ネットワーク分析ポリシーと侵入ポリシーの概要

「ネットワーク分析ポリシーと侵入ポリシーの概要」の章では、Snort 検査エンジンの概要およびネットワーク分析ポリシーと侵入ポリシーを示します。システム提供とカスタムのネットワーク分析ポリシーと侵入ポリシーを洞察し、これらのポリシーの要件と前提条件を示します。

ネットワーク分析ポリシーと侵入ポリシーの基本

ネットワーク分析ポリシーと侵入ポリシーは、侵入検知および防御の機能の一部として連携して動作します。

- 侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的にモニタおよび分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。これは「IDS」とも呼ばれます。
- 侵入防御という用語には、侵入検知の概念が含まれますが、さらにネットワークを通過中の悪意のあるトラフィックをブロックしたり変更したりする機能も追加されます。これは「IPS」とも呼ばれます。

侵入防御の展開では、システムがパケットを検査するときに次のことが行われます。

- **ネットワーク分析ポリシー**は、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。

- **侵入ポリシー**では侵入およびプリプロセッサルール（総称的に「侵入ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映することができます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィックが分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別途ネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。このポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、通知および防御に役立ちます。

システムには、同様の名前（Balanced Security and Connectivity など）が付いたいくつかのネットワーク分析ポリシーおよび侵入ポリシーが付属しており、それらは互いに補完しあい、連携して動作します。システム付属のポリシーを使用することで、Cisco Talos Intelligence Group（Talos）の経験を活用できます。これらのポリシーでは、Talos は侵入ルールとインスペクタルールの状態を設定するとともに、インスペクタとその他の詳細設定の初期設定も提供します。

また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシーの設定を調整することで、各自に最も役立つ方法でトラフィックを検査できます。これによって、管理対象デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

Webインターフェイスで同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、Web インターフェイスの左側にナビゲーション パネルが表示され、右側にさまざまな設定ページが表示されます。

追加のサポートと情報については、以下のビデオを参照してください。

- Snort 3 基本の概要
- Snort 3 拡張の概要

Snort 検査エンジン

Snort 検査エンジンは、FTDデバイスに不可欠な部分です。検査エンジンは、トラフィックをリアルタイムで分析して、パケットを詳細に検査します。ネットワーク分析ポリシーと侵入ポリシーでは、Snort 検査エンジンの機能を利用して、侵入を検出して保護します。

Snort 3

Snort 3 は Snort 検査エンジンの最新バージョンで、以前のバージョンの Snort と比較して大幅に改善されています。Snort の古いバージョンは Snort 2 です。Snort 3 はより効率的で、パフォーマンスとスケーラビリティが向上します。

Snort 3 はアーキテクチャが再設計され、Snort 2 と比較すると同等のリソースでより多くのトラフィックを検査します。Snort 3 では、トラフィックパーサーを簡単かつ柔軟に挿入できます。Snort 3 には、ルールの記述を容易にし、同等の共有オブジェクトルールを表示できる新しいルールシンタックスも用意されています。

Snort 3 のその他の重要な変更点は次のとおりです。

- 複数の Snort インスタンスを使用する Snort 2 とは異なり、Snort 3 は複数のスレッドを単一の Snort インスタンスに関連付けます。これにより、使用するメモリが少なくなり、Snort のリロード時間が短縮され、より多くの侵入ルールとより大きなネットワークマップがサポートされます。Snort スレッドの数はプラットフォームによって異なり、各プラットフォームの Snort 2 インスタンスの数と同じです。使用方法はほぼ透過的です。
- FTD ごとの Snort バージョン：Snort インスペクションエンジンは FTD 固有であり、FMC 固有ではありません。FMC はそれぞれが Snort のいずれかのバージョン（Snort 2 および Snort 3）である、複数の FTD を管理できます。FMC の侵入ポリシーは一意ですが、システムは、デバイスの選択した検査エンジンに応じて、侵入保護のために Snort 2 または Snort 3 バージョンの侵入ポリシーを適用します。デバイスの検査エンジンの詳細については、Snort 3 の有効化と無効化を参照してください。
- デコーダルール：パケットデコーダルールは、デフォルトの侵入ポリシーでのみ起動します。他のポリシーで有効にしたデコーダルールは無視されます。
- 共有オブジェクトルール：Snort 3 は、すべてでなく一部の共有オブジェクト（SO）の侵入ルール（ジェネレータ ID（GID）が 3 のルール）をサポートします。サポートされていない有効な共有オブジェクトルールはトリガーされません。
- セキュリティ インテリジェンスのマルチレイヤ検査：Snort 2 はマルチレイヤトラフィックの 2 つのレイヤを検査します。Snort 3 は、レイヤに関係なく最も内側の IP アドレスを検出します。
- ハードウェアサポート：Snort 3 はバージョン 7.0 以降の FTD でのみサポートされます。Snort 3 は、ASA 5500-X または Firepower 7000 および 8000 シリーズ デバイスではサポートされていません。
- 管理対象デバイス：バージョン 7.0 の FMC は、バージョン 6.4、6.5、6.6、6.7、および 7.0 の Snort 2 FTD とバージョン 7.0 の Snort 3 FTD を同時にサポートできます。
- Snort バージョンの切り替え時のトラフィックの中断：Snort のバージョンを切り替えると、トラフィックの検査が中断され、展開中にいくつかのパケットがドロップされる可能性があります。

