機密データの検出

ここでは、機密データ検出とその設定方法について説明します。

機密データ検出の基本

社会保障番号、クレジット カード番号、運転免許証番号などのセンシティブ データは、インターネットに意図的に、または誤って漏洩される可能性があります。システムには、ASCII テキストのセンシティブ データに関するイベントを検出し、生成できるセンシティブ データ プロセッサが用意されています。このプロセッサは、特に誤って漏洩されたデータの検出に役立ちます。

グローバル センシティブ データ プリプロセッサ オプションは、プリプロセッサの動作を制御します。以下のことを指定するグローバル オプションを変更できます。

- プリプロセッサが、ルールをトリガーしたパケットで、クレジット カード番号または社会保障番号の下位 4 桁を除くすべての桁を置換するかどうか
- センシティブ データをモニタする、ネットワーク上の宛先ホスト
- イベントの生成基準となる、単一のセッションでの全データ タイプの合計オカレンス数

個別のデータ タイプによって、指定した宛先ネットワーク トラフィックで検出しイベントを生成できるセンシティブ データを特定します。以下のことを指定するデータ タイプ オプションのデフォルト設定を変更できます。

- 検出されたデータ タイプに対して単一のセッションごとのイベントを生成する基準とするしきい値
- 各データ タイプをモニターする宛先ポート
- 各データ タイプをモニターするアプリケーション プロトコル

指定するデータ パターンを検出するためのカスタム データ タイプを作成および変更することができます。たとえば、病院で患者番号を保護するためのデータ タイプを作成したり、大学で固有の番号パターンを持つ学生番号を検出するためのデータ タイプを作成したりすることが考えられます。

システムはトラフィックに対して個別のデータ タイプを照合することによって、TCPセッションごとにセンシティブ データを検出します。侵入ポリシーの、各データ タイプのデフォルト設定およびすべてのデータ タイプに適用されるグローバル オプションのデフォルト設定は変更できます。Firepower システムには、一般的に使用されているデータ タイプがすでに定義されています。カスタム データ タイプを作成することも可能です。

センシティブ データのプリプロセッサ ルールは、各データ タイプに関連付けられます。各データ タイプのセンシティブ データ検出とイベント生成を有効にするには、そのデータ タイプに対応するプリプロセッサ ルールを有効にします。設定ページのリンクを使用すると、センシティブ データ ルールにフィルタリングされたビューが [ルール（Rules）] ページに表示されます。このビューで、ルールを有効または無効にしたり、その他のルール属性を設定したりできます。

変更を侵入ポリシーに保存する際に提示されるオプションによって、データ タイプに関連付けられたルールが有効になっていてセンシティブ データ検出が無効になっている場合には、自動的にセンシティブ データ プリプロセッサを有効にすることができます。

ヒント 機密データ プリプロセッサでは、FTP またはHTTP を使用してアップロードおよびダウンロードされる暗号化されていない Microsoft Word ファイル内の機密データを検出できます。これが可能である理由は、Word ファイルが ASCII テキストとフォーマット設定コマンドを分けてグループ化する方式だからです。

このシステムは、暗号化または難読化された機密データ、あるいは圧縮または符号化された形式の機密データ（たとえば、Base64 でエンコードされた電子メールの添付ファイルなど）の検出は行いません。たとえば、システムは電話番号 (555)123-4567 を検出しますが、(5 5 5) 1 2 3 - 4 5 6 7 のようにスペースで難読化されたバージョン、あるいは (555)-123--4567 のようにHTML コードが介在するバージョンは検出しません。ただし、(555)-123-4567 のように、HTMLにコーディングされた番号のパターンの途中にコードが入っていなければ検出されます。

グローバル センシティブ データ検出オプション

グローバル センシティブ データ オプションはポリシーに固有であり、すべてのデータ タイプに適用されます。

マスク

ルールをトリガーしたパケットで、クレジット カード番号および社会保障番号の下位4桁を除くすべての桁を「X」に置換します。Web インターフェイスの侵入イベント パケット ビューおよびダウンロードされたパケットでは、マスクされた番号が表示されます。

ネットワーク

センシティブ データをモニターする1つ以上の宛先ホストを指定します。単一のIPアドレス、アドレスブロック、あるいはこのいずれかまたは両方のカンマ区切りリストを指定できます。空白のフィールドは、`any` として解釈されます。これは、任意の宛先 IP アドレスを意味します。

