GTP 検査インスペクタ

- GTP 検査インスペクタの概要 （1 ページ）
- GTP 検査インスペクタのパラメータ （1 ページ）
- GTP 検査インスペクタのルール （4 ページ）
- GTP 検査インスペクタの侵入ルールのオプション （4 ページ）

GTP 検査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	`false`

General Packet Radio Service（GPRS）Tunneling Protocol（GTP）により、GTP コア ネットワークを介した通信が実現します。

`gtp_inspect` インスペクタは、GTP トラフィックの異常を検出し、コマンド チャネル シグナリング メッセージを検査するためにルールエンジンに転送します。

GTP 検査インスペクタのパラメータ

GTP 検査サービスとポートの設定

`binder` インスペクタは GTP 検査のサービスと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": {
           "service": "gtp_inspect",
           "role": any
       },
       "use": {
           "type": "gtp_inspect"
       }
   },
   {
       "when": {
           "proto": "tcp",
           "role": "server",
           "ports": "2123 2152 3386"
       },
       "use": {
           "type": "gtp_inspect"
       }
   }
]
```

version

有効な GTP バージョンを指定します。

型：整数

有効な値：0、1、2

デフォルト値：2

messages[]

有効な GTP メッセージに関する情報の配列を指定します。

型：配列（オブジェクト）

例：

```
{
    messages: [
        {
            "type": 0,
            "name": ""
        }
    ]
}
```

messages[].type

有効な GTP メッセージタイプを指定します。「表 2 : GTP メッセージ タイプ」の表を参照してください。

型：整数

有効な範囲：0 ～ 255

デフォルト値：なし

messages[].name

有効な GTP メッセージ名を指定します。「表 2 : GTP メッセージ タイプ」の表を参照してください。

型：文字列

有効な値：有効な GTP メッセージ名

デフォルト値：なし

infos[]

GTP 情報要素の配列を指定します。

型：配列（オブジェクト）

例：

