IEC104 インスペクタ

IEC104 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	`false`

IEC 60870-5-104（IEC104）プロトコルは、電力システム間で遠隔制御メッセージを交換するための通信規格について説明します。IEC104 プロトコルは TCP ポート 2404 を使用します。

`iec104` インスペクタは、ネットワークトラフィック内の IEC104 メッセージを検出します。`iec104` インスペクタは、複数のフレームにまたがるメッセージを組み合わせるか、または1つのフレーム内で複数のメッセージを分割することで、IEC104 メッセージを分析し、正規化します。

有効にすると、侵入ルールのオプションは、IEC104 アプリケーションプロトコル制御情報（APCI）タイプとアプリケーション サービス データ ユニット（ASDU）機能コードにアクセスできるようになります。

IEC104 インスペクタのパラメータ

IEC104 TCP ポートの設定

binder インスペクタは、IEC104 TCP ポート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": "server",
            "proto": "tcp",
            "ports": "2404"
         },
        "use": {
            "type": "iec104"
        }
    }
]
```

（注） iec104 インスペクタはパラメータを提供しません。

IEC104 インスペクタのルール

iec104 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 : IEC104* インスペクタのルール

GID:SID	ルール メッセージ
151:1	IEC104 APCI ヘッダーの長さが、指定された IEC104 ASDU タイプ ID に必要な長さと一致しない（Length in IEC104 APCI header does not match the length needed for the given IEC104 ASDU type id）
151:2	IEC104 開始バイトが 0x68 と一致しない（IEC104 Start byte does not match 0x68）
151:3	予約済みの IEC104 ASDU タイプ ID は使用中になっている（Reserved IEC104 ASDU type id in use）
151:4	IEC104 APCI U 予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI U Reserved field contains a non-default value）

GID:SID	ルール メッセージ
151:5	IEC104 APCI U メッセージタイプが無効な値に設定された（IEC104 APCI U message type was set to an invalid value）
151:6	IEC104 APCI S 予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI S Reserved field contains a non-default value）
151:7	IEC104 APCI I 要素数がゼロに設定されている（IEC104 APCI I number of elements set to zero）
151:8	IEC104 APCI I 機能をサポートしていない ASDU に SQ ビットが設定されている（IEC104 APCI I SQ bit set on an ASDU that does not support the feature）
151:9	IEC104 APCI I 機能をサポートしていない ASDU で要素の数が 2 以上に設定されている（IEC104 APCI I number of elements set to greater than one on an ASDU that does not support the feature）
151:10	IEC104 APCI I 初期化の原因が予約値に設定されている（IEC104 APCI I Cause of Initialization set to a reserved value）
151:11	IEC104 APCI I 問い合わせコマンドの修飾子が予約済みの値に設定されている（IEC104 APCI I Qualifier of Interrogation Command set to a reserved value）
151:12	IEC104 APCI I カウンタ問い合わせコマンドの修飾子の要求パラメータが予約済みの値に設定されている（IEC104 APCI I Qualifier of Counter Interrogation Command request parameter set to a reserved value）
151:13	IEC104 APCI I 測定値のパラメータの修飾子のパラメータの種類が予約済みの値に設定されている（Qualifier of Parameter of Measured Values kind of parameter set to a reserved value）
151:14	IEC104 APCI I 測定値のパラメータの修飾子のローカルパラメータの変更が技術的に有効だが未使用の値に設定されている（Qualifier of Parameter of Measured Values local parameter change set to a technically valid but unused value）
151:15	IEC104 APCI I 測定値のパラメータの修飾子のパラメータオプションが技術的に有効だが未使用の値に設定されている（IEC104 APCI I Qualifier of Parameter of Measured Values parameter option set to a technically valid but unused value）
151:16	IEC104 APCI I パラメータアクティベーションの修飾子が予約済みの値に設定されている（IEC104 APCI I Qualifier of Parameter Activation set to a reserved value）

GID:SID	ルール メッセージ
151:17	IEC104 APCI I コマンドの修飾子が予約値に設定されている（Qualifier of Command set to a reserved value）
151:18	IEC104 APCI I リセットプロセスの修飾子が予約値に設定されている（Qualifier of Reset Process set to a reserved value）
151:19	IEC104 APCI I ファイルの準備完了修飾子が予約値に設定されている（File Ready Qualifier set to a reserved value）
151:20	IEC104 APCI I セクションの準備完了修飾子が予約済みの値に設定されている（Section Ready Qualifier set to a reserved value）
151:21	IEC104 APCI I 選択して呼び出しの修飾子が予約値に設定されている（Select and Call Qualifier set to a reserved value）
151:22	IEC104 APCI I 最終セクションまたはセグメントの修飾子が予約値に設定されている（Last Section or Segment Qualifier set to a reserved value）
151:23	IEC104 APCI I 応答確認のファイルまたはセクションの修飾子が予約済みの値に設定されている（Acknowledge File or Section Qualifier set to a reserved value）
151:24	IEC104 APCI I 構造修飾子が効力がないメッセージに設定されている（Structure Qualifier set on a message where it should have no effect）
151:25	IEC104 APCI I シングルポイント情報予約済みフィールドにデフォルト以外の値が含まれている（Single Point Information Reserved field contains a non-default value）
151:26	IEC104 APCI I ダブルポイント情報予約済みフィールドにデフォルト以外の値が含まれている（Double Point Information Reserved field contains a non-default value）
151:27	IEC104 APCI I 送信原因が予約値に設定されている（Cause of Transmission set to a reserved value）