- 統合ポリシー：管理対象の FTD で有効になっている基盤の Snort エンジンのバージョンに関係なく、FMC で設定されたアクセス コントロール ポリシー、侵入ポリシー、およびネットワーク アクセス ポリシーは、ポリシーの適用時にシームレスに機能します。FMC バージョン 7.0 以降のすべての侵入ポリシーには、Snort 2 バージョンと Snort 3 バージョンの 2 つのバージョンがあります。侵入ポリシーは、一意の名前、ベースポリシー、および検査モードを保持するという意味で統合されますが、ポリシーには 2 つのバージョン（Snort 2 バージョンと Snort 3 バージョン）があります。侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンでは、ルール設定の観点からは異なる場合があります。ただし、侵入ポリシーがデバイスに適用されると、システムはデバイスで有効になっている Snort バージョンを自動的に識別し、そのバージョンに設定されたルール設定を適用します。

- Lightweight Security Package（LSP）：SRU を Snort 3 の次世代の侵入ルールと設定の更新に置き換えます。更新をダウンロードすると、Snort 3 LSP と Snort 2 SRU の両方がダウンロードされます。

  LSP の更新では、新規と更新後の侵入ルールとインスペクタルール、既存のルールの変更後の状態、および FMC と FTD バージョン 7.0 以降の変更後のデフォルトの侵入ポリシー設定が提供されます。FMC をバージョン 6.7 以前から 7.0 にアップグレードすると、LSP と SRU の両方がサポートされます。LSP の更新では、システムにより提供されたルールが削除されたり、新しいルールカテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。LSP の更新については、『*Firepower Management Center Configuration Guide*』の最新バージョンの「*Update Intrusion Rules*」のトピックを参照してください。

- Snort 2 と Snort 3 のルールと事前設定のマッピング：Snort 2 と Snort 3 のルールがマッピングされ、マッピングはシステムによって提供されます。ただし、1 対 1 のマッピングではありません。システムによって提供される侵入ベースポリシーは、Snort 2 と Snort 3 の両方に対して事前に設定されており、ルールセットが異なる場合でも同じ侵入防御を提供します。システムによって提供される Snort 2 と Snort 3 のベースポリシーは、同じ侵入防御設定で相互にマッピングされます。詳細については、Snort 2 と Snort 3 のベースポリシーのマッピングの表示を参照してください。

- Snort 2 と Snort 3 ルールオーバーライドの同期：FTD が 7.0 にアップグレードされると、FTD の検査エンジンを Snort 3 バージョンにアップグレードできます。FMC は Snort 2 バージョンの侵入ポリシーの既存のルールのすべてのオーバーライドを、Talos が提供するマッピングを使用して、対応する Snort 3 ルールにマッピングします。ただし、アップグレード後に実行した追加のオーバーライドがある場合や、新しい FTD のバージョン 7.0 をインストール場合は、それらを手動で同期する必要があります。詳細については、Snort 2 のルールと Snort 3 の同期を参照してください。

- カスタム侵入ルール：Snort 3 でカスタム侵入ルールを作成できます。また、Snort 2 に存在するカスタム侵入ルールを Snort 3 にインポートすることもできます。詳細については、Snort 3 のカスタムルールを参照してください。

