CHAPTER 11

グローバル相関の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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。次の事項について説明します。

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。IPS デバイスをシスコの中央脅威データベースである SensorBase ネットワークに参加させることで、グローバル相関のアップデートを受信して取り込むことができます。グローバル相関のアップデート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。

センサーがグローバル相関のアップデートやテレメトリ データの送信に参加するよう設定できます。両方のサービスをオフにすることも可能です。イベント内のレピュテーション スコアや、攻撃者のレピュテーション スコアを参照できます。レピュテーション フィルタからの統計を参照することも可能です。

SensorBase ネットワークへの参加

Cisco IPS には、セキュリティ機能である Cisco グローバル相関が含まれています。これには、長年にかけて蓄積してきた非常に優れたセキュリティ機能が使用されています。Cisco IPS は、通常の間隔でシスコ SensorBase ネットワークから脅威の更新を受信します。これには、連続攻撃者、ボットネット収穫プログラム、マルウェアの大発生、およびダークネットなど、インターネットに対する既知の脅威に関する詳細情報が含まれています。IPS は、この情報を使用して、最も悪質な攻撃者が重要な資産を攻撃する機会を得る前にそのような攻撃者をフィルタリングして除外します。その後、グローバルな脅威データをシステムに組み込んで、悪意のあるアクティビティをさらに早く検出して防止します。

SensorBase ネットワークへの参加に同意すると、シスコは、IPS 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を収集します。これには、Cisco IPS ネットワーク トラフィック プロパティと、Cisco アプライアンスによるこのトラフィックの処理方法に関するサマリー データが含まれます。トラフィックのデータ コンテンツやその他のビジネスまたは個人の機密情報は収集しません。すべてのデータは集約され、定期的にセキュアな HTTP によって Cisco SensorBase ネットワーク サーバに送信されます。シスコと共有されるデータはすべて匿名で、極秘扱いにされます。

表 11-1 に、シスコでのデータの使用方法を示します。

表 11-1　Cisco 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
部分的	プロトコル属性 （たとえば、TCP 最大セグメント サイズおよびオプションの文字列）	潜在的脅威を追跡し、脅威による影響を理解するために役立ちます。
	攻撃のタイプ （たとえば、発行されたシグニチャ、リスク レーティング）	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 のサマリー パフォーマンス （CPU 使用率、メモリ使用率、インライン対 無差別など）	製品の有効性を追跡します。
完全	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。

部分的または完全なネットワーク参加をイネーブルにすると、ネットワーク参加の免責条項が表示されます。参加するには、[Agree] をクリックする必要があります。ライセンスをインストールしていない場合は、センサーがライセンスされるまで、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 フィルタリングがディセーブルになっていることを伝え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

センサーの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.16-5）を参照してください。

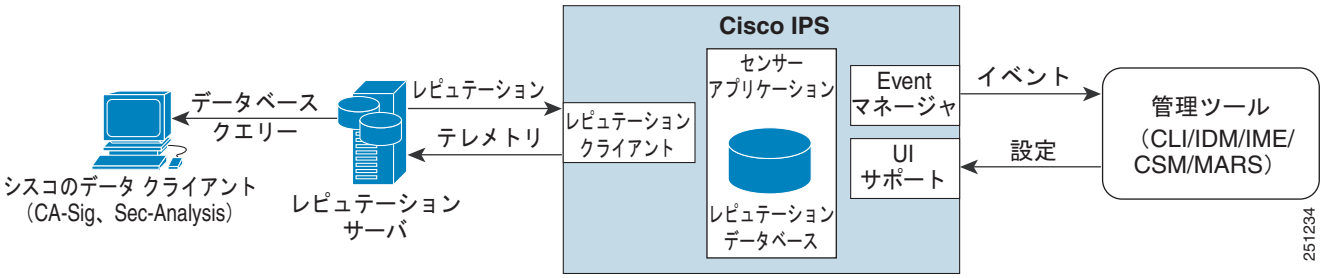
レピュテーションについて

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。既存のネットワーク インフラを使用してコラボレーションを行うには、現場に設置されている IPS センサーのベースをイネーブルにします。レピュテーションがあるデバイスは、悪意のある、または感染している可能性が最も高いデバイスです。レピュテーション情報と統計を、IDM で参照できます。