151:28	IEC104 APCI I 送信の原因がASDU に許可されていない値に設定されている（Cause of Transmission set to a value not allowed for the ASDU）
151:29	IEC104 APCI I 無効な 2 オクテットの共通アドレス値が検出された（IEC104 APCI I invalid two octet common address value detected）
151:30	IEC104 APCI I 品質記述子構造の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Quality Descriptor Structure Reserved field contains a non-default value）

GID:SID	ルール メッセージ
151:31	IEC104 APCI I 保護装置構造のイベントの品質記述子の予約済みフィールドにデフォルト以外の値が含まれている（Quality Descriptor for Events of Protection Equipment Structure Reserved field contains a non-default value）
151:32	IEC104 APCI I IEEE STD 754 値が NaN になる（IEEE STD 754 value results in NaN）
151:33	IEC104 APCI I IEEE STD 754 値が無限大になる（IEC104 APCI I IEEE STD 754 value results in infinity）
151:34	IEC104 APCI I 保護装置構造の単一イベントの予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Single Event of Protection Equipment Structure Reserved field contains a non-default value）
151:35	IEC104 APCI I 保護装置構造の開始イベントの予約フィールドにデフォルト以外の値が含まれている（IEC104 APCI I Start Event of Protection Equipment Structure Reserved field contains a non-default value）
151:36	IEC104 APCI I 出力回路情報構造の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Output Circuit Information Structure Reserved field contains a non-default value）
151:37	IEC104 APCI I 異常な固定テストビットパターンが検出された（IEC104 APCI I Abnormal Fixed Test Bit Pattern detected）
151:38	IEC104 APCI I 単一コマンド構造の予約済みフィールドにデフォルト以外の値が含まれている（Single Command Structure Reserved field contains a non-default value）
151:39	IEC104 APCI I ダブルコマンド構造に無効な値が含まれている（Double Command Structure contains an invalid value）
151:40	IEC104 APCI I 規制ステップコマンド構造の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Regulating Step Command Structure Reserved field contains a non-default value）
151:41	IEC104 APCI I Time2a ミリ秒が許容範囲外に設定されている（IEC104 APCI I Time2a Millisecond set outside of the allowable range）
151:42	IEC104 APCI I Time2a の分が許容範囲外に設定されている（IEC104 APCI I Time2a Minute set outside of the allowable range）
151:43	IEC104 APCI I Time2a の分の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Time2a Minute Reserved field contains a non-default value）

GID:SID	ルール メッセージ
151:44	IEC104 APCI I Time2a の時間が許容範囲外に設定されている（IEC104 APCI I Time2a Hours set outside of the allowable range）
151:45	IEC104 APCI I Time2a の時間の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Time2a Hours Reserved field contains a non-default value）
151:46	IEC104 APCI I Time2a の日が許容範囲外に設定されている（IEC104 APCI I Time2a Day of Month set outside of the allowable range）
151:47	IEC104 APCI I Time2a の月が許容範囲外に設定されている（IEC104 APCI I Time2a Month set outside of the allowable range）
151:48	IEC104 APCI I Time2a の月の予約済みフィールドにデフォルト以外の値が含まれている（IEC104 APCI I Time2a Month Reserved field contains a non-default value）
151:49	IEC104 APCI I Time2a の年が許容範囲外に設定されている（IEC104 APCI I Time2a Year set outside of the allowable range）
151:50	IEC104 APCI I Time2a 年の予約フィールドにデフォルト以外の値が含まれている（Time2a Year Reserved field contains a non-default value）
151:51	IEC104 APCI I セグメント長に null 値が検出された（IEC104 APCI I a null Length of Segment value has been detected）
151:52	IEC104 APCI I セグメント長に無効な値が検出された（IEC104 APCI I an invalid Length of Segment value has been detected）
151:53	IEC104 APCI I ファイルのステータスが予約済みの値に設定されている（IEC104 APCI I Status of File set to a reserved value）
151:54	IEC104 APCI I セットポイントコマンド ql フィールドの修飾子が予約済みの値に設定されている（IEC104 APCI I Qualifier of Set Point Command ql field set to a reserved value）

IEC104 インスペクタの侵入ルールのオプション

iec104_apci_type

IEC104 メッセージが、オプションで設定されている IEC104 アプリケーションプロトコル情報制御（APIC）タイプと一致することを確認します。

`iec104_apci_type` 侵入ルールオプションは、完全な APIC タイプ名、あるいは大文字または小文字の APIC タイプの省略形を使用して指定された文字列を受け入れます。

型：文字列

シンタックス： `iec104_apci_type: <apic_type>;`

例：

```
iec104_apci_type: unnumbered_control_function;
iec104_apci_type: S;
iec104_apci_type: I;
iec104_apci_type: i;
```

iec104_asdu_func

IEC104 メッセージが、オプションで設定された IEC104 アプリケーション サービス データ ユニット（ASDU）機能コードと一致していることを確認します。

`iec104_asdu_func`侵入ルールオプションでは、大文字または小文字の ASDU 機能コードを使用して指定された文字列を使用できます。

型：文字列

シンタックス： `iec104_asdu_func: <asdu_func>;`

例：

```
iec104_asdu_func: M_SP_NA_1;
iec104_asdu_func: m_sp_na_1;
```

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。