- ルールグループ：FMC は、システムによって提供されるベースポリシーの一部である Snort 3 ルールをグループ化します。ルールグループはルールの論理グループであり、ルールのアクセシビリティ、ルールのナビゲーション、およびルールグループのセキュリティレベルの制御を強化するための簡単な管理インターフェイスを提供します。

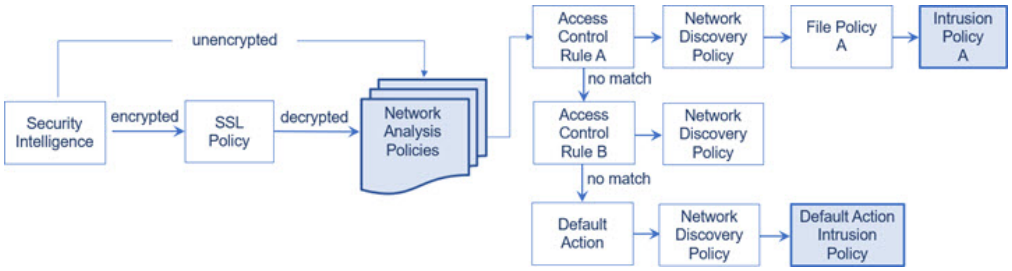
- Snort 2 エンジンと Snort 3 エンジンの切り替え：Snort 3 をサポートする FTD は Snort 2 もサポートできます。Snort 3 から Snort 2 への切り替えは、有効性の観点から推奨されません。ただし、切り替えが必要な場合は、Snort 3 の有効化と無効化の手順に従ってください。

重要 Snort のバージョンは自由に切り替えることができますが、Snort の一方バージョンでの侵入ルールを変更しても、もう一方のバージョンでは自動的に更新されません。Snort の一方のバージョンでルールのルールアクションを変更する場合は、Snort のバージョンを切り替える前に、もう一方のバージョンの変更を必ず複製してください。システムにより提供される同期オプションは、侵入ポリシーの Snort 2 バージョンの変更のみを Snort 3 バージョンに同期します。その逆の同期は行いません。

ポリシーがトラフィックで侵入を検査する方法

アクセスコントロールの展開の一部としてシステムがトラフィックを分析すると、ネットワーク分析（復号化と前処理）フェーズが侵入防御（侵入ルールおよび詳細設定）フェーズとは別にその前に実行されます。

次の図に、インラインでのトラフィック分析、侵入防御、およびネットワーク展開での AMP の順序を簡略化して示します。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序が示されています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



インライン展開（つまり、ルーテッド、スイッチド、トランスペアレントインターフェイスまたはインラインインターフェイスのペアを使用して関連設定がデバイスに展開される展開）では、システムは上図のプロセスのほぼすべての段階において、追加のインスペクションなしでトラフィックをブロックすることができます。セキュリティインテリジェンス、SSLポリシー、ネットワーク分析ポリシー、ファイルポリシー、および侵入ポリシーのすべてで、トラフィックをドロップまたは変更できます。唯一の例外として、パッシブにパケットを検査するネットワーク検出ポリシーは、トラフィック フローに影響を与えることができません。

同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサイベント（総称的に「侵入イベント」とも呼ばれる）は、パケットまたはそのコンテンツがセキュリティリスクを含んでいる可能性を示唆しています。

ヒント SSLインスペクションの設定で暗号化トラフィックの通過が許可されている場合や、SSLインスペクションが設定されていない場合について、この図は、そのような場合のアクセス コントロール ルールによる暗号化トラフィックの処理を反映していません。デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイル インスペクションは無効になっています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

復号化、正規化、前処理：ネットワーク分析ポリシー

デコードと前処理を実行しないと、プロトコルの相違によりパターンマッチングを行えなくなるので、侵入についてトラフィックを適切に評価できません。これらのトラフィック処理タスクは、以下のタイミングでネットワーク分析ポリシーによる処理の対象となります。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた**後**
- 暗号化トラフィックがオプションの SSL ポリシーによって復号化された**後**
- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる**前**

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の3つのTCP/IP層を通ったパケットを復号化し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケットデコーダは、パケットヘッダーとペイロードを、インスペクタや後で侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーのさまざまな異常動作も検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のインスペクタや侵入ルールによる検査用にパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。
- ネットワーク層とトランスポート層のさまざまなインスペクタは、IPフラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