グローバルしきい値（Global Threshold）

グローバルしきい値イベントの生成基準となる、単一セッションでの全データ タイプの合計オカレンス数を指定します。データ タイプの組み合わせを問わず、プリプロセッサは指定された数のデータ タイプを検出すると、グローバルしきい値イベントを生成します。1 ～ 65535 の値を指定できます。

シスコでは、このオプションに、ポリシーで有効にする個々のデータ タイプに対するしきい値のどれよりも大きい値を設定することを推奨しています。

グローバルしきい値については、以下の点に注意してください。

- 複数のデータ タイプを合わせたオカレンス数を検出して イベントを生成し、インライン展開では、違反パケットをドロップします。 するには、プリプロセッサ ルールの 139:1 を有効にする必要があります。
- プリプロセッサが生成するグローバルしきい値イベントは、セッションあたり最大1件です。
- グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立しています。つまり、グローバルしきい値に達すると、個別データ タイプに対するイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も当てはまります。

個別のセンシティブ データ タイプのオプション

最低でも、カスタム データ タイプごとにイベントしきい値を指定し、モニタする少なくとも1 つのポートまたはアプリケーション プロトコルを指定する必要があります。

各システム定義済みデータ タイプでは、デフォルト値が変更されない限り、アクセス不能な sd_pattern キーワードを使用して、トラフィックで検出する組み込みデータ パターンを定義します。カスタム データ タイプを作成して、そのデータ タイプに対し、単純な正規表現を使用して独自のデータ パターンを指定することもできます。

センシティブ データ タイプは、センシティブ データ検出が有効になっているすべての侵入ポリシーに表示されます。システム提供のデータ タイプは読み取り専用として表示されます。カスタム データ タイプの場合、名前とパターン フィールドは読み取り専用として表示されますが、他のオプションはポリシー固有の値に設定できます。

表 *1*: 個別のデータ タイプのオプション

オプション	説明
データ タイプ	データ タイプの一意の名前を指定します。
しきい値（Threshold）	イベント生成の基準とする、データ タイプのオカレンス数を指定します。1 ～ 255 の値を指定できます。 プリプロセッサが検出したデータ タイプに対して生成するイベント数は、セッションごとに 1 つであることに注意してください。グローバルしきい値イベントと個別データ タイプ イベントは、互いに独立していることにも注意してください。つまり、データ タイプ イベントしきい値に達すると、グローバルイベントしきい値に達しているかどうかに関わらず、プリプロセッサがイベントを生成します。その逆も同様です。
宛先ポート（Destination Ports）	データ タイプでモニターする宛先ポートを指定します。単一のポート、複数のポートをカンマで区切ったリスト、または任意の宛先ポートを意味する any を指定できます。
アプリケーション プロトコル（Application Protocols）	データ タイプでモニタする最大 8 つのアプリケーション プロトコルを指定します。モニタするアプリケーション プロトコルを識別するには、アプリケーション ディテクタをアクティブにする必要があります。 従来のデバイスの場合、この機能には制御ライセンスが必要であることに注意してください。
パターン	検出するパターンを指定します。このフィールドは、カスタム データ タイプの場合にのみ存在します。

関連トピック

ディテクタのアクティブおよび非アクティブの設定

システム提供のセンシティブ データのタイプ

それぞれの侵入ポリシーには、よく使用されるデータ パターンを検出するためのシステム提供のデータ タイプが含まれています。これらのデータ パターンには、クレジット カード番号、

電子メールアドレス、米国の電話番号、および米国の社会保障番号などがあります（番号にはハイフン付きのパターン、ハイフン抜きのパターンがあります）。

それぞれのシステム提供のデータ タイプは、ジェネレータ ID（GID）が 138 に設定された単一のセンシティブ データのプリプロセッサ ルールに関連付けられます。侵入ポリシーで関連する機密データ ルールを有効にして、ポリシーで使用する各データ タイプに対して イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

