# SIP インスペクタ



## SIP 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_udp` |
| 有効 | `true` |

Session Initiation Protocol（SIP）は、1 人以上の参加者を含むリアルタイム呼び出しセッションの作成、変更、および破棄を管理します。SIP が制御できるアプリケーションには、インターネット電話、マルチメディア会議、インスタントメッセージ、オンラインゲーム、ファイル転送などがあります。SIP プロトコルは、テキストベースの要求および応答プロトコルです。

各 SIP 要求には、要求の目的を識別する `method` フィールドと、要求の送信先を指定する `Request-URI` が含まれています。各 SIP 応答のステータス コードは、要求されたアクションの結果を示します。SIP プロトコルは、TCP（ポート 5060）または UDP（ポート 5061）を使用します。

SIP がコールセッションを作成すると、SIP は Real-time Transport Protocol（RTP）を介してオーディオストリームとビデオストリームを送信できます。SIP メッセージの本文には、データチャネルパラメータのネゴシエーション、セッション通知、およびセッションの招待がSession Description Protocol（SDP）の形式で埋め込まれます。

sip インスペクタは、ネットワークトラフィック内の SIP メッセージを検出して分析します。sip インスペクタは、SIP ヘッダーとメッセージ本文を抽出し、SIP メッセージ本文のデータを検出エンジンに渡します。

sip インスペクタは、SIP トラフィックの異常や障害や無効などのコールシーケンスなど既知の脆弱性を検出します。

（注）

- sip インスペクタは RTP メッセージを復号化しません。sip インスペクタは、SDP データで定義されているポートに基づいて RTP チャネルを識別します。
- UDP は通常、SIP でサポートされるメディア セッションを伝送します。sip インスペクタは、復号化された UDP ストリームからセッションの追跡情報を取得します。
- SIP ルールのオプションを使用すると、検索カーソルを SIP パケットヘッダーやメッセージ本文に配置し、パケットの検出を特定の SIP メソッドまたはステータスコードに限定することができます。