トランスポートおよびネットワークインスペクタの一部の詳細設定は、アクセス コントロールポリシーのターゲットデバイスで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセスコントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルールエンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。
- Modbus、DNP3、CIP、および s7commplus SCADA インスペクタは、トラフィックの以上を検出し、侵入ルールにデータを提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャプロセス、および設備プロセスからのデータをモニタ、制御、取得します。
- 一部のインスペクタでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレートベースの攻撃など、特定の脅威を検出できます。

  侵入ポリシーで、ASCII テキストのクレジットカード番号や社会保障番号などの機密データを検出する機密データインスペクタを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックの前処理を制御します。初期段階では、デフォルトで Balanced Security and Connectivity ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致するトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせてトラフィックの前処理オプションを調整できます。

アクセス コントロール ルール：侵入ポリシーの選択

最初の前処理の後、アクセスコントロールルール（ある場合）はトラフィックを評価します。ほとんどの場合、パケットが一致した最初のアクセス コントロール ルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、ディスカバリ データ、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセスコントロール ルールに一致しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、ディスカバリ データと侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに**関わらず**、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。

ポリシーがトラフィックで侵入を検査する方法 （5 ページ）の図に、インラインの侵入防御と AMP のネットワーク展開を次のように経由するトラフィックのフローを示します。

- アクセス コントロール ルール A により、一致したトラフィックの通過が許可されます。次にトラフィックは、ネットワーク検出ポリシーによるディスカバリ データの検査、ファイル ポリシー A による禁止ファイルおよびマルウェアの検査、侵入ポリシー A による侵入の検査を受けます。
- アクセス コントロール ルール B も一致したトラフィックを許可します。ただし、このシナリオでは、トラフィックは侵入（あるいはファイルまたはマルウェア）について検査されないので、ルールに関連付けられている侵入ポリシーやファイル ポリシーはありません。通過を許可されたトラフィックは、デフォルトでネットワーク検出ポリシーによって検査されます。したがって、この設定を行う必要はありません。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションで、一致したトラフィックを許可しています。次に、トラフィックはネットワーク検出ポリシー、さらにその後侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。

侵入インスペクション：侵入ポリシー、ルール、変数セット

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

侵入ルールとインスペクタ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。

システムには、Cisco Talos インテリジェンス グループ（Talos）によって作成された次のタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされており、変更できません（ただし、送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）。
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- プリプロセッサルール。ネットワーク分析ポリシーのインスペクタとパケットデコーダの検出オプションが関連付けられたルールです。インスペクタルールはコピーしたり、編集したりできません。ほとんどのインスペクタルールはデフォルトで無効になっています。イベントを生成し、インライン展開で、違反パケットをドロップするためにインスペクタを使用するには、ルールを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理する際には、最初にルール オプティマイザが、基準（トランスポート層、アプリケーションプロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルールエンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが3種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキストルールを記述および追加することで、検出を調整できます。Firepower 推奨機能を使用して、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアントアプリケーションプロトコルを、それらの資産を保護するために作成されたルールに関連付けることもできます。

（注） ブロックルールと照合して特定のトラフィックを処理するのに十分なパケットがない場合、システムは残りのトラフィックを他のルールと照合して評価を続行します。残りのトラフィックのいずれかが、ブロックするように設定されているルールに一致すると、セッションはブロックされます。ただし、通過させる残りのトラフィックをシステムが分析すると、トラフィックステータスには、完全なパケットが不足しているルールで保留中と表示されます。

変数セット

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セット使用します。セット内の大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元およ

び宛先の IP アドレスとポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される 1 つのデフォルト変数セットが含まれています。システム提供の共有オブジェクト ルールと標準テキスト ルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 `$HOME_NET` を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 `$EXTERNAL_NET` を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、`$HTTP_SERVERS` 変数および `$HTTP_PORTS` 変数を使用します。

ヒント システム提供の侵入ポリシーを使用する場合でも、シスコでは、デフォルト セットの主要なデフォルト変数を変更すること**強く**推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。高度なユーザは、1 つ以上のカスタム侵入ポリシーとペアリングするために、カスタム変数セットを作成して使用できます。

重要 カスタム変数セットを作成する場合は、カスタム変数セット名の最初の文字として数字を使用しないでください（たとえば、3Snort）。このようにして、FMC の FTD ファイアウォールに設定を展開すると、Snort 3 の検証が失敗します。