次の表に、各データ タイプの説明と対応するプリプロセッサ ルールの一覧を示します。

表 *2:* システム提供のセンシティブ データのタイプ

データ タイプ	説明	プリプロセッサ ルール GID
クレジットカード番号	Visa®、MasterCard®、Discover®、および American Express® の 15 桁または 16 桁のクレジット カード番号（通常の区切り文字として使用されるハイフンまたはスペースが含まれるパターンと含まれないパターン）に一致します。また、Luhn アルゴリズムを使用してクレジット カード番号の検査数字を確認します。	138:2
電子メール アドレス	電子メール アドレスに一致します。	138:5
米国の電話番号	米国の電話番号（`(\d{3}) ?\d{3}-\d{4}` のパターンに準拠）に一致します。	138:6
米国の 社会保障番号（ハイフンなし）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用していない番号）に一致します。	138:4
米国の 社会保障番号（ハイフンあり）	米国の 9 桁の社会保障番号（有効な 3 桁のエリア番号と有効な 2 桁のグループ番号が含まれ、ハイフンを使用している番号）に一致します。	138:3

社会保障番号以外の 9 桁の番号からの誤検出を軽減するために、プリプロセッサでは、各社会保障番号の 4 桁のシリアル番号の前にある 3 桁のエリア番号と 2 桁のグループ番号を検証するアルゴリズムを使用します。プリプロセッサは 2009 年 11 月末までの社会保障グループ番号を検証します。

機密データの検出のライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護、または手順に示されているとおり。

機密データの検出の要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

センシティブ データ検出の設定

機密データ検出は、システムのパフォーマンスに非常に大きな影響を与える可能性があるため、シスコでは以下のガイドラインに従うことを推奨しています。

- 基本侵入ポリシーとして [アクティブなルールなし（No Rules Active）] デフォルト ポリシーを選択します。
- 次の設定が対応するネットワーク分析ポリシーで有効になっていることを確認します。
  - **アプリケーション層プリプロセッサ**での **FTP と Telnet の設定**
  - [トランスポートまたはネットワーク レイヤ プロセッサ（Transport/Network Layer Preprocessors）] の下の [IP 最適化（IP Defragmentation）] および [TCP ストリームの構成（TCP Stream Configuration）]

始める前に

クラシックデバイスの場合、この手順には 保護 または Control ライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）] 見出し** > **[侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（  ） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（✎）をクリックします。

ステップ 6 次の選択肢があります。

- グローバル センシティブ データ検出オプション （3 ページ）の説明に従って、グローバル設定を変更します。
- [ターゲット（Targets）] セクションでデータ タイプを選択し、個別のセンシティブ データ タイプのオプション （3 ページ）の説明に従って、データ タイプ構成を変更します。
- カスタムセンシティブデータを検査するには、カスタム機密データ タイプ （11 ページ）を参照してください。

ステップ 7 データ タイプでモニターするアプリケーション プロトコルを追加または削除します。監視対象のアプリケーション プロトコルおよび機密データ （8 ページ）を参照してください。

（注）
FTP トラフィック内の機密データを検出するには、次の点を確認します。

- ファイルポリシーがアクセス コントロール ポリシーに対して有効になっていることを確認します。
- `Ftp data` アプリケーションプロトコルを追加する必要があります。

ステップ 8 オプションで、センシティブ データ プリプロセッサ ルールを表示するには、[センシティブ データ検出のルールの設定（Configure Rules for Sensitive Data Detection）] をクリックします。

リストされているルールを有効または無効にすることができます。[ルール（Rules）]ページで使用可能なその他の操作（ルールの抑制、レートベース攻撃防止など）のセンシティブデータルールも設定できます。詳細については、侵入ルールのタイプを参照してください。

ステップ 9 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

ポリシーでセンシティブ データ プリプロセッサ ルールを有効にして、センシティブ データ検出を有効にしていなければ、変更をポリシーに保存する際に、センシティブデータ検出を有効にするよう求めるプロンプトが出されます。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 侵入イベントを生成する場合は、センシティブ データ検出ルール（138:2、138:3、138:4、138:5、138:6、138:>999999、または 139:1）を有効にします。詳細については、侵入ルー

ルの状態、グローバル センシティブ データ検出オプション （3 ページ）、システム提供のセンシティブ データのタイプ （4 ページ）、およびカスタム 機密データ タイプ （11 ページ）を参照してください。