IPS センサーはグローバル相関サーバ（レピュテーション サーバとも）と協働してセンサーの有効性を向上させます。

図 11-1 に、センサーとグローバル相関サーバの役割を示します。

図 11-1　　IPS 管理とグローバル相関サーバの相互作用



グローバル相関サーバは、悪意のあるホストや感染したホストを示す可能性がある特定の IP アドレスについての情報をセンサーに提供します。センサーはこの情報を使用して、既知のレピュテーションを持つホストから潜在的に危険なトラフィックを受信した場合に実行が必要となるアクションを決定します。グローバル相関のデータベースは急速に変化するため、センサーは定期的にグローバル相関更新をグローバル相関サーバから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 / 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 アプライアンスのコンフィギュレーションおよび IPS SSP で実行中のアクティビティのタイプに応じて、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のいずれかになります。

詳細情報

グローバル相関の統計情報参照の詳細については、「統計情報の表示」（P.17-31）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、シスコは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正確性が高まります。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。

ネットワーク参加では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
- 最大セグメントのサイズ
- 攻撃対象の IP アドレス
- 攻撃対象のポート
- シグニチャ 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では、アラートのヒットとミス、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表示されます。

ネットワーク参加には 3 つのモードがあります。

- Off : 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、Cisco SensorBase ネットワークへの接続試行を行いません。
- Partial Participation : 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、SensorBase ネットワークとの通信を行います。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。
- Full Participation : 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、SensorBase ネットワークとの通信を行います。収集されたデータは、ネットワーク参加データから除外する IP アドレス以外、すべて送信されます。

ネットワーク参加には、インターネット接続が必要です。

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 / 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 アプライアンスのコンフィギュレーションおよび IPS SSP で実行中のアクティビティのタイプに応じて、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のいずれかになります。

詳細情報

ネットワーク参加の設定の詳細については、「ネットワーク参加の設定」（P.11-10）を参照してください。

有効性について

参加している IPS クライアントからデータを取得し、脅威についての既存の知識のコーパスと組み合わせて使用することで、IPS の有効性が向上されます。有効性は、次の要素をもとに評価されます。

- 実行可能なイベントの false positive（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 false negative（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 チームはデータを使用してシグニチャの正確性を高め、IPS エンジニアリング チームはデータを使用してさまざまなタイプのセンサー配置についての理解を深めます。

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.11-5）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可能性を示す概念です。ネットワーク上の特定のイベントに関連したリスクを数量化して数値を割り当てます。デフォルトでは、リスク レーティングがきわめて高いアラートによって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。アラーム チャネルによってこのレピュテーションに特定のスコアが計算されてリスク レーティングに加算され、こうして IPS の有効性が向上します。攻撃者のレピュテーション スコアが悪い場合、さらに大きな値にするため、増分リスクがリスク レーティングに加算されます。

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。アラート処理ユニットには、複数の集約技術、アクション オーバーライド、アクション フィルタ、攻撃者レピュテーション、アクションごとに特化した処理メソッドがあります。アラーム チャネルでの攻撃者のスコア付けには、レピュテーション参加クライアントからの大量のレピュテーション データが使用され、このスコアがリスク レーティングとアラートのアクションに影響を与えます。

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.9-3）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、「脅威レーティングについて」（P.9-4）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 フィルタについて」（P.9-5）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.9-6）を参照してください。

グローバル相関の機能と目的

グローバル相関には、次の 3 つの主な機能があります。

- グローバル相関インスペクション：グローバル相関の攻撃者に関するレピュテーション知識を使用して、悪いスコアを持つ攻撃者がセンサーに出現した場合のアラート処理や拒否アクションを変更します。
- 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：センサーがアラートと 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 ライセンスが必要です。グローバル相関機能の統計情報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。

- ネットワーク参加免責事項への同意。
- センサーの外部接続と DNS サーバ。

  Cisco IPS のグローバル相関機能では、センサーを 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によってだけ使用されます。