# SIP インスペクタのパラメータ

### SIP サービスの設定

binder インスペクタは、SIP 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": {
            "role": "any",
            "service": "sip"
        },
        "use": {
            "type": "sip"
        }
    }
]
```

### ignore_call_channel

オーディオ/ビデオ データ チャネル トラフィックを検査するかどうかを指定します。有効にすると、sip インスペクタはデータ以外のすべての SIP チャネルトラフィックを復号化し、オーディオ/ビデオ SIP データチャネルのトラフィックを無視します。

**型**：ブール値

**有効な値**：true、false

**デフォルト値**：false

### max_call_id_len

Call-IDヘッダーフィールドで許可されるバイトの最大数を指定します。Call-IDフィールドでは、要求と応答のSIPセッションが一位に識別されます。max_call_id_lenが0の場合、sipインスペクタはアラートを生成しません。

ルール140:5を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sipインスペクタは、Call-IDヘッダーの長さがmax_call_id_lenの値より大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 〜 65535

**デフォルト値**：256

### max_contact_len

Contactヘッダーフィールドで許可されるバイトの最大数を指定します。Contactフィールドには、後続のメッセージの連絡先を指定するURIが示されます。値が0の場合、sipインスペクタはアラートを生成しません。

ルール140:15を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sipインスペクタは、Contactヘッダーフィールドの長さがmax_contact_lenの値より大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 〜 65535

**デフォルト値**：256

### max_content_len

メッセージ本文のコンテンツで許可されるバイトの最大数を指定します。値が0の場合、sipインスペクタはアラートを生成しません。

ルール140:16を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。コンテンツの長さがmax_content_lenの値より大きい場合に、sipインスペクタはイベントを生成します。

**型**：整数

**有効な範囲**：0 〜 65535

**デフォルト値**：1024

### max_dialogs

ストリームセッション内で許容されるダイアログの最大数を指定します。ダイアログの数が設定した制限以上の場合、ダイアログの数が指定した最大数を超えない数まで、sipインスペクタは最も古いダイアログをドロップします。

ルール140:27を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。

**型**：整数

**有効な範囲**：1 ～ 4,294,967,295 (max32)

**デフォルト値**：4

### max_from_len

Fromヘッダーフィールドで許可されるバイトの最大数を指定します。Fromフィールドは、メッセージの発信者を識別します。値が 0 の場合、sip インスペクタはアラートを生成しません。

ルール 140:9 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sipインスペクタは、Fromフィールド長さがmax_from_lenの値よりも大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 ～ 65535

**デフォルト値**：256

### max_request_name_len

要求名で許可されるバイトの最大数を指定します。SIP 要求名は、SIP CSeq トランザクション識別子に指定したメソッドの名前を参照します。値が 0 の場合、sip インスペクタはアラートを生成しません。

ルール 140:7 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sip インスペクタは、要求名の長さが max_request_name_len の値よりも大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 ～ 65535

**デフォルト値**：20

### max_requestName_len

max_requestName_len パラメータは推奨されていません。代わりに max_request_name_len パラメータを使用します。

### max_to_len

Toヘッダーフィールドで許可されるバイトの最大数を指定します。Toフィールドは、メッセージの受信側を識別します。値が 0 の場合、sip インスペクタはアラートを生成しません。

ルール 140:11 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sipインスペクタは、Toフィールドの長さがmax_to_lenの値より大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 ～ 65535

**デフォルト値**：256

#### max_uri_len

Request-URI で許可されるバイトの最大数を指定します。Request-URI は、要求したリソースへの接続先パスを示します。値が 0 の場合、sip インスペクタはアラートを生成しません。

ルール 140:3 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sip インスペクタは、Request-URI フィールドの長さが max_uri_len の値より大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 ～ 65535

**デフォルト値**：256

#### max_via_len

Via ヘッダーフィールドで許可されるバイトの最大数を指定します。Via フィールドは、要求で使用するトランスポートと受信者の場所を識別します。値が 0 の場合、sip インスペクタはアラートを生成しません。

ルール 140:13 を有効にしてイベントを生成し、インライン展開で問題のあるパケットをドロップします。sip インスペクタは、Via フィールドの長さが max_via_len の値より大きい場合にイベントを生成します。

**型**：整数

**有効な範囲**：0 ～ 65535

**デフォルト値**：1024

#### 方法

検出する SIP メソッドのリストを指定します。メソッド名では大文字と小文字が区別されません。リスト内のメソッド名を区切るには、コンマまたはスペースを使用します。メソッド名には英字、数字、下線文字のみが使用できます。