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出 （10 ページ）

監視対象のアプリケーション プロトコルおよび機密データ

各データ タイプでモニタするアプリケーション プロトコルを最大 8 つ指定できます。選択するアプリケーション プロトコルごとに、少なくとも 1 つのディテクタを有効にする必要があります。デフォルトでは、すべてのディテクタがアクティブになっています。有効になっているディテクタがないアプリケーション プロトコルについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザ定義ディテクタが有効になります。

各データ タイプをモニタするアプリケーション プロトコルまたはポートを少なくとも 1 つ指定する必要があります。ただし、FTP トラフィックでセンシティブ データを検出する場合を除き、シスコでは最も包括的なカバレッジにするために、アプリケーション プロトコルを指定する際には対応するポートを指定することを推奨しています。たとえば、HTTP を指定するとしたら、既知の HTTP ポート 80 を設定することお勧めします。このように設定すると、ネットワークの新しいホストが HTTP を実装する場合には、システムは新しい HTTP アプリケーション プロトコルを検出する間、ポート 80 をモニタします。

FTP トラフィックでセンシティブ データを検出する場合は、`FTP data` アプリケーション プロトコルを指定する必要があります。この場合、ポート番号を指定する利点はありません。

関連トピック

ディテクタのアクティブおよび非アクティブの設定
特別なケース：FTP トラフィックでのセンシティブ データの検出 （10 ページ）

モニター対象のアプリケーション プロトコルの選択

モニター対象のアプリケーション プロトコルは、システムが提供するセンシティブ データ タイプとカスタムのセンシティブ データ タイプの両方で指定できます。選択するアプリケーション プロトコルはポリシー固有になります。

始める前に

クラシックデバイスの場合、この手順には Control ライセンスが必要です。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]**を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（）をクリックします。

ステップ 6 [データ タイプ（Data Types）] の下でデータ タイプの名前をクリックします。

ステップ 7 [アプリケーションプロトコル（Application Protocols）] フィールドの横にある [編集（Edit）]（） をクリックします。

ステップ 8 次の選択肢があります。

- モニターするアプリケーションプロトコルを追加するには、[使用可能（Available）] リストからアプリケーションプロトコルを 1 つ以上選択して、右矢印（[>]）をクリックします。モニタするアプリケーション プロトコルは、8 つまで追加できます。
- モニター対象からアプリケーションプロトコルを削除するには、[有効（Enabled）] リストから削除するプロトコルを選択して、左矢印（[<]）をクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 最後のポリシーの確定以降に、このポリシーに加えた変更を保存するには、ナビゲーション ウィンドウで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

特別なケース：FTP トラフィックでのセンシティブ データの検出 （10 ページ）

特別なケース：FTP トラフィックでのセンシティブ データの検出

一般に、センシティブデータをモニタするトラフィックを決めるには、導入でのモニタ対象のポートを指定するか、アプリケーション プロトコルを指定します。

ただし、FTP トラフィックでセンシティブ データを検出するには、ポートまたはアプリケーション プロトコルを指定するだけでは不十分です。FTP トラフィックのセンシティブ データは、FTPアプリケーションプロトコルのトラフィックで検出されますが、FTPアプリケーション プロトコルは断続的に発生し、一時的なポート番号を使用するため、センシティブ データを検出するのが困難です。FTP トラフィックでセンシティブデータを検出するには、以下の設定を含めることが**必須**となります。

- `FTP data` アプリケーション プロトコルを指定すると、FTP トラフィックでのセンシティブ データの検出が可能になります。

  FTP トラフィックでセンシティブ データを検出するという特殊な場合では、`FTP data` アプリケーションプロトコルを指定すると、検出が呼び出される代わりに、FTP トラフィックでセンシティブ データを検出するために FTP/Telnet プロセッサの高速処理が呼び出されます。

- FTP データ ディテクタが有効であることを確認します（デフォルトで有効にされています）。
- 設定に、センシティブデータをモニターするポートが少なくとも 1 つ含まれていることを確認します。
- ファイルポリシーがアクセス コントロール ポリシーに対して有効になっていることを確認します。

FTP トラフィックでセンシティブデータを検出することだけが目的の場合を除き（そのような場合はほとんどありません）、FTP ポートを指定する必要はありません。通常のセンシティブデータ設定には、HTTP ポートや電子メール ポートなどの他のポートが含まれることになります。モニター対象の FTP ポートを 1 つだけ指定し、他のポートを指定しない場合、シスコでは FTP コマンド ポート `23` を指定することを推奨しています。