```
{
    infos: [
        {
            "type": 0,
            "name": "echo_request",
            "length": 0
        }
    ]
}
```

infos[].type

有効な GTP 要素タイプコードを指定します。「表 3 : GTP 情報要素」の表を参照してください。

型：整数

有効な範囲：0 〜 255

デフォルト値：0

infos[].name

有効な GTP 要素名を指定します。

型：文字列

有効な値：有効な GTP 情報要素の名前。「表 3 : GTP 情報要素」の表を参照してください。

infos[].length

有効な GTP 情報要素の長さを指定します。

型：整数

有効な範囲：0 〜 255

デフォルト値：0

GTP 検査インスペクタのルール

gtp_inspect 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: GTP* インスペクタのルール

GID:SID	ルール メッセージ
143:1	メッセージ長が無効（message length is invalid）
143:2	情報要素長が無効（information element length is invalid）
143:3	情報要素の順序が正しくない（information elements are out of order）
143:4	TEID がない（TEID is missing）

GTP 検査インスペクタの侵入ルールのオプション

gtp_inspect インスペクタの侵入ルールのオプションを使用すると、GTP コマンドチャネルの GTP バージョン、メッセージタイプ、および情報要素を検査できます。

GTP オプションは、content または byte_jump と組み合わせて使用することはできません。gtp_info または gtp_type を使用するルールそれぞれで gtp_version を使用する必要があります。

gtp_version

指定した GTP バージョンを GTP 制御メッセージのバージョンと照合します。

型：整数

シンタックス：`gtp_version: <version>;`

有効な値：0、1、2

例：`gtp_version: 1;`

gtp_type

それぞれの GTP メッセージは、数値と文字列で構成されるメッセージ タイプによって識別されます。指定した GTP タイプを GTP メッセージのタイプと照合します。

次の例に示すように、メッセージ タイプとして定義済みの 10 進数値、定義済み文字列、あるいはどちらか（または両方）を任意に組み合わたカンマ区切りリストを指定できます。

型：文字列

シンタックス：`gtp_type: <message_type>;`

有効な値：GTP メッセージタイプの表に示します。「表 2 : GTP メッセージ タイプ」の表を参照してください。

例：`gtp_type: "10, 11, echo_request";`

リスト内のそれぞれの値または文字列を照合するとき、システムは OR 演算を使用します。値と文字列を列挙する順序は重要ではありません。リスト内のいずれか 1 つの値または文字列の一致により、キーワードが一致します。認識されない文字列または範囲外の値を含むルールを保存しようとすると、エラーが生成されます。

GTP バージョンに応じて、同じメッセージタイプの値が異なる場合があります。たとえば `sgsn_context_request` メッセージタイプの値は GTPv0 と GTPv1 では `50` ですが、GTPv2 では `130` です。

パケット内のバージョン番号に応じて、`gtp_type` オプションは異なる値と一致します。たとえば、`sgsn_context_request` メッセージは GTPv0 パケットまたは GTPv1 パケットでは値 `50` と一致し、GTPv2 パケットでは値 `130` と一致します。パケット内のメッセージタイプの値が、パケットで指定されたバージョンの既知の値でない場合は、オプションはパケットと一致しません。

メッセージタイプに整数を指定した場合、パケット内に指定されたバージョンとは無関係に、メッセージタイプが GTP パケット内の値と一致すればオプションは一致します。

`gtp_message_type` は、表 2 : GTP メッセージ タイプ の表の数値またはキーワードです。

表 *2 : GTP* メッセージ タイプ

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
1	`echo_request`	`echo_request`	`echo_request`
2	`echo_response`	`echo_response`	`echo_response`
3	`version_not_supported`	`version_not_supported`	`version_not_supported`
4	`node_alive_request`	`node_alive_request`	該当なし
5	`node_alive_response`	`node_alive_response`	該当なし
6	`redirection_request`	`redirection_request`	該当なし
7	`redirection_response`	`redirection_response`	該当なし
16	`create_pdp_context_request`	`create_pdp_context_request`	該当なし
17	`create_pdp_context_response`	`create_pdp_context_response`	該当なし
18	`update_pdp_context_request`	`update_pdp_context_request`	該当なし
19	`update_pdp_context_response`	`update_pdp_context_response`	該当なし
20	`delete_pdp_context_request`	`delete_pdp_context_request`	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
21	delete_pdp_context_response	delete_pdp_context_response	該当なし
22	create_aa_pdp_context_request	init_pdp_context_activation_request	該当なし
23	create_aa_pdp_context_response	init_pdp_context_activation_response	該当なし
24	delete_aa_pdp_context_request	該当なし	該当なし
25	delete_aa_pdp_context_response	該当なし	該当なし
26	error_indication	error_indication	該当なし
27	pdu_notification_request	pdu_notification_request	該当なし
28	pdu_notification_response	pdu_notification_response	該当なし
29	pdu_notification_reject_request	pdu_notification_reject_request	該当なし
30	pdu_notification_reject_response	pdu_notification_reject_response	該当なし
31	該当なし	supported_ext_header_notification	該当なし
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	該当なし	該当なし	change_notification_request
39	該当なし	該当なし	change_notification_response
48	identification_request	identification_request	該当なし
49	identification_response	identification_response	該当なし
50	sgsn_context_request	sgsn_context_request	該当なし
51	sgsn_context_response	sgsn_context_response	該当なし
52	sgsn_context_ack	sgsn_context_ack	該当なし
53	該当なし	forward_relocation_request	該当なし
