳細については、「イベント アクション フィルタの概要」（P.11-5）を参照してください。
- アラーム チャネルの詳細については、「SensorApp について」（P.A-22）を参照してください。
- イベント アクション集約の詳細については、「イベント アクションの集約」（P.11-6）を参照してください。

グローバル相関機能と目的

グローバル相関には、次の 3 つの主要機能があります。

- グローバル相関インスペクション：攻撃者に関するグローバル相関レピュテーション ナレッジに基づいてアラート処理を変更します。また、センサー上で悪いスコアを持つ攻撃者が認識されると、その攻撃者によるアクションを拒否します。
- レピュテーション フィルタリング：悪意のある既知のサイトからのパケットに対して自動拒否アクションを適用します。
- ネットワーク レピュテーション：センサーはアラートおよび TCP フィンガープリント データを SensorBase ネットワークに送信します。

グローバル相関には、次の目的があります。

- アラートをインテリジェントに処理することにより、有効性を高める。

- 悪意のある既知のサイトに対する保護を強化する。
- テレメトリ データを SensorBase ネットワークと共有して、アラートおよびセンサー アクションの可視性をグローバル規模で向上する。
- 設定を簡素化する。
- 情報のアップロードおよびダウンロードを自動的に処理する。

グローバル相関の要件

グローバル相関には、次の要件があります。

- 有効なライセンス

  グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

- ネットワーク参加の免責事項への同意
- センサーおよび DNS サーバの外部接続

  Cisco IPS のグローバル相関機能では、センサーが Cisco SensorBase ネットワークに接続する必要があります。これらの機能が動作するには、ドメイン名解決も必要となります。DNS クライアントが稼動している HTTP プロキシ サーバを介して接続するようにセンサーを設定するか、またはセンサーの管理インターフェイスにルーティング可能なインターネット アドレスを割り当て、DNS サーバを使用するようにセンサーを設定できます。Cisco IPS では、HTTP プロキシと DNS サーバはグローバル相関機能でのみ使用されます。

  （注） slow コマンドと制御接続を使用して環境に配置されたセンサーは、グローバル相関更新のダウンロードが遅くなります。

- IPv6 アドレスはサポートされない

  グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

- インライン モードのセンサー

  センサーは、インライン モードで動作する必要があります。これにより、グローバル相関機能でインライン拒否アクションを使用できるようになり、その有効性が高まります。

- グローバル相関機能をサポートするセンサー

  （注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

- グローバル相関機能をサポートする IPS バージョン

  （注） IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

詳細情報

- センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。
- ネットワーク参加の免責事項の詳細については、「SensorBase ネットワークへの参加」（P.13-2）を参照してください。
- グローバル相関をサポートする DNS または HTTP プロキシ サーバ設定の詳細については、「ネットワークの設定」（P.6-2）を参照してください。
- グローバル相関のトラブルシューティングの詳細については、「グローバル相関のトラブルシューティング」（P.13-13）を参照してください。

グローバル相関のセンサー ヘルス状態メトリックについて

グローバル相関では、センサー ヘルス モニタに次のメトリックが追加されました。

- 緑色は、最後の更新が成功したことを示します。
- 黄色は、過去 86,400 秒以内に成功した更新はないことを示します。
- 赤色は、過去 3 日（259,200 秒）以内に成功した更新はないことを示します。

ネットワーク参加では、センサー ヘルス モニタに次のメトリックが追加されました。

- 緑色は、最後の接続が成功したことを示します。
- 黄色は、連続して失敗した接続（6 回未満）があることを示します。
- 赤色は、連続して失敗した接続（6 回超）があることを示します。

メトリックは、[Sensor Health] ガジェットと [Global Correlation Health] ガジェットで表示できます。

（注） グローバル相関のヘルス状態ステータスはデフォルトで赤色に設定され、グローバル相関更新が成功すると緑色に変更されます。グローバル相関更新を成功させるには、DNS サーバまたは HTTP プロキシ サーバが必要です。DNS と HTTP プロキシ サーバの設定機能は IPS 7.0(1)E3 から実装されたため、7.0(1)E3 以降にアップグレードした場合は未設定の状態になっています。このため、グローバル相関ヘルス状態および全般的なセンサー ヘルス状態ステータスは、センサーで DNS または HTTP プロキシ サーバを設定するまで、赤色になります。DNS または HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合は、グローバル相関をディセーブルにし、グローバル相関ヘルス状態ステータスを含まないようにセンサー ヘルス状態ステータスを設定することで、赤色のグローバル相関ヘルス状態と全般的なセンサー ヘルス状態ステータスに対処できます。