侵入イベントの生成

侵入されている可能性を特定すると、システムは侵入イベントまたはプリプロセッサイベント（まとめて侵入イベントと呼ばれることもあります）を生成します。管理対象デバイスはFMCにイベントを送信します。ここで、集約データを確認し、ネットワーク アセットに対する攻撃を的確に把握できます。インライン展開では、管理対象デバイスは、有害であると判明しているパケットをドロップまたは置き換えることができます。

データベース内の各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報、さらに攻撃の送信元とそのターゲットに関するコンテキスト情報が含まれています。パケット ベースのイベントの場合、システムは復号化されたパケット ヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。パケットを検査する侵入ポリシー内の

付随するデコーダルールが有効な場合、システムは後でインスペクタイベントを生成します。

- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、インスペクタはこれを潜在的な攻撃と解釈し、付随するインスペクタルールが有効な場合は、システムによってインスペクタイベントが生成されます。
- 侵入ルールエンジン内では、ほとんどの標準テキストルールおよび共有オブジェクトルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

データベースに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システム提供およびカスタムネットワーク分析ポリシーと侵入ポリシー

新しいアクセス コントロール ポリシーを作成することは、システムを使用してトラフィックフローを管理するための最初のステップの1つです。デフォルトでは、新しく作成されたアクセス コントロール ポリシーは、システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。初期段階では、システムによって提供される *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトです。
- アクセス コントロール ポリシーのデフォルト アクションは、システム付属の *Balanced Security and Connectivity* 侵入ポリシーによる検査に従って、悪意のないトラフィックをすべて許可します。デフォルトアクションはトラフィックの通過を許可するので、侵入ポリシーが悪意のあるトラフィックを検査して潜在的にブロックする前に、検出機能によって、ホスト、アプリケーション、ユーザ データについてトラフィックを検査できます。
- ポリシーは、デフォルトのセキュリティ インテリジェンス オプション（グローバルなブロックリストとブロックなしリストのみ）を使用し、SSLポリシーによる暗号化トラフィッ

クの復号化や、アクセス コントロール ルールを使用したネットワークトラフィックの特別な処理や検査は実行しません。

侵入防御展開を調整するために実行できるシンプルなステップは、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。システムには、これらのポリシーの複数のペアが提供されています。

または、カスタムポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されているインスペクタオプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティのニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システム提供のネットワーク分析ポリシーと侵入ポリシー

システムには、ネットワーク分析ポリシーと侵入ポリシーのペアがいくつか付属しています。システムによって提供されるネットワーク分析と侵入ポリシーを使用することで、Cisco Talos インテリジェンスグループ（Talos）の経験を活用できます。これらのポリシーでは、Talos が侵入ルールとインスペクタルールの状態とともに、インスペクタやその他の詳細設定の初期設定も提供します。

すべてのネットワーク プロファイル、最小トラフィック、または防御ポスチャに対応したシステム付属ポリシーはありません。これらの各ポリシーは一般的なケースとネットワークのセットアップに対応しているため、これらのポリシーに基づいて適切に調整された防御ポリシーを策定することができます。システム付属ポリシーは、変更せずにそのまま使用できますが、カスタム ポリシーのベースとして使用し、カスタム ポリシーを各自のネットワークに合わせて調整することが推奨されます。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境が正確に反映されるように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトのセットにある主要なデフォルトの変数を変更します。

新たな脆弱性が判明すると、Talos は侵入ルールの更新（*Lightweight Security Package*（LSP）ともいう）をリリースします。これらのルールの更新により、システムによって提供されるネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールやインスペクタルールの新規作成または更新、既存ルールの状態の変更、デフォルトのポリシー設定の変更が行われます。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルールカテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効したものとして扱います。変更を有効にするには、更新されたポリシーを再展開する必要があります。

必要に応じて、影響を受けた侵入ポリシーを（単独で、または影響を受けたアクセス コントロール ポリシーと組み合わせて）自動的に再展開するように、ルールの更新を設定できます。

これにより、新たに検出されたエクスプロイトおよび侵入から保護するために展開環境を容易に自動的に最新に維持することができます。

前処理の設定を最新の状態に保つには、アクセス コントロール ポリシーを再展開する**必要があります**。これにより、現在実行されているものとは異なる、関連するSSLポリシー、ネットワーク分析ポリシー、ファイルポリシーが再展開され、前処理とパフォーマンスの詳細設定オプションのデフォルト値も更新できるようになります。

