CHAPTER 10

グローバル相関の設定

この章では、グローバル相関の設定について説明します。次のような構成になっています。

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。シスコの中央脅威データベースである SensorBase に IPS デバイスを参加させることにより、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。参加する各 IPS デバイスは、グローバル相関データベース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。

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センサーを設定でき、両方のサービスをオフにすることもできます。イベントのレピュテーション スコアを表示でき、攻撃者のレピュテーション スコアを確認できます。

SensorBase ネットワークへの参加

Cisco IPS が持つ新しいセキュリティ機能であるシスコ グローバル相関では、長年シスコが蓄積してきた膨大な量のセキュリティ インテリジェンスが使用されます。Cisco IPS は、定期的にシスコの SensorBase ネットワークから脅威情報の更新を受信します。この情報には、インターネット上の既知の脅威（連続攻撃者、ボットネット ハーベスタ、マルウェア アウトブレイク、ダークネットなど）に関する詳細情報が入っています。IPS はこの情報を使用して、悪質な攻撃者が大切な資産を攻撃する前に排除します。その後、グローバル脅威データをシステムに取り込み、悪意のあるアクティビティを検出して未然に阻止します。

SensorBase ネットワークへの参加に同意した場合、シスコは、IPS に送信されたトラフィックに関する集約統計を収集します。これには、Cisco IPS ネットワークのトラフィック特性や、シスコのアプライアンスが実行したトラフィックへの対処方法についての要約データが含まれています。トラフィック データの中身や企業または個人の機密情報を収集することはありません。定期的にすべてのデータが集約され、セキュア HTTP を使用してシスコの SensorBase ネットワーク サーバに送信されます。シスコが共有するデータはすべて匿名であり、極秘に扱われます。

表 10-1 に、シスコでのデータの使用方法を示します。

表 10-1　シスコ ネットワーク参加データの用途

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。
	攻撃の種類 （シグニチャの発動、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 パフォーマンスの要約 （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
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

Partial または Full の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事項が表示されます。参加するには、**yes** と入力する必要があります。ライセンスがインストールされていないと、センサーのライセンスがインストールされるまでグローバル相関の検査およびレピュテーション フィルタリングは使用できないことを示す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 キーのインストール」（P.4-56）を参照してください。

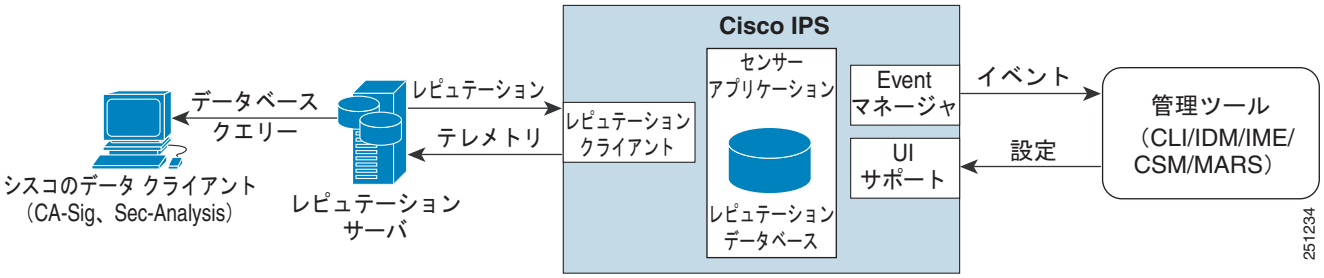
レピュテーションについて

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。現場での IPS センサーのインストール ベースで、既存のネットワーク インフラストラクチャを使用したコラボレーションを可能にします。レピュテーションのあるネットワーク デバイスは、ほとんどが悪意があるか、感染しています。レピュテーション情報および統計情報は、IDM で確認できます。

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）と連携してセンサーの有効性を高めます。

図 10-1 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 10-1　IPS 管理とグローバル相関サーバの相互動作