54	該当なし	forward_relocation_response	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
55	該当なし	forward_relocation_complete	該当なし
72	該当なし	relocation_cancel_request	該当なし
57	該当なし	relocation_cancel_response	該当なし
58	該当なし	forward_srns_contex	該当なし
59	該当なし	forward_relocation_complete_ack	該当なし
60	該当なし	forward_srns_contex_ack	該当なし
64	該当なし	該当なし	modify_bearer_command
65	該当なし	該当なし	modify_bearer_failure_indication
66	該当なし	該当なし	delete_bearer_command
67	該当なし	該当なし	delete_bearer_failure_indication
68	該当なし	該当なし	bearer_resource_command
69	該当なし	該当なし	bearer_resource_failure_indication
70	該当なし	ran_info_relay	downlink_failure_indication
71	該当なし	該当なし	trace_session_activation
72	該当なし	該当なし	trace_session_deactivation
73	該当なし	該当なし	stop_paging_indication
95	該当なし	該当なし	create_bearer_request
96	該当なし	mbms_notification_request	create_bearer_response
97	該当なし	mbms_notification_response	update_bearer_request
98	該当なし	mbms_notification_reject_request	update_bearer_response
99	該当なし	mbms_notification_reject_response	delete_bearer_request
100	該当なし	create_mbms_context_request	delete_bearer_response
101	該当なし	create_mbms_context_response	delete_pdn_request
102	該当なし	update_mbms_context_request	delete_pdn_response
103	該当なし	update_mbms_context_response	該当なし
104	該当なし	delete_mbms_context_request	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
105	該当なし	delete_mbms_context_response	該当なし
112	該当なし	mbms_register_request	該当なし
113	該当なし	mbms_register_response	該当なし
114	該当なし	mbms_deregister_request	該当なし
115	該当なし	mbms_deregister_response	該当なし
116	該当なし	mbms_session_start_request	該当なし
117	該当なし	mbms_session_start_response	該当なし
118	該当なし	mbms_session_stop_request	該当なし
119	該当なし	mbms_session_stop_response	該当なし
120	該当なし	mbms_session_update_request	該当なし
121	該当なし	mbms_session_update_response	該当なし
128	該当なし	ms_info_change_request	identification_request
129	該当なし	ms_info_change_response	identification_response
130	該当なし	該当なし	sgsn_context_request
131	該当なし	該当なし	sgsn_context_response
132	該当なし	該当なし	sgsn_context_ack
133	該当なし	該当なし	forward_relocation_request
134	該当なし	該当なし	forward_relocation_response
135	該当なし	該当なし	forward_relocation_complete
136	該当なし	該当なし	forward_relocation_complete_ack
137	該当なし	該当なし	forward_access
138	該当なし	該当なし	forward_access_ack
139	該当なし	該当なし	relocation_cancel_request
140	該当なし	該当なし	relocation_cancel_response
141	該当なし	該当なし	configuration_transfer_tunnel
149	該当なし	該当なし	detach

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
150	該当なし	該当なし	detach_ack
151	該当なし	該当なし	cs_paging
152	該当なし	該当なし	ran_info_relay
153	該当なし	該当なし	alert_mme
154	該当なし	該当なし	alert_mme_ack
155	該当なし	該当なし	ue_activity
156	該当なし	該当なし	ue_activity_ack
160	該当なし	該当なし	create_forward_tunnel_request
161	該当なし	該当なし	create_forward_tunnel_response
162	該当なし	該当なし	suspend
163	該当なし	該当なし	suspend_ack
164	該当なし	該当なし	resume
165	該当なし	該当なし	resume_ack
166	該当なし	該当なし	create_indirect_forward_tunnel_request
167	該当なし	該当なし	create_indirect_forward_tunnel_response
168	該当なし	該当なし	delete_indirect_forward_tunnel_request
169	該当なし	該当なし	delete_indirect_forward_tunnel_response
170	該当なし	該当なし	release_access_bearer_request
171	該当なし	該当なし	release_access_bearer_response
176	該当なし	該当なし	downlink_data
177	該当なし	該当なし	downlink_data_ack
179	該当なし	該当なし	pgw_restart
180	該当なし	該当なし	pgw_restart_ack
200	該当なし	該当なし	update_pdn_request
201	該当なし	該当なし	update_pdn_response
211	該当なし	該当なし	modify_access_bearer_request

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
212	該当なし	該当なし	modify_access_bearer_response
231	該当なし	該当なし	mbms_session_start_request
232	該当なし	該当なし	mbms_session_start_response
233	該当なし	該当なし	mbms_session_update_request
234	該当なし	該当なし	mbms_session_update_response
235	該当なし	該当なし	mbms_session_stop_request
236	該当なし	該当なし	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	該当なし
241	data_record_transfer_response	data_record_transfer_response	該当なし
254	該当なし	end_marker	該当なし
255	pdu	pdu	該当なし

gtp_info

1 つの GTP メッセージには多数の情報要素が含まれることがあり、それぞれの要素は定義済み数値および定義済み文字列によって識別されます。gtp_info オプションを使用すると、指定した情報要素の先頭から検査を開始し、その情報要素に検査を限定することができます。

