グローバル相関の設定

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

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。グローバル相関を使用すると、世界中のネットワークから収集された悪意のあるアクティビティに関する情報を動的に使用して、悪意のある既知のデバイスを発信元とするイベントのリスク レーティングを変更できます。

グローバル相関を設定するには、センサーで IPS 7.0+ ソフトウェアが実行されている必要があります。グローバル相関は、Cisco IOS IPS デバイスでは使用できません。

この章は次のトピックで構成されています。

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。

ヒント Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の Botnet Traffic Filter 機能は、ネットワークに展開して、悪意のあるアクティビティに対する防衛を実現できるもう 1 つの動的機能です。IPS デバイスでグローバル相関を設定し、ASA ファイアウォールでボットネット トラフィック フィルタリングを設定すると、効果的な統合セキュリティ実装を実現できます。ボットネット トラフィック フィルタリングの詳細については、ファイアウォールの Botnet Traffic Filter ルールの管理を参照してください。

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：IPS は、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。レピュテーションの詳細については、レピュテーションについて （3 ページ）を参照してください。
- 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。
- ネットワーク参加：センサーは、他のユーザがコミュニティ ナレッジで共有できるように、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。詳細については、ネットワーク参加について （4 ページ）を参照してください。

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。

ヒント Report Manager を使用して、グローバル相関により生成されたアラート数と従来の IPS 検査によって生成されたアラート数を比較するレポートを生成できます。Inspection/Global Correlation レポートの詳細については、全般 IPS レポートについてを参照してください。レポートの生成については、レポートの起動と生成を参照してください。

グローバル相関の設定方法については、次の項を参照してください。

- グローバル相関の要件および制限 （5 ページ）
- 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 （7 ページ）

• ネットワーク参加の設定 （8 ページ）

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。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、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 デバイスを特定できます。

グローバル相関データベースは、デバイスに関するデータを収集し、デバイスにレピュテーション スコアを割り当てることにより、IPS センサーが攻撃のリスク レーティングの調整に使用できる重要なデータを提供します。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します。各シグニチャには、リスク レーティングが割り当てられています。グローバル相関をイネーブルにすると、IPS センサーは、攻撃者のレピュテーションに基づいてスコアを計算し、そのスコアをイベントのリスク レーティングに追加します。更新されたリスク レーティングは、イベント アクション オーバーライドおよびフィルタ ポリシーで使用でき、イベントに適用するアクションを決定するときに役立ちます。

単にアラートを生成するために初期設定されたイベントが存在する場合があります。ただし、攻撃者に悪いレピュテーションがある場合、IPS はリスク レーティングの数値を高くして、Deny Packet Inline アクションを追加するイベント アクション オーバーライド ルールをトリガーできるようにします。したがって、一部の送信元デバイスでは、イベントによって単にアラートが生成されるだけですが、他の送信元デバイスでは、アラートの生成に加えてパケットがドロップされます。

ヒント グローバル相関によってイベントのリスク レーティングが上がるたびに、またはグローバル相関によって Deny Packet Inline アクションまたは Deny Attacker Inline アクションが追加されると、Produce Alert アクションがイベントに追加されます。

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。

レピュテーション スコアを使用してイベントのリスク レーティングを調整すると、次のメトリックが向上し、センサーの有効性が高まります。

- 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）。

関連項目

• グローバル相関について （1 ページ）

- ネットワーク参加の設定 （8 ページ）
- 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 （7 ページ）
- ネットワーク参加の設定 （8 ページ）

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ーは、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。
- **部分的参加**：ネットワーク参加サーバーは、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。

（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**：ネットワーク参加サーバーは、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。

部分的参加または完全な参加を選択した場合、参加の契約に同意するように要求されます。参加するには契約に同意する必要があります。同意しないと、参加モードを変更できません。

次の表に、収集されるデータおよびデータ収集の目的を示します。

表 *1*: ネットワーク参加データの共有および使用

参加レベル	データのタイプ	目的
一部	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。
	攻撃のタイプ（発行されたシグニチャ [シグニチャの ID やバージョンなど]、リスク レーティング、レピュテーションなど）。	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 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（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。

ネットワーク参加を設定する場合、IPS デバイスには、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。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 （8 ページ）を参照してください。

グローバル相関の要件および制限

次のリストに、IPS デバイスでグローバル相関を設定し、適切に使用するために必要な要件を示します。制限についてもいくつか説明しています。

- **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を取得している必要があります。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。ライセンスの設定については、IPS ライセンス ファイルの更新を参照してください。
- **ネットワーク参加の免責事項への同意**：ネットワーク参加を設定することを決定した場合は、免責事項に同意する必要があります。詳細については、ネットワーク参加について（4 ページ）およびネットワーク参加の設定 （8 ページ）を参照してください。
- **センサーおよび DNS サーバーや HTTP プロキシの外部接続**：グローバル相関では、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 クライアントが稼働している 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。詳細については、DNS サーバの識別およびHTTP プロキシ サーバの識別を参照してください。