詳細情報

- センサー ヘルス状態メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関をディセーブルにする手順については、「グローバル相関のディセーブル化」（P.13-13）を参照してください。
- [Sensor Health] ガジェットおよび [Global Correlation Health] ガジェットの詳細については、「IME ガジェット」（P.3-2）を参照してください。

グローバル相関インスペクションおよびレピュテーションの設定

ここでは、グローバル相関インスペクションおよびレピュテーションを設定する方法について説明します。内容は次のとおりです。

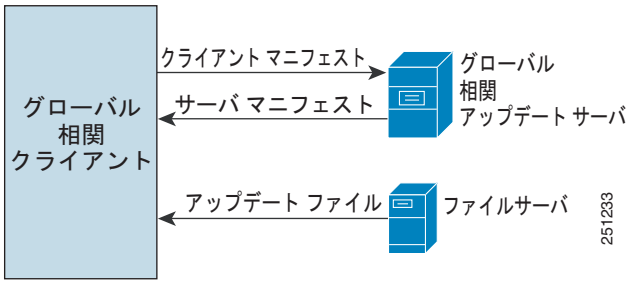
[Inspection/Reputation] ペイン

（注）　インスペクション/レピュテーションを設定するには、管理者権限またはオペレータ権限が必要です。

[Inspection/Reputation] ペインで、SensorBase ネットワークからの更新を使用してセンサーを設定し、リスク レーティングを調整できます。クライアントは、グローバル相関アップデート サーバおよびファイル サーバと通信することで、センサーに適用可能な利用できる更新を判断します。グローバル相関アップデート サーバは、センサーにサーバ マニフェスト ドキュメントを提供します。このドキュメントによって、使用可能な更新、およびファイル サーバからそれらを取得する方法が特定されます。センサーは、サーバ マニフェストの情報を使用して、ファイル サーバから更新ファイルをダウンロードします。

図 13-2 に、グローバル相関アップデート クライアントがファイルを取得する方法を示します。

図 13-2　　グローバル相関アップデート クライアント



注意　グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

グローバル相関を設定すると、更新は自動的に定期的な間隔で行われます。デフォルトの間隔は約 5 分ですが、この間隔はグローバル相関サーバで変更できます。センサーは、完全な更新を取得し、その後は定期的に差分更新を適用します。

HTTP プロキシまたは DNS サーバの設定は、[Network] ペインで行います。グローバル相関をオンにしている場合は、悪意のあるホストに対してどれだけ積極的に拒否アクションを実施するかを選択できます。次に、悪意のある既知のホストへのアクセスを拒否するために、レピュテーション フィルタリ

ングをイネーブルにします。発生する可能性があった内容に関するレポートだけが必要な場合は、[Test Global Correlation] をイネーブルにします。これにより、センサーは監査モードに設定され、センサーが実行したと想定されるアクションがイベント内に生成されます。

[Sensor Health] ガジェットでグローバル相関のステータスを表示するには、[Details] をクリックします。グローバル相関のステータスには、[Normal]、[Needs Attention]、または [Critical] が表示されます。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

[Inspection/Reputation] ペインのフィールド定義

[Inspection/Reputation] ペインには次のフィールドがあります。

- [Global Correlation Inspection]：グローバル相関をオフまたはオンにします。オンの場合、センサーは、SensorBase ネットワークからの更新を使用して、リスク レーティングを調整します。デフォルトはオフです。センサーが拒否アクションを開始する場合にどれだけ積極的にグローバル相関情報を使用するかを指定する 3 つのモードがあります。
  - [Permissive]：拒否アクションに対する影響は最も少なくなります。
  - [Standard]：拒否アクションに対する影響は中程度です。
  - [Aggressive]：拒否アクションに対する影響は非常に大きくなります。
- [Reputation Filtering]：レピュテーション フィルタリングをオンまたはオフにできます。オンの場合、センサーは、グローバル相関データベースにリストされている悪意のあるホストへのアクセスを拒否します。デフォルトはオフです。
- [Test Global Correlation]：グローバル相関の影響を受ける拒否アクションのレポートをイネーブルにします。実際にホストを拒否することなく、グローバル相関機能をテストできます。

詳細情報

- センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。
- センサー ヘルス状態メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定

グローバル相関インスペクションおよびレピュテーション フィルタリングを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Global Correlation] > [Inspection/Reputation] を選択します。

ステップ 3　グローバル相関インスペクションおよびレピュテーション フィルタリングをオンにするには、[On] オプション ボタンをクリックします。グローバル相関インスペクションおよびレピュテーション フィルタリングはデフォルトでオフになっています。