関連トピック

FTP/Telnet デコーダ
ディテクタのアクティブおよび非アクティブの設定
センシティブ データ検出の設定 （6 ページ）

カスタム 機密データ タイプ

作成するカスタム データ タイプごとに、単一の機密データ プリプロセッサ ルールも作成します。このルールのジェネレータ ID（GID）は 138 で、[Snort ID]（SID）は 1000000 以上（これは、ローカル ルールの SID）です。

ポリシーで使用する各カスタム データ タイプに対し、関連付けられた機密データ ルールを有効にして検出を有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。 する必要があります。

機密データ ルールを有効にするには、設定ページに表示されるリンクを利用できます。このリンクを使用すると、すべてのシステム定義済み機密データ ルールおよびカスタム機密データ ルールを表示するフィルタリングされたビューの侵入ポリシーの [ルール（Rules）] ページが表示されます。また、侵入ポリシーの [ルール（Rules）] ページでローカル フィルタリング カテゴリを選択することで、カスタム機密データ ルールをカスタム ローカル ルールとともに表示できます。カスタム機密データ ルールは、侵入ルール エディタ ページ（**[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]**）には表示されないことに注意してください。

カスタムデータタイプを作成すると、システム内の任意の侵入ポリシーで有効にすることができます。カスタム データ タイプを有効にするには、そのカスタム データ タイプの検出に使用するポリシーで、関連する機密データ ルールを有効にする必要があります。

カスタム機密データ タイプのデータ パターン

カスタム データ タイプのデータ パターンを定義するには、以下の要素からなる単純な正規表現のセットを使用します。

- 3 つのメタ文字
- メタ文字をリテラル文字として使用するためのエスケープ文字
- 6 文字クラス

メタ文字は正規表現内で特別な意味を持つリテラル文字です。

表 *3:* 機密データ パターンのメタ文字

メタ文字	説明	例
?	先行する文字またはエスケープ シーケンスのゼロまたは 1 つのオカレンスに一致します。つまり、先行する文字またはエスケープ シーケンスはオプションです。	`colou?r` は、`color` または `colour` に一致します。
{n}	先行する文字またはエスケープ シーケンスの n 回の繰り返しに一致します。	たとえば、`\d{2}` は `55`、`12` などに `\l{3}` は `AbC`、`www` など、`\w{3}` は `a1B`、25C など、`x{5}` は`xxxxx` に一致します

メタ文字	説明	例
\	メタ文字を実際の文字として使用できます。また、事前定義された文字クラスを指定するためにも使われます。	\? は疑問符、\\ はバックスラッシュ、\d は数字に一致します。

特定の文字をリテラル文字として機密データ プリプロセッサに正しく解釈させるには、バックスラッシュで文字をエスケープする必要があります。

表 *4*: 機密データ パターンのエスケープ文字

使用するエスケープ文字	表現されるリテラル文字
\?	?
\{	{
\}	}
\\	\

カスタム機密データ パターンを定義するときは、文字クラスを使用できます。

表 *5*: 機密データ パターンの文字クラス

文字クラス	説明	文字クラスの定義
\d	ASCII 文字の数字 0 ～ 9 に一致します。	0 ～ 9
\D	ASCII 文字の数字ではないバイトに一致します。	0 ～ 9 以外
\l （小文字の「エル」）	任意の ASCII 文字に一致します。	a ～ zA ～ Z
\L	ASCII 文字ではないバイトに一致します。	a ～ z および A ～ Z 以外
\w	任意の ASCII 英数字に一致します。 PCRE 正規表現とは異なり、アンダースコア（_）は含まれないことに注意してください。	a ～ z、A ～ Z、および 0 ～ 9
\W	ASCII 英数字でないバイトに一致します。	a ～ z、A ～ Z、および 0 ～ 9 以外

プリプロセッサは、そのまま入力された文字を、正規表現の一部ではなく、リテラル文字として扱います。たとえば、データ パターン 1234 は 1234 に一致します。

以下に、システム定義済み機密データ ルール 138:4 で使用するデータ パターンの例を示します。このパターンでは、エスケープされた数値の文字クラス、複数個を示すメタ文字およびオ