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の可能性がある特定の IP アドレス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有害な可能性のあるトラフィックを受信した場合に実行するアクション（ある場合）を決定します。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、グローバル相関更新をグローバル相関サーバから定期的にダウンロードする必要があります。

注意　シグニチャ アップデートと同様に、センサーはグローバル相関更新を適用するときにバイパスをトリガーする場合があります。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。

詳細情報

グローバル相関統計情報の表示の詳細については、「統計情報の表示」（P.17-24）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、シスコは世界中のセンターからほぼリアルタイムでデータを収集できます。カスタマー サイトに設置されているセンサーは、SensorBase にデータを送信できます。これらのデータが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 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 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、アラートが正しかった回数、誤っていた回数、レピュテーション アクション、および拒否されたパケット数のカウンタが示されます。

ネットワーク参加には、次の 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、またはシスコ SensorBase ネットワークへの接続試行は行いません。
- 部分的参加：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 収集されたすべてのデータが送信されます。

ネットワーク参加には、少なくとも 100 MB の使用可能なメモリ、センサーへのネットワーク接続、およびインターネットへのネットワーク接続が必要です。

注意　シグニチャ アップデートと同様に、センサーはグローバル相関更新を適用するときにバイパスをトリガーする場合があります。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。

詳細情報

- ネットワーク参加の詳細については、「ネットワーク参加の設定」（P.10-11）を参照してください。
- バイパス モードの詳細については、「インライン バイパス モードの設定」（P.6-38）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、そのデータと併せて既存の脅威ナレッジの集積を使用することで、IPS の有効性は高まります。有効性は、次の基準で評価されます。

- 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）

詳細情報

レピュテーションおよびリスク 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.10-5）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かどうかの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対して、そのイベントのリスクを定量化した数値を割り当てます。デフォルトでは、リスク レーティングが非常に高いアラートが発生すると、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。Alarm Channel は、このレピュテーションに対するスコア値を計算し、その値をリスク レーティングに追加します。これによって、IPS の有効性が高まります。攻撃者が悪いレピュテーション スコアを持つ場合、加算されたリスクがリスク レーティングに追加されるため、より強力に対処されることになります。

Alarm Channel 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、複数の集約テクニック、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、アクション別カスタム対処方法があります。レ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、Alarm Channel で攻撃者のスコアを付けてから、そのスコアを使用してリスク レーティングおよびアラート アクションを調整します。

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.7-12）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.7-14）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 フィルタの設定」（P.7-20）を参照してください。
- Alarm Channel の詳細については、「SensorApp について」（P.A-25）を参照してください。
- イベント アクションの集約の詳細については、「イベント アクションの集約について」（P.7-34）を参照してください。

グローバル相関と Produce Alert イベント アクション

produce-alert イベント アクションは、次の状況でイベントに追加されます。

- グローバル相関によって、イベントのリスク レーティングが増加した。
- グローバル相関によって、deny-packet-inline または deny-attacker-inline のどちらかのイベント アクションが追加された。

produce-alert イベント アクションが追加されると、グローバル相関によって拒否されたすべてのイベントでアラートが生成され、それをモニタリング ツールで確認できるようになります。このようにすると、グローバル相関がどのようなイベントを拒否したかを知ることができます。

（注）　この機能は、特定のシグニチャと一致しない場合にトラフィックを許可する、グローバル相関インスペクションにのみ適用されます。シグニチャ分析の前にパケットを拒否するレピュテーション フィルタリングには適用されないため、レピュテーション フィルタリングによってパケットが拒否されるときには、アラートが生成されません。

詳細情報

イベント アクションの詳細については、「イベント アクション」（P.7-4）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 に送信します。

グローバル相関 には、次のような目的があります。

- 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 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を使用するには、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 サーバへの外部接続

  グローバル相関機能を使用するには、センサーがシスコの SensorBase ネットワークに接続される必要があります。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 プロキシおよび DNS サーバはグローバル相関機能でのみ使用されます。

注意　コマンドおよび制御接続が低速な環境に設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速度も遅くなります。