注意　コマンド接続と制御接続が遅い環境に配置されたセンサーでは、グローバル相関の更新も遅くなります。

- サポートされない IPv6 アドレス

  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、インライン拒否アクションを使用してグローバル相関機能の有効性を増すために、インライン モードで動作する必要があります。

- グローバル相関機能をサポートするセンサー
- グローバル相関機能をサポートする IPS のバージョン

詳細情報

- センサーの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.16-5）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.11-2）を参照してください。
- グローバル相関をサポートするような DNS または HTTP プロキシ サーバの設定については、「ネットワークの設定」（P.4-2）を参照してください。

グローバル相関センサー ヘルス メトリックについて

グローバル相関では、次のメトリックがセンサー ヘルス モニタリングに追加されます。

- グリーンは前回のアップデートが成功したことを示します。
- イエローは過去 1 日（86,400 秒）の間に成功したアップデートがないことを示します。
- レッドは過去 3 日（259,200 秒）の間に成功したアップデートがないことを示します。

ネットワーク参加では、次のメトリックがセンサー ヘルス モニタリングに追加されます。

- グリーンは前回の接続が成功したことを示します。
- イエローは連続して 6 回未満接続に失敗していることを示します。
- レッドは連続して 6 回以上接続に失敗していることを示します。

メトリックは [Sensor Health] ガジェットと [Global Correlation Health] ガジェットに表示されます。

（注）　グローバル相関ヘルス ステータスはデフォルトでレッドになり、グローバル相関の更新成功後にグリーンに変わります。グローバル相関の更新成功には、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 サーバの設定機能があるのは IPS 7.0(1)E3 以降なため、6.*x* から 7.0(1)E3 以降にアップグレードした場合は未設定になっています。その結果、グローバル相関のヘルスと全体のセンサー ヘルス ステータスは、DNS か HTTP プロキシ サーバをセンサーに設定するまで、レッドになります。センサーが DNS や HTTP サーバが利用できない環境に配置されているためにグローバル相関ヘルスおよび全体のセンサー ヘルス ステータスがレッドになっている場合、グローバル相関をディセーブルにし、センサー ヘルス ステータスにグローバル相関ヘルス ステータスを含めないよう設定することで処理できます。

詳細情報

- センサー ヘルス メトリックの詳細については、「センサー ヘルスの設定」（P.16-9）を参照してください。
- グローバル相関をサポートするような DNS または HTTP プロキシ サーバの設定については、「ネットワークの設定」（P.4-2）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」（P.11-8）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

この項では、グローバル相関インスペクションとレピュテーションの設定方法について説明します。次の項目を取り上げます。

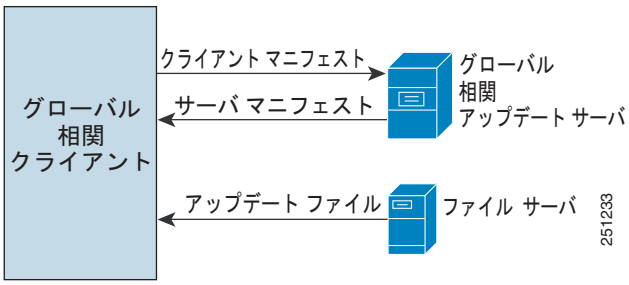
[Inspection/Reputation] ペイン

（注）　インスペクション / レピュテーション設定を変更するには、管理者またはオペレータである必要があります。

[Inspection/Reputation] ペインでは、SensorBase ネットワークからのアップデートを利用してリスク レーティングを調整するようセンサーを設定できます。クライアントは、グローバル相関更新サーバおよびファイル サーバと通信し、どのアップデートがセンサーに対して利用可能かつ適用可能かを決定します。グローバル相関更新サーバは、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 11-2 に、グローバル相関更新クライアントのファイル取得方法を示します。

図 11-2　グローバル相関更新クライアント



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 ライセンスが必要です。グローバル相関機能の統計情報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。

いったんグローバル相関を設定すると、アップデート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。センサーはフル アップデートを取得し、その後は定期的に差分更新を適用します。