ステップ 4　ドロップダウン リストから、センサーが拒否アクションを開始する場合にグローバル相関情報を使用する程度を選択します。

- [Permissive]：拒否アクションに対する影響は最も少なくなります。
- [Standard]：拒否アクションに対する影響は中程度です。
- [Aggressive]：拒否アクションに対する影響は非常に大きくなります。

ステップ 5　レピュテーション フィルタリングをオンにするには、[On] オプション ボタンをクリックします。レピュテーション フィルタリングはデフォルトでオフになっています。

ステップ 6　トラフィックを拒否するかどうかについてグローバル相関に影響せずにグローバル相関のテストを実行するには、[Test Global Correlation] チェックボックスをオンにします。このように設定すると、グローバル相関インスペクションおよびレピュテーション フィルタリングがオンであるようにレポートが作成されます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 7　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

ネットワーク参加の設定

ここでは、ネットワーク参加の設定方法について説明します。内容は次のとおりです。

[Network Participation] ペイン

（注）　ネットワーク参加を設定するには、管理者権限またはオペレータ権限が必要です。

[Network Participation] ペインでは、SensorBase ネットワークにデータを送信するようにセンサーを設定できます。完全な参加を行うようにセンサーを設定し、すべてのデータを SensorBase ネットワークに送信することができます。または、潜在的に機密性が高いと見なされるデータ（トリガー パケットの宛先 IP アドレスなど）は除いてデータを収集するようにセンサーを設定できます。

（注） センサーを部分的ネットワーク参加用に設定すると、第三者が、内部ネットワークに関する調査情報をグローバル相関データベースから抽出するときに制限が課されます。

完全な参加を選択すると、ネットワーク参加データから除外する IP アドレスを指定できます。除外された攻撃者 / 攻撃対象者の IP アドレスは、シスコには送信されません。

[Network Participation] ペインのフィールド定義

[Network Participation] ペインには次のフィールドがあります。

- [Off]：どのデータも SensorBase ネットワークに提供されません。
- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：除外された攻撃者 / 攻撃対象者の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

ネットワーク参加の設定

ネットワーク参加を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Global Correlation] > [Network Participation] を選択します。

ステップ 3　ネットワーク参加をオンにするには、[Partial] または [Full] オプション ボタンをクリックします。

- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：除外された攻撃者 / 攻撃対象者の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

注意　ネットワーク参加に参加するには、免責事項に同意する必要があります。

ステップ 4　ネットワーク参加データから除外する IP アドレスまたはアドレス範囲を指定するには、[Add] をクリックし、[IP Address] フィールドに IP アドレスまたはアドレス範囲を入力します。除外した IP アドレスは、[IP Addresses] テーブルに表示されます。

ステップ 5　除外した IP アドレスまたはアドレス範囲を削除するには、[IP Addresses] テーブルから該当の IP アドレスまたはアドレス範囲を選択し、[Delete] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 6　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

グローバル相関のトラブルシューティング

グローバル相関を設定するときに、次の点に注意してください。

- グローバル相関更新は、センサー管理インターフェイスを介して発生するため、ファイアウォールで、ポート 443 および 80 のトラフィックが許可されている必要があります。
- グローバル相関機能を動作させるには、HTTP プロキシ サーバまたは DNS サーバを設定する必要があります。
- グローバル相関機能を動作させるには、有効な IPS ライセンスが必要です。
- グローバル相関機能には、外部 IP アドレスだけが含まれているため、社内ラボにセンサーを配置した場合は、グローバル相関情報を受信できません。
- 使用しているセンサーが、グローバル相関機能をサポートしていることを確認します。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

- 使用している IPS バージョンが、グローバル相関機能をサポートしていることを確認します。

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

グローバル相関のディセーブル化

DNS サーバまたは HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合、グローバル相関をディセーブルにして、全般的なセンサー ヘルス状態でグローバル相関のヘルス状態が（問題があることを示す）赤色で表示されないようにすることができます。グローバル相関のステータスを除外するように、センサー ヘルス状態を設定することもできます。

グローバル相関インスペクション、レピュテーション フィルタリング、およびネットワーク参加をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Global Correlation] > [Inspection/Reputation] を選択します。

ステップ 3　グローバル相関インスペクションおよびレピュテーション フィルタリングをディセーブルにするには、[Off] オプション ボタンをクリックします。

ステップ 4　レピュテーション フィルタリングをディセーブルにするには、[Off] オプション ボタンをクリックします。

ステップ 5　[Configuration] > *sensor_name* > [Policies] > [Global Correlation] > [Network Participation] を選択します。

ステップ 6　ネットワーク参加をディセーブルにするには、[Off] オプション ボタンをクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 7　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。