- IPv6 アドレスのサポートなし

  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は、IPv6 アドレスをサポートしていません。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。

- グローバル相関をサポートする IPS バージョン

  （注）　Cisco IPS 6.1 および 6.2 は、グローバル相関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センサー

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 キーのインストール」（P.4-56）を参照してください。
- ネットワーク参加の免責事項については、「SensorBase ネットワークへの参加」（P.10-2）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に HTTP プロキシまたは DNS サーバを設定する方法については、「グローバル相関用の DNS サーバおよびプロキシ サーバの設定」（P.4-9）を参照してください。

グローバル相関のセンサー ヘルス メトリックについて

グローバル相関に関しては、次のメトリックがセンサー ヘルス モニタに追加されます。

- 緑は、最後の更新が正常実行されたことを示します。
- 黄色は、最近 1 日（86,400 秒）の間、正常実行された更新がないことを示します。
- 赤は、最近 3 日（259,200 秒）の間、正常実行された更新がないことを示します。

ネットワーク参加に関しては、次のメトリックがセンサー ヘルス モニタに追加されます。

- 緑は、最後の接続が正常実行されたことを示します。
- 黄色は、連続して接続に失敗した回数が 6 回未満であることを示します。
- 赤は、連続して接続に失敗した回数が 7 回以上であることを示します。

センサーのヘルス統計情報を設定するには、サービス サブモードで、**health-monitor** コマンドを使用します。**health-monitor** コマンドの結果を表示するには、**show health** コマンドを使用します。

グローバル相関のヘルス ステータスはデフォルトでは赤です。グローバル相関更新が正常実行されると緑に変化します。グローバル相関更新を正常実行するためには、DNS サーバまたは HTTP プロキシ サーバが必要です。DNS サーバまたは HTTP プロキシ サーバの設定機能は IPS 7.0 で新たに導入された機能であるため、7.0 にアップグレードしても未設定のままとなります。このため、グローバル相関のヘルスおよびセンサーのヘルス ステータス全体は、DNS サーバまたは HTTP プロキシ サーバをセンサーに設定するまで赤になります。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を設置した場合は、グローバル相関をディセーブルにし、グローバル相関のヘルス ステータスを除外するようにセンサー ヘルス ステータスを設定することによって、グローバル相関のヘルスおよびセンサー ヘルス ステータス全体が赤になる問題を解決できます。

詳細情報

- センサー ヘルス メトリックの表示手順については、「センサーのヘルス ステータス全体の表示」（P.17-14）を参照してください。
- DNS サーバまたは HTTP プロキシ サーバの追加手順については、「グローバル相関用の DNS サーバおよびプロキシ サーバの設定」（P.4-9）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.10-13）を参照してください。
- グローバル相関のヘルスをセンサー ヘルス全体から除外する手順については、「ヘルス ステータス情報の設定」（P.17-10）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

ここでは、グローバル相関インスペクションとレピュテーション フィルタリング、およびそれらの設定方法について説明します。次の項目について説明します。

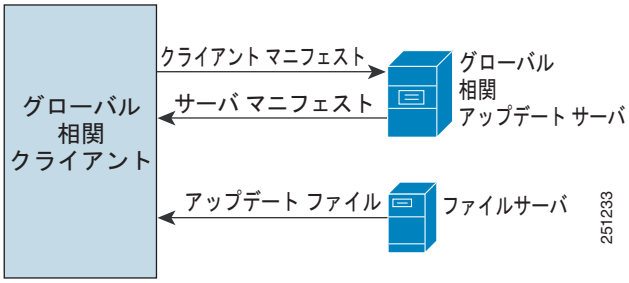
- 「グローバル相関インスペクションおよびレピュテーション フィルタリングについて」（P.10-8）
- 「グローバル相関インスペクションおよびレピュテーション フィルタリングの設定」（P.10-9）