プション指定子のメタ文字、リテラル ハイフン（-）文字、および左右の括弧 () 文字を使用して、米国の電話番号を検出します。

```
(\d{3}) ?\d{3}-\d{4}
```

カスタム データ パターンを作成する際には注意が必要です。以下に、電話番号を検出するための別のデータ パターンを示します。このパターンでは有効な構文を使用しているものの、多数の誤検出が発生する可能性があります。

```
(?\d{3})? ?\d{3}-?\d{4}
```

上記の2番目の例では、オプションの括弧、オプションのスペース、オプションのハイフンを組み合わせているため、目的とする以下のパターンの電話番号が検出されます。

- `(555)123-4567`
- `555123-4567`
- `5551234567`

ただし、2 番目の例のパターンでは、以下の潜在的に無効な無効なパターンも検出されて、結果的に誤検出となります。

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

最後に、説明目的の極端な例として、小規模な企業ネットワーク上のすべての宛先トラフィックで小さいイベントしきい値を使用して、小文字の a を検出するデータ パターンを作成するとします。このようなデータ パターンは、わずか数分で文字通り数百万ものイベントを生成することになり、システムを過負荷に陥らせる可能性があります。

カスタム センシティブ データ タイプの設定

データ タイプのセンシティブ データ ルールがいずれかの侵入ポリシーで有効にされている場合、そのデータ タイプを削除することはできません。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブデータの検出（Sensitive Data Detection）] の横にある[編集（Edit）]（）をクリックします。

ステップ 6 [データタイプ（Data Types）] の横にある[追加（Add）] ()をクリックします。

ステップ 7 データ タイプの名前を入力します。

ステップ 8 このデータ タイプで検出するパターンを入力します。カスタム機密データ タイプのデータ パターン （11 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 必要に応じて、データ タイプ名をクリックし、個別のセンシティブ データ タイプのオプション （3 ページ）で説明されているオプションを変更します。

ステップ 11 必要に応じて、[削除（Delete）]（）をクリックしてカスタムデータタイプを削除し、[OK] をクリックして確認します。

（注）
いずれかの侵入ポリシーでデータ タイプのセンシティブ データ ルールが有効になっている場合は、そのデータ タイプを削除できないことが警告されます。再度削除を試みる前に、影響を受けるポリシーでセンシティブ データ ルールを無効にする必要があります。侵入ルール状態の設定を参照してください。

ステップ 12 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- データ型を使用する各ポリシーで、関連付けられたカスタム センシティブ データの前処理ルールを有効にします。侵入ルール状態の設定を参照してください。
- 設定変更を展開します設定変更の展開を参照してください。

関連トピック

カスタムセンシティブ データ タイプの編集 （14 ページ）

カスタムセンシティブ データ タイプの編集

カスタム センシティブ データ タイプのすべてのフィールドを編集できます。ただし、名前またはパターン フィールドを変更すると、システム内のすべての侵入ポリシーのこれらの設定が変更されることに注意してください。その他のオプションは、ポリシー固有の値に設定できます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）] 見出し > [侵入（Intrusion）]** を選択します。

ステップ 2 編集するポリシーの横にある [Snort 2バージョン（Snort 2 Version）] をクリックします。

代わりに [表示（View）]（👁） 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション ウィンドウで [詳細設定（Advanced Settings）] をクリックします。

ステップ 4 [特定の脅威検出（Specific Threat Detection）] の下の [センシティブ データ検出（Sensitive Data Detection）] が無効になっている場合は、[有効（Enabled）] をクリックします。

ステップ 5 [センシティブ データ検出（Sensitive Data Detection）] の横にある [編集（Edit）] をクリックします。

ステップ 6 [ターゲット（Targets）] セクションで、カスタム データ タイプの名前をクリックします。

ステップ 7 [データ タイプの名前およびパターンの編集（Edit Data Type Name and Pattern）] をクリックします。

ステップ 8 データ タイプの名前およびパターンを変更します。カスタム機密データ タイプのデータ パターン （11 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 残りのオプションをポリシー固有の値に設定します。個別のセンシティブ データ タイプのオプション （3 ページ）を参照してください。

ステップ 11 最後のポリシー確定後にこのポリシーで行った変更を保存するには、ナビゲーションパネルで [ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

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。