HTTP プロキシ サーバや DNS サーバは [Network] ペインで設定できます。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 グローバル相関] 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] ガジェットに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は [Normal]、[Needs Attention]、[Critical] で表されます。

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 / 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 アプライアンスのコンフィギュレーションおよび IPS SSP で実行中のアクティビティのタイプに応じて、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のいずれかになります。

[Inspection/Reputation] ペインのフィールド定義

[Inspection/Reputation] ペインには、次のようなフィールドがあります。

- [グローバル相関 Inspection] : グローバル相関のオンとオフを制御します。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。拒否アクションを開始するためにセンサーがグローバル相関の情報をどれほど利用するかを、3 つのモードから決定できます。
  - [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の大きさになります。
  - [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 フィルタリングのオンとオフを制御できます。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た拒否アクションの報告機能をイネーブルにします。実際のホストを拒否することなく、グローバル相関機能のテストが行えます。

詳細情報

- センサーの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.16-5）を参照してください。
- センサー ヘルス メトリックの詳細については、「センサー ヘルスの設定」（P.16-9）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、次の手順に従います。

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

ステップ 2　[Configuration] > [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、デフォルトでは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、拒否アクション開始にグローバル相関情報をどれほど利用するかを選択します。

- [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の大きさになります。
- [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、デフォルトではオフになっています。

ステップ 6　グローバル相関が実際のトラフィックを拒否するかどうかには影響を与えずにグローバル相関のテストを行うには、[Test Global Correlation] チェックボックスをクリックします。これにより、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になっていると想定したレポートが表示されます。

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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

ネットワーク参加の設定

この項では、ネットワーク参加を設定する方法について説明します。次の項目を取り上げます。

- 「[Network Participation] ペイン」（P.11-11）
- 「[Network Participation] ペインのフィールド定義」（P.11-11）
- 「ネットワーク参加の設定」（P.11-11）

[Network Participation] ペイン

（注）　ネットワーク参加機能を設定するには、管理者またはオペレータである必要があります。

[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センサーを設定できます。全面的に参加してすべてのデータを SensorBase ネットワークに送るようセンサーを設定できます。データの収集は行うものの、トリガー パケットの宛先 IP アドレスなど機密データの可能性があるものを除くよう設定することも可能です。

（注）　センサーを部分的ネットワーク参加として設定すると、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。

[Network Participation] ペインのフィールド定義

[Network Participation] ペインには、次のようなフィールドがあります。

- [Off]：いずれのデータも 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るため送信されません。
- [Full]：すべてのデータは、除外する攻撃者や攻撃対象の IP アドレスを除き、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 IDM にログインします。

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

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るため送信されません。
- [Full]：すべてのデータは、除外する攻撃者や攻撃対象の IP アドレスを除き、SensorBase ネットワークに提供されます。

注意　ネットワーク参加への参加にあたっては、免責条項への同意が必要です。

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 4　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

グローバル相関のトラブルシューティング

グローバル相関の設定時に、次の点を確認してください。

- グローバル相関の更新はセンサー管理インターフェイスから行われるため、ファイアウォールではポート 443/80 のトラフィックを許可する必要があります。
- グローバル相関機能が動作するには、HTTP プロキシ サーバまたは DNS サーバが設定されている必要があります。
- グローバル相関機能が動作するには、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、内部ラボにセンサーを設置した場合は、グローバル相関情報を受信できません。
- センサーでグローバル相関機能がサポートされていることを確認します。
- ご使用の IPS バージョンでグローバル相関機能がサポートされていることを確認します。

詳細情報

- センサーの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.16-5）を参照してください。
- グローバル相関をサポートするような DNS または HTTP プロキシ サーバの設定については、「ネットワークの設定」（P.4-2）を参照してください。

グローバル相関のディセーブル化

DNS サーバや HTTP プロキシ サーバが利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することで、グローバル相関ヘルスが全体のセンサー ヘルスで赤く表示される（問題の発生を示す）ことがないよう設定できます。また、センサー ヘルスからグローバル相関ステータスを除外するよう設定することも可能です。

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、ネットワーク参加をディセーブルにするには、次の手順に従います。

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

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

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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。