- **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と IPS バージョン**：センサーは、IPS 7.0+ ソフトウェアを実行している必要があります。Cisco IOS IPS デバイスでグローバル相関を設定することはできません。
- **使用可能な十分なメモリ**：ネットワーク参加を設定するには、IPS デバイスに少なくとも 100 MB の使用可能なメモリが必要です。
- **ポート 80、443 トラフィックのファイアウォールアクセス**：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、センサーとインターネット間にあるすべてのファイアウォールで、ポート 80 および 443 のトラフィックが許可されている必要があります。HTTP プロキシを使用することもできます（HTTP プロキシ サーバの識別を参照）。
- **外部トラフィックへの公開**：グローバル相関データベースには、外部 IP アドレスだけが含まれているため、外部ネットワークと通信できない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。この機能を使用しても何の効果もありません。
- **グローバル相関の更新時にバイパスモードがトリガーされる可能性がある**：シグニチャの更新と同様、センサーがグローバル相関更新を適用するときに、バイパスがトリガーされる可能性があります。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アップデートの適用中にトラフィックの送信を停止します。
- **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。

関連項目

- グローバル相関について （1 ページ）
- レピュテーションについて （3 ページ）
- ネットワーク参加について （4 ページ）
- 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 （7 ページ）

• ネットワーク参加の設定 （8 ページ）

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

インスペクション/レピュテーション ポリシーを使用して、SensorBase ネットワークからの更新によってイベントのリスク レーティングを調整するようにセンサーを設定します。センサー上のグローバル相関クライアントは、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 サーバからアップデート ファイルをダウンロードします。

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、最初に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。

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。

ヒント Event Viewer で IPS イベントを表示すると、イベント テーブルに追加できるグローバル相関固有の複数のカラムが示されます。これらのカラムは、デフォルトでは表示されないため、使用しているビューに追加する必要があります。一般的なグローバル相関のモニタでは、IPS Device Manager（IDM）を使用して、センサー ヘルス ガジェットをモニタします。完全な機能を備えた IDM を使用するか、デバイス ビューでデバイスを右クリックして[デバイス マネージャ（Device Manager）] を選択して、Security Manager から読み取り専用コピーを開きます。

はじめる前に

- グローバル相関が機能するためには、DNS サーバまたはHTTP プロキシも設定する必要があります。詳細については、DNS サーバの識別またはHTTP プロキシ サーバの識別を参照してください。
- グローバル相関を設定する前に、認識しておく必要がある設定上の要件および制限がいくつかあります。詳細については、 グローバル相関の要件および制限 （5 ページ）を参照してください。

関連項目

- グローバル相関について （1 ページ）
- レピュテーションについて （3 ページ）
- ネットワーク参加の設定 （8 ページ）

ステップ 1 次のいずれかを実行して、[Inspection/Reputation] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [グローバル相関（Global Correlation）] > [インスペクション/レピュテーション（Inspection/Reputation）] を選択します。
- （ポリシービュー）ポリシー タイプセレクタから [IPS] > [グローバル相関（Global Correlation）] > [インスペクション/レピュテーション（Inspection/Reputation）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次を設定します。

- [グローバル相関インスペクション（Global Correlation Inspection）]：グローバル相関インスペクションをイネーブルにするかどうか。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。インスペクションをディセーブルにするには、このオプションの選択を解除します。
- [グローバル相関の影響（Global Correlation Influence）]：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。次のいずれかを選択します。
  - [限定的（Permissive）]：拒否アクションに対する影響は最も少なくなります。
  - [標準（Standard）]：（デフォルト）。 拒否アクションに対する影響は中程度です。
  - [アグレッシブ（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。
- [レピュテーションフィルタリング（Reputation Filtering）]：レピュテーション フィルタリングをオンにするかオフにするかを選択します。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。
- [グローバル相関をテスト（Test Global Correlation）]：グローバル相関を監査モードに設定するかどうか。監査モードでは、レピュテーション フィルタリングは悪意のある既知のホストへのアクセスを拒否しません。発生した可能性がある内容に関するレポートが単に生成されます。

監査モードを使用すると、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。望ましい効果が得られた場合は、このオプションの選択を解除して、レピュテーション フィルタリングをアクティブ化します。

ネットワーク参加の設定

ネットワーク参加ポリシーを使用して、データを SensorBase ネットワークに送信するようにセンサーを設定します。完全に参加して、すべてのデータを SensorBase ネットワークに送信する

ようにセンサーを設定するか、またはデータは収集するが、潜在的に機密性の高いデータ（トリガー パケットの宛先 IP アドレスなど）は除くようにセンサーを設定することができます。ネットワーク参加および収集されるデータの詳細については、ネットワーク参加について（4 ページ）を参照してください。

関連項目

- グローバル相関について （1 ページ）
- レピュテーションについて （3 ページ）
- グローバル相関の要件および制限 （5 ページ）
- 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 （7 ページ）

ステップ 1 次のいずれかを実行して、[Network Participation] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS]>[グローバル相関（Global Correlation）]>[ネットワーク参加（Network Participation）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS]>[グローバル相関（Global Correlation）]>[ネットワーク参加（Network Participation）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [ネットワーク参加（Network Participation）] リストから、次に示す参加レベルを選択します。

- [オフ（Off）]：いずれのデータも SensorBase ネットワークに提供されません。
- [部分的（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。

（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。

- [フル（Full）]：すべてのデータが SensorBase ネットワークに提供されます。

ステップ 3 [Full] または [Partial] を選択した場合、[Save] をクリックすると、[Network Participation Disclaimer] ダイアログボックスが開き、免責事項を読んで同意するように要求されます。免責事項をよく読みます。同意する場合は、[同意する（Agree）] をクリックします。

[同意しない（Disagree）] をクリックした場合、ネットワーク参加をイネーブルにすることはできません。設定を [Off] に変更し、ポリシーを保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。