



IMAP インспекタ

- [IMAP インспекタの概要 \(1 ページ\)](#)
- [IMAP インспекタのパラメータ \(2 ページ\)](#)
- [IMAP インспекタのルール \(4 ページ\)](#)
- [IMAP インспекタの侵入ルールのオプション \(5 ページ\)](#)

IMAP インспекタの概要

タイプ	インспек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спекタが必要	stream_tcp
有効	true

Internet Message Application Protocol (IMAP) は、電子メールクライアントを有効にし、リモート IMAP3 サーバーからメッセージを取得するようにします。IMAP3 サーバーは、安全でないセッションに TCP ポート 143 を使用するか、SSL/TLS を介した IMAP に TCP ポート 993 を使用します。

imap インспекタは、IMAP トラフィックを検出し、IMAP コマンドと応答を分析します。

imap インспекタは、IMAP 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、多目的のインターネットメール拡張 (MIME) 添付ファイルを抽出して復号化することができます。MIME 添付ファイルには、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る場合があります。

imap インспекタは、IMAP トラフィックを識別し、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 IMAP トラフィックの発生時にイベントを生成します。

IMAP インспекタのパラメータ

IMAP サービスの設定

`binder` インспекタは、IMAP サービスの設定を定義します。詳細については、『[バインディング インспекタの概要](#)』を参照してください。

例：

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

`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 141:4 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ため）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

`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 141:8 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 141:8 を有効にします。

型：整数

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 141:8 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 141:5 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 141:7 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、またはデータが破損していることが原因で) 復号化が失敗したときに問題のあるパケットをドロップできます。

型：整数

有効な範囲：-1 ~ 65535

デフォルト値：-1

IMAP インспекタのルール

imap インспекタのルールを有効にし、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: IMAP インспекタのルール

GID:SID	ルール メッセージ
141:1	不明な IMAP3 コマンド (unknown IMAP3 command)
141:2	不明な IMAP3 応答 (unknown IMAP3 response)
141:4	Base64 の復号化に失敗した (base64 decoding failed)
141:5	Quoted-Printable の復号化に失敗した (quoted-printable decoding failed)
141:7	Unix-to-Unix の復号化に失敗した (Unix-to-Unix decoding failed)

GID:SID	ルール メッセージ
141:8	ファイルの圧縮解除に失敗した (file decompression failed)

IMAP インспек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。