システムに付属しているネットワーク分析ポリシーと侵入ポリシーのペアは以下のとおりです。

Balanced Security and Connectivity ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織および展開タイプにとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続（すべてのリソースに到達可能な）の方がネットワークインフラストラクチャのセキュリティより優先される組織向けに作られています。この侵入ポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

Security over Connectivity ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先される組織向けに作られています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

Maximum Detection ネットワーク分析ポリシーおよび侵入ポリシー

このポリシーは、Security over Connectivity ポリシー以上にネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active 侵入ポリシーでは、すべての侵入ルールと侵入ルールのしきい値を除くすべての詳細設定が無効にされます。このポリシーは、他のシステムによって提供されるポリシーのいずれかで有効になっているルールをベースにするのではなく、独自の侵入ポリシーを作成する場合の出発点を提供します。

（注） 選択されているシステムから提供されるベース ポリシーによって、ポリシーの設定が異なります。ポリシー設定を表示するには、ポリシーの横にある [編集（Edit）] アイコンをクリックしてから、[ベースポリシー（Base Policy）] リンクをクリックします。

カスタムネットワーク分析ポリシーと侵入ポリシーの利点

システムによって提供されるネットワーク分析ポリシーおよび侵入ポリシーに設定されたインスペクタオプション、侵入ルール、およびその他の詳細設定は、組織のセキュリティのニーズに十分に対応しない場合があります。

カスタム侵入ポリシーを作成すると、環境内のシステムのパフォーマンスを向上させ、ネットワークで発生する悪意のあるトラフィックやポリシー違反を重点的に観察できるようになります。設定できるカスタムポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーまたは侵入ポリシーを効率的に管理するために使用できる構成要素です。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシーチェーンの根本的な基礎としてシステム付属ポリシーが含まれています。システム付属のポリシーはルールアップデートによって変更される可能性があるので、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によって展開が影響を受けると、Web インターフェイスは影響を受けたポリシーを失効として扱います。

カスタム ネットワーク分析ポリシーの利点

デフォルトでは、1 つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはインスペクタによって異なりますが、インスペクタやデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用しないインスペクタは無効にできます。たとえば、HTTP Inspect インスペクタは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが含まれてい

ないことが確実な場合は、IIS 特有のトラフィックを検出するインスペクタオプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタムネットワーク分析ポリシーでインスペクタが無効化されているときに、パケットを有効な侵入ルールまたはインスペクタルールと照合して評価するためにインスペクタを使用する必要がある場合、システムはインスペクタを自動的に有効にして使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではインスペクタは無効のままになります。

- 必要に応じて、特定のインスペクタのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートや、Telnet、HTTP、RPC トラフィックを復号化するポートを特定できます。

複雑な環境での高度なユーザの場合は、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを別々に前処理するように調整することができます。さらに、トラフィックのセキュリティ ゾーン、ネットワーク、または VLAN に応じて前処理が制御されるようにこれらのポリシーを設定できます（ASA FirePOWER モジュールでは、VLAN による前処理を制限することはできません）。

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。

カスタム侵入ポリシーの利点

侵入防御を実行するように初期設定して、新規にアクセス コントロール ポリシーを作成した場合、そのポリシーでは、デフォルトアクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、またはデフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。

侵入防御展開をカスタマイズするために、複数の侵入ポリシーを作成し、それぞれがトラフィックを異なる方法で検査するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。

侵入ポリシーの主な機能は、次のように、どの侵入ルールやインスペクタルールを有効にし、どのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効になっていることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。どのルールで悪質なパケットをドロップまたは変更するかを指定できます。
- Firepower 推奨機能を使用すると、ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアント アプリケーション プロトコルを、それらの資産を保護するために作成されたルールに関連付けることができます。
- 必要に応じて、既存のルールの変更や、新しい標準テキストルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出する他のインスペクタは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。
- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。
- Web インターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、syslog ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。これらのポリシー単位のアラート設定に加えて、各ルールまたはルール グループの侵入イベントを通知する電子メール アラートをグローバルに有効化/無効化できます。どの侵入ポリシーがパケットを処理するかに関わらず、ユーザの電子メール アラート設定が使用されます。