**型**：文字列

**有効な値**：ack、benotify、bye、cancel、do、info、invite、join、message、notify、options、prack、publish、quath、refer、register、service、sprack、subscribe、unsubscribe、update

**デフォルト値**： invite cancel ack bye register options

# SIP インスペクタのルール

sip インスペク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 : SIP* インスペクタのルール

| GID:SID | ルール メッセージ |
|---|---|
| 140:2 | 要求 URI が空になっている（empty request URI） |
| 140:3 | URI が長すぎる（URI is too long） |
| 140:4 | コール ID が空になっている（empty call-Id） |
| 140:5 | コール ID が長すぎる（Call-Id is too long） |
| 140:6 | CSeq 番号が大きすぎるかまたは負になっている（CSeq number is too large or negative） |
| 140:7 | CSeq 内の要求名が長すぎる（request name in CSeq is too long） |
| 140:8 | From ヘッダーが空になっている（empty From header） |
| 140:9 | From ヘッダーが長すぎる（From header is too long） |
| 140:10 | To ヘッダーが空になっている（empty To header） |
| 140:11 | To ヘッダーが長すぎる（To header is too long） |
| 140:12 | Via ヘッダーが空になっている（empty Via header） |
| 140:13 | Via ヘッダーが長すぎる（Via header is too long） |
| 140:14 | 連絡先が空になっている（empty Contact） |
| 140:15 | 連絡が長すぎる（contact is too long） |
| 140:16 | コンテンツの長さが大きすぎるか負になっている（content length is too large or negative） |
| 140:17 | パケット内に複数の SIP メッセージがある（multiple SIP messages in a packet） |
| 140:18 | コンテンツ長が一致しない（content length mismatch） |
| 140:19 | 要求名が無効（request name is invalid） |
| 140:20 | 反射攻撃の招待（Invite replay attack） |
| 140:21 | セッション情報の不正な変更（illegal session information modification） |
| 140:22 | 応答ステータスコードが 3 桁の数字ではない（response status code is not a 3 digit number） |
| 140:23 | Content-type ヘッダーが空になっている（empty Content-type header） |

| GID:SID | ルール メッセージ |
|---|---|
| 140:24 | SIP バージョンが無効（SIP version is invalid） |
| 140:25 | 要求の METHOD と CSEQ ヘッダーが一致しない（mismatch in METHOD of request and the CSEQ header） |
| 140:26 | メソッドが不明（method is unknown） |
| 140:27 | セッション内のダイアログの最大数に到達した（maximum dialogs within a session reached） |

# SIP インスペクタの侵入ルールのオプション

### sip_method

SIP 要求メソッドは要求の目的を識別します。`sip_method` キーワードを使用して、SIP 要求のメソッドを照合します。メソッド名では大文字と小文字が区別されません。複数のメソッド名はコンマで区切ります。

**型**：文字列

**シンタックス**：`sip_method: <methods>;`

**有効な値**：`ack`、`benotify`、`bye`、`cancel`、`do`、`info`、`invite`、`join`、`message`、`notify`、`options`、`prack`、`publish`、`quath`、`refer`、`register`、`service`、`sprack`、`subscribe`、`unsubscribe`、`update`

**例**： `sip_method: "ack,service,info,bye";`

### sip_stat_code

SIP応答には、3桁のステータスコードが含まれます。SIPステータスコードは、要求したアクションの結果を示します。`sip_stat_code` キーワードを使用して、SIP応答を指定したステータスコードと照合します。

3 桁のステータスコードの最初の桁を表す 1 桁の数字、3 桁の数字、またはいずれかの数字の組み合わせを使用した数字のコンマ区切りのリストを指定できます。リスト内のいずれか1つの番号が SIP 応答内のコードに一致する場合、そのリストが一致します。

**型**：整数

**シンタックス**：`sip_stat_code: <codes>;`

**有効な範囲**：

- `1 〜 9`
- `100 〜 999`

**例**： `sip_stat_code: "1";`

表 *2: SIP* パラメータ値とステータスコード

| パラメータ値 | 検出されたステータスコード | 説明 |
|---|---|---|
| 189 | 189 | 特定のステータスコードを設定します。 |
| 1 | 100 ～ 199 | 1 桁の数字を設定します。 |
| 222, 3 | 222; 300 ～ 399 | 3 桁または 1 桁の数字のコンマ区切りのリストを設定します。 |

### sip_header

`sip_header` キーワードを使用して、抽出された SIP ヘッダーバッファの先頭に検出カーソルを配置します。検査をヘッダーフィールドに制限します。

**シンタックス**：`sip_header;`

**例**：`sip_header;`

### sip_body

`sip_body` キーワードを使用して、抽出された SIP メッセージの本文の先頭に検出カーソルを配置します。検査をメッセージの本文に制限します。

**シンタックス**：`sip_body;`

**例**：`sip_body;`

（注） `sip` インスペクタはメッセージの本文全体を抽出して、ルールエンジンで使用できるようにします。ルールエンジンは、Session Description Protocol（SDP）コンテンツの検索に限定されません。

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。