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 フィルタリングについて

SensorBase から得た更新を使用してリスク レーティングを調整するように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 サーバと通信して、センサーに使用可能で適用可能な更新を特定します。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 10-2 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 10-2　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を使用するには、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、その後は定期的に増分更新を適用します。

HTTP プロキシまたは DNS サーバは、サービス ネットワーク設定サブモードで設定します。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。

センサーのヘルス ステータス情報全体を表示するには、特権 EXEC モードで、**show health** コマンドを使用します。ヘルス ステータス カテゴリは赤と緑によってレーティングされ、赤は重大なステータスを示します。

注意　シグニチャ アップデートと同様に、センサーはグローバル相関更新を適用するときにバイパスをトリガーする場合があります。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。

詳細情報

- グローバル相関機能の設定手順については、「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.10-9）を参照してください。
- センサー ヘルス メトリックの表示手順については、「センサーのヘルス ステータス全体の表示」（P.17-14）を参照してください。
- CollaborationApp の詳細については、「CollaborationApp」（P.A-30）を参照してください。
- バイパス モードの詳細については、「インライン バイパス モードの設定」（P.6-38）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

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのどちらが必ず設定されている必要があります。

次のオプションが適用されます。

- **global-correlation-inspection {on | off}**：グローバル相関インスペクションをオンまたはオフにします。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 on です。
- **global-correlation-inspection-influence {permissive | standard | aggressive}**：グローバル相関インスペクションのレベルを選択します。デフォルトは standard です。
  - **permissive**：グローバル相関データは、トラフィックの拒否決定にほとんど影響を与えません。
  - **standard**：グローバル相関は、トラフィックの拒否決定にある程度影響を与えます。
  - **aggressive**：グローバル相関データは、トラフィックの拒否決定に大きな影響を与えます。
- **reputation-filtering {on | off}**：レピュテーション フィルタリングをオンまたはオフにします。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 on です。
- **test-global-correlation {on | off}**：グローバル相関による影響を受ける拒否アクションについて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。デフォルトは off です。

グローバル相関機能を設定するには、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 CLI にログインします。

ステップ 2　グローバル相関サブモードをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service global-correlation
sensor(config-glo)#
```

ステップ 3　グローバル相関インスペクションをオンにします。

```
sensor(config-glo)# global-correlation-inspection on
sensor(config-glo)#
```

ステップ 4　グローバル相関インスペクションのレベルを指定します。

```
sensor(config-glo)# global-correlation-inspection-influence aggressive
sensor(config-glo)#
```

ステップ 5　レピュテーション フィルタリングをオンにします。

```
sensor(config-glo)# reputation-filtering on
sensor(config-glo)#
```

ステップ 6　グローバル相関データをテストします。実際にはトラフィックを拒否しません。

```
sensor(config-glo)# test-global-correlation on
sensor(config-glo)#
```

ステップ 7　設定を確認できます。

```
sensor(config-glo)# show settings
   global-correlation-inspection: on default: on
   global-correlation-inspection-influence: aggressive default: standard
   reputation-filtering: on default: on
   test-global-correlation: on default: off
sensor(config-glo)#
```

ステップ 8　グローバル相関サブモードを終了します。

```
sensor(config-glo)# exit
```

```
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

詳細情報

- グローバル相関をサポートするように HTTP プロキシまたは DNS サーバを設定する方法については、「グローバル相関用の DNS サーバおよびプロキシ サーバの設定」（P.4-9）を参照してください。
- 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 キーのインストール」（P.4-56）を参照してください。
- センサーのヘルス メトリックの詳細については、「センサーのヘルス ステータス全体の表示」（P.17-14）を参照してください。

ネットワーク参加の設定

（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。

SensorBase にデータを送信するようにセンサーを設定できます。センサーに完全な参加を設定すると、すべてのデータを SensorBase に送信できます。また、データを収集するが、トリガー パケットの宛先 IP アドレスなど、機密性が高い可能性のあるデータは無視するようセンサーを設定することもできます。