カスタム ポリシーの制限

前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは、管理対象デバイスでアクセス コントロール ポリシーにより処理されるすべてのトラフィックを、1つのネットワーク分析ポリシーを使用して前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理と侵入防御フェーズは強調表示されています。

アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が、デフォルトのネットワーク分析ポリシーによってどのように制御されるのか注意してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。ただし、カスタムネットワーク分析ポリシーでインスペクタを無効にしたときに、前処理されたパケットを有効な侵入ルールまたはインスペクタルールと照合して評価する必要がある場合、システムはインスペクタを自動的に有効にして使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではインスペクタは無効なままになります。

（注） インスペクタを無効にするパフォーマンス上の利点を得るには、侵入ポリシーでそのインスペクタを必要とするルールが有効になっていないことを確認する**必要があります**。

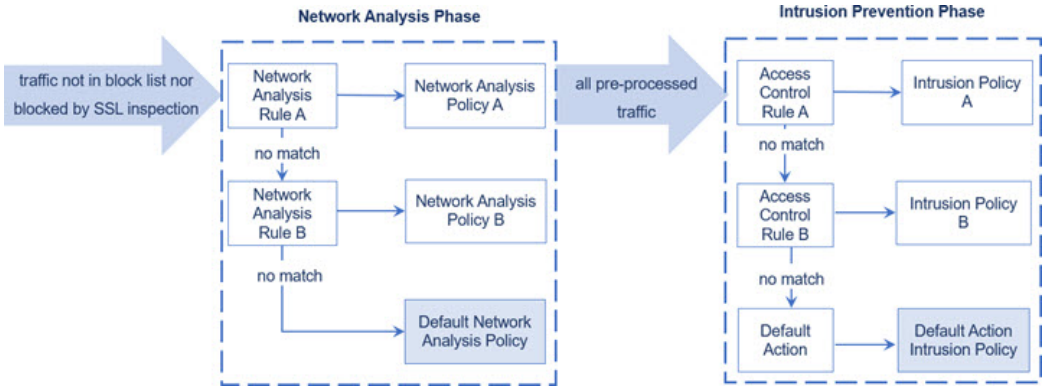
複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーン、ネットワーク、VLAN に合わせて前処理を調整できます。（ASA FirePOWER では、VLAN による前処理を制限することはできません）。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールにはネットワーク分析ポリシーが関連付けられており、ルールに一致するトラフィックの前処理を制御します。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。いずれのネットワーク分析ルールにも一致しないトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、それら独自のプロセスにおいて引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。アクセス コントロール ポリシーを設定するときは、そのポリシーが正しいネットワーク分析ポリシーおよび侵入ポリシーを呼び出して特定のパケットを評価するように、慎重に行う**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図では検出フェーズとファイル/マルウェア インスペクション フェーズが省かれています。また、デフォ

ルトのネットワーク分析ポリシーおよびデフォルトアクションの侵入ポリシーを強調表示しています。



このシナリオでは、アクセス コントロール ポリシーに、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーが設定されています。

- Network Analysis Rule A は、一致するトラフィックを Network Analysis Policy A で前処理します。その後、このトラフィックを Intrusion Policy A で検査されるようにすることができます。
- Network Analysis Rule B は、一致するトラフィックを Network Analysis Policy B で前処理します。その後、このトラフィックを Intrusion Policy B で検査されるようにすることができます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、このトラフィックをアクセスコントロールポリシーのデフォルトアクションに関連付けられた侵入ポリシーによって検査されるようにすることができます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図では、2 つのアクセス コントロール ルールとデフォルト アクションが含まれるアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy A によって検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。トラフィックはその後、Intrusion Policy B によって検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。トラフィックはその後、デフォルトアクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティゾーンのトラフィックの処理をポリシーペアによって制御することを意図している場合に、誤まって、異なるゾーンを使用するように2つのルールの条件を設定したとします。この誤設定により、ト

ラフィックが誤って前処理される可能性があります。したがって、ネットワーク分析ルールおよびカスタム ポリシーを使用した前処理の調整は、**高度な**タスクです。

単一の接続の場合は、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、一部の前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定には影響**しません**。

ネットワーク分析ポリシーと侵入ポリシーのライセンス要件

FTDライセンス

脅威

従来のライセンス

保護

ネットワーク分析と侵入ポリシーの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意（Any）

ユーザロール

- 管理者
- サポートされるドメイン

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。