POP インスペクタ

POP インスペクタの概要

タイプ	インスペクタ（サービス）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	`stream_tcp`
有効	`true`

Post Office Protocol バージョン 3（POP3）を使用すると、電子メールクライアントはリモートの POP3 サーバーからメッセージを取得できるようになります。POP3 サーバーは、安全でないセッションには TCP ポート 110 を使用し、POP over SSL/TLS には TCP ポート 995 を使用します。

`pop` インスペクタは、POP トラフィックを検出し、POP コマンドと応答を分析します。

`pop` インスペクタは、POP メッセージのコマンド、ヘッダー、および本文のセクションを識別し、Multi-purpose Internet Mail Extension（MIME）添付ファイルを抽出し、復号化することができます。`pop` インスペクタは、MIME 添付ファイルを処理します。これには、複数の添付ファイルや、複数のパケットにまたがる大きな添付ファイルが含まれます。

`pop` インスペクタは、POP メッセージを識別し、Snort 許可リストに追加します。有効にすると、侵入ルールは異常な POP トラフィックの発生時にイベントを生成します。

POP インスペクタのパラメータ

（注） 復号化またはMIME電子メール添付ファイルの復号化が不要な場合の抽出の場合は、複数の添付ファイルや複数のパケットにまたがる大きな添付ファイルが含まれている可能性があります。

最大値は、`b_64_decode_depth`、`bitnc_decode_depth`、`qp_decode_depth`、または`uu_decode_depth`パラメータの値が次の点で異なる場合に使用されます。

- デフォルトのネットワーク分析ポリシー
- 同じアクセス コントロール ポリシーのネットワーク分析ルールによって呼び出される、他のカスタム ネットワーク分析ポリシー

POP サービスの設定

`binder`インスペクタは、POPサービスの設定を定義します。詳細については、『バインダインスペクタの概要』を参照してください。

例：

```
[
    {
        "when": {
           "service": "pop",
           "role": any
        },
        "use": {
           "type": "pop"
        }
    }
]
```

b_64_decode_depth

各 Base64 エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 142:4 を有効にして、このパラメーターのイベントを生成し、インライン展開で、デコードが失敗したときに問題のあるパケットをドロップすることができます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

bitenc_decode_depth

バイトの最大数を指定し、エンコードされていない各MIME電子メールの添付ファイルから抽出します。65535 未満の整数を指定するか、または 0 を指定して、エンコードされていない MIME添付ファイルの抽出を無効にすることができます。抽出するバイト数に制限を設定しない場合は、-1 を指定します。これらの添付ファイルのタイプには、7 ビット、8 ビット、バイナリ、ならびにプレーンテキスト、JPEG イメージと PNG イメージ、および MP4 ファイルなど、マルチパートのコンテンツタイプが含まれます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

decompress_pdf

MIME 添付ファイルの `application/pdf` （PDF） ファイルを圧縮解除するかどうかを指定します。

このパラメータのイベントを生成し、インライン展開で問題のあるパケットをドロップするには、ルール 142:8 を有効にします。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

decompress_swf

MIME 添付ファイルの `application/vnd.adobe.flash-movie` （SWF）の圧縮を解除するかどうかを指定します。

このパラメータのイベントを生成し、インライン展開で問題のあるパケットをドロップするには、ルール 142:8 を有効にします。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

decompress_vba

MIME 添付ファイルの Microsoft Office Visual Basic for Applications のマクロファイルの圧縮を解除するかどうかを指定します。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

decompress_zip

MIME 添付ファイルのアプリケーション/zip（ZIP）ファイルを解凍するかどうかを指定します。

このパラメータのイベントを生成し、インライン展開で問題のあるパケットをドロップするには、ルール 142:8 を有効にします。

型：ブール値

有効な値：`true`、`false`

デフォルト値：`false`

qp_decode_depth

各 quoted-printable（QP）エンコード MIME 電子メール添付ファイルから抽出してデコードできる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 142:5 を有効にしてこのパラメータのイベントを生成し、インライン展開で、（エンコードが正しくないか、またはデータが壊れていることが原因で）復号化が失敗した場合に問題のあるパケットをドロップすることができます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

uu_decode_depth

各 Unix-to-Unix エンコード（UU エンコード）MIME 電子メール添付ファイルから抽出して復号化できる最大バイト数を指定します。65535 未満の整数を指定するか、または 0 を指定して復号化を無効にすることができます。復号化するバイト数に制限を設定しない場合は、-1 を指定します。

ルール 142:7 を有効にしてこのパラメータのイベントを生成し、インライン展開で、（エンコードが正しくないか、またはデータが壊れていることが原因で）復号化が失敗した場合に問題のあるパケットをドロップすることができます。

型：整数

有効な範囲：`-1` 〜 `65535`

デフォルト値：`-1`

POP インスペクタのルール

`pop` インスペクタ ルールを有効にし、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。。

表 *1 : POP* インスペクタのルール

GID:SID	ルール メッセージ
142:1	不明な POP3 コマンド（unknown POP3 command）
142:2	不明な POP3 応答（unknown POP3 response）
142:4	Base64 の復号化に失敗した（base64 decoding failed）
142:5	Quoted-Printable の復号化に失敗した（quoted-printable decoding failed）
142:7	Unix-to-Unix の復号化に失敗した（Unix-to-Unix decoding failed）
142:8	ファイルの圧縮解除に失敗した（file decompression failed）

POP インスペクタの侵入ルールのオプション

vba_data

検出カーソルを Microsoft Office Visual Basic for Applications マクロバッファに設定します。

シンタックス：`vba_data;`

例：`vba_data;`

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。