次のオプションが適用されます。

- **network-participation**：ネットワーク参加のレベルを設定します。デフォルトは off です。
  - **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**：データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除かれます。
  - **full**：すべてのデータが SensorBase ネットワークに提供されます。

    （注）　ネットワーク参加をオンにするには、ネットワーク参加の免責事項に同意する必要があります。

ネットワーク参加 をオンにするには、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 CLI にログインします。

ステップ 2　グローバル相関サブモードをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service global-correlation
sensor(config-glo)#
```

ステップ 3　ネットワーク参加をオンにします。

```
sensor(config-glo)# network-participation {full | partial]
sensor(config-glo)# exit
```

ステップ 4　**yes** を入力して、SensorBase ネットワークへの参加に同意します。

```
If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS
network traffic properties and how this traffic was handled by the Cisco appliances.  We
do not collect the data content of traffic or other sensitive business or personal
information.  All data is aggregated and sent via secure HTTP to the Cisco SensorBase
Network servers in periodic intervals.  All data shared with Cisco will be anonymous and
treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

ステップ 5　設定を確認できます。

```
sensor(config-glo)# show settings
   network-participation: full default: off
   global-correlation-inspection: on default: on
   global-correlation-inspection-influence: aggressive default: standard
   reputation-filtering: on default: on
   test-global-correlation: on default: off
sensor(config-glo)#
```

ステップ 6　グローバル相関サブモードを終了します。

```
sensor(config-glo)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

詳細情報

SensorBase ネットワークへの参加の詳細については、「SensorBase ネットワークへの参加」（P.10-2）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を設置した場合、センサー ヘルス全体に赤（問題があることを示す色）のグローバル相関ヘルスが表示されないようにするには、グローバル相関をディセーブルにする必要があります。また、グローバル相関を除外するようにセンサー ヘルスを設定することもできます。

次のオプションが適用されます。

- **global-correlation-inspection {on | off}**：グローバル相関インスペクションをオンまたはオフにします。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 on です。
- **reputation-filtering {on | off}**：レピュテーション フィルタリングをオンまたはオフにします。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 on です。
- **network-participation**：ネットワーク参加のレベルを設定します。デフォルトは off です。
  - **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**：データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除かれます。
  - **full**：すべてのデータが SensorBase ネットワークに提供されます。

グローバル相関機能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 CLI にログインします。

ステップ 2　グローバル相関サブモードをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service global-correlation
sensor(config-glo)#
```

ステップ 3　グローバル相関インスペクションをオフにします。

```
sensor(config-glo)# global-correlation-inspection off
sensor(config-glo)#
```

ステップ 4　レピュテーション フィルタリングをオフにします。

```
sensor(config-glo)# reputation-filtering off
sensor(config-glo)#
```

ステップ 5　ネットワーク参加をオフにします。

```
sensor(config-glo)# network-participation off
sensor(config-glo)# exit
```

ステップ 6　設定を確認できます。

```
sensor(config-glo)# show settings
   network-participation: full default: off
   global-correlation-inspection: on default: off
   reputation-filtering: on default: off
sensor(config-glo)#
```

ステップ 7　グローバル相関サブモードを終了します。

```
sensor(config-glo)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

詳細情報

グローバル相関をセンサー ヘルス全体から除外する手順については、「ヘルス ステータス情報の設定」（P.17-10）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

グローバル相関を設定するときは、次の点を確認してください。

- 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使用して実行されるため、ポート 443/80 のトラフィックをファイアウォールで許可する必要があります。
- グローバル相関が機能するためには、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使用するには、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るため、センサーを社内ラボに配置した場合はグローバル相関情報を受信できません。
- 使用す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てください。
- 使用する IPS バージョンがネットワーク参加機能をサポートしていることを確認してください。

（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

- DNS サーバまたは HTTP プロキシ サーバの設定手順については、「グローバル相関用の DNS サーバおよびプロキシ サーバの設定」（P.4-9）を参照してください。
- IPS ライセンスを取得する手順については、「ライセンス キーのインストール」（P.4-56）を参照してください。