情報要素に対して定義された 10 進数値と定義された文字列のどちらでも指定できます。単一の値または文字列を指定することも、1 つのルール内で複数の gtp_info オプションを使って複数の情報要素を検査することもできます。

1 つのメッセージに同じタイプの複数の情報要素が含まれている場合は、すべてが照合対象として検査されます。情報要素が無効な順序で出現する場合は、最後のインスタンスだけが検査されます。

バージョンに応じて、GTP メッセージは同じ情報要素に対して異なる値を使用できます。たとえば cause 情報要素の値は GTPv0 と GTPv1 では 1 ですが、GTPv2 では 2 です。

パケット内のバージョン番号に応じて、gtp_info オプションは異なる値と一致します。上記の例の場合、GTPv0 または GTPv1 パケットではキーワードが情報要素値 1 と一致しますが、GTPv2 パケットでは値 2 と一致します。パケット内の情報要素値が、パケットで指定されたバージョンの既知の値でない場合は、オプションがパケットと一致しません。

情報要素に整数を指定した場合、パケット内に指定されたバージョンとは無関係に、メッセージタイプが GTP パケット内の値と一致すればオプションが一致します。

型：文字列

シンタックス：gtp_info: <identifier>;

有効な値：表 3 : GTP 情報要素の表に示します。

例： `gtp_info: "qos";`

表 *3 : GTP* 情報要素

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	該当なし
5	p_tmsi	p_tmsi	該当なし
6	qos	該当なし	該当なし
8	recording_required	recording_required	該当なし
9	authentication	authentication	該当なし
10	該当なし	該当なし	該当なし
11	map_cause	map_cause	該当なし
12	p_tmsi_sig	p_tmsi_sig	該当なし
13	ms_validated	ms_validated	該当なし
14	recovery	recovery	該当なし
15	selection_mode	selection_mode	該当なし
16	flow_label_data_1	teid_1	該当なし
17	flow_label_signalling	teid_control	該当なし
18	flow_label_data_2	teid_2	該当なし
19	ms_unreachable	teardown_ind	該当なし
20	該当なし	nsapi	該当なし
21	該当なし	ranap	該当なし
22	該当なし	rab_context	該当なし
23	該当なし	radio_priority_sms	該当なし
24	該当なし	radio_priority	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
25	該当なし	packet_flow_id	該当なし
26	該当なし	charging_char	該当なし
27	該当なし	trace_ref	該当なし
28	該当なし	trace_type	該当なし
29	該当なし	ms_unreachable	該当なし
71	該当なし	該当なし	apn
72	該当なし	該当なし	ambr
73	該当なし	該当なし	ebi
74	該当なし	該当なし	ip_addr
75	該当なし	該当なし	mei
76	該当なし	該当なし	msisdn
77	該当なし	該当なし	indication
78	該当なし	該当なし	pco
79	該当なし	該当なし	paa
80	該当なし	該当なし	bearer_qos
80	該当なし	該当なし	flow_qos
82	該当なし	該当なし	rat_type
83	該当なし	該当なし	serving_network
84	該当なし	該当なし	bearer_tft
85	該当なし	該当なし	tad
86	該当なし	該当なし	uli
87	該当なし	該当なし	f_teid
88	該当なし	該当なし	tmsi
89	該当なし	該当なし	cn_id
90	該当なし	該当なし	s103pdf
91	該当なし	該当なし	s1udf

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
92	該当なし	該当なし	delay_value
93	該当なし	該当なし	bearer_context
94	該当なし	該当なし	charging_id
95	該当なし	該当なし	charging_char
96	該当なし	該当なし	trace_info
97	該当なし	該当なし	bearer_flag
99	該当なし	該当なし	pdn_type
100	該当なし	該当なし	pti
101	該当なし	該当なし	drx_parameter
103	該当なし	該当なし	gsm_key_tri
104	該当なし	該当なし	umts_key_cipher_quin
105	該当なし	該当なし	gsm_key_cipher_quin
106	該当なし	該当なし	umts_key_quin
107	該当なし	該当なし	eps_quad
108	該当なし	該当なし	umts_key_quad_quin
109	該当なし	該当なし	pdn_connection
110	該当なし	該当なし	pdn_number
111	該当なし	該当なし	p_tmsi
112	該当なし	該当なし	p_tmsi_sig
113	該当なし	該当なし	hop_counter
114	該当なし	該当なし	ue_time_zone
115	該当なし	該当なし	trace_ref
116	該当なし	該当なし	complete_request_msg
117	該当なし	該当なし	guti
118	該当なし	該当なし	f_container
119	該当なし	該当なし	f_cause

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
120	該当なし	該当なし	plmn_id
121	該当なし	該当なし	target_id
123	該当なし	該当なし	packet_flow_id
124	該当なし	該当なし	rab_contex
125	該当なし	該当なし	src_rnc_pdcp
126	該当なし	該当なし	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	該当なし
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	該当なし	qos	node_type
136	該当なし	authentication_qu	fqdn
137	該当なし	tft	ti
138	該当なし	target_id	mbms_session_duration
139	該当なし	utran_trans	mbms_service_area
140	該当なし	rab_setup	mbms_session_id
141	該当なし	ext_header	mbms_flow_id
142	該当なし	trigger_id	mbms_ip_multicast
143	該当なし	omc_id	mbms_distribution_ack
144	該当なし	ran_trans	rfsp_index
145	該当なし	pdp_context_pri	uci
146	該当なし	addi_rab_setup	csg_info

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
147	該当なし	sgsn_number	csg_id
148	該当なし	common_flag	cmi
149	該当なし	apn_restriction	service_indicator
150	該当なし	radio_priority_lcs	detach_type
151	該当なし	rat_type	ldn
152	該当なし	user_loc_info	node_feature
153	該当なし	ms_time_zone	mbms_time_to_transfer
154	該当なし	imei_sv	throttling
155	該当なし	camel	arp
156	該当なし	mbms_ue_context	epc_timer
157	該当なし	tmp_mobile_group_id	signalling_priority_indication
158	該当なし	rim_routing_addr	tmgi
159	該当なし	mbms_config	mm_srvcc
160	該当なし	mbms_service_area	flags_srvcc
161	該当なし	src_rnc_pdcp	nmbr
162	該当なし	addi_trace_info	該当なし
163	該当なし	hop_counter	該当なし
164	該当なし	plmn_id	該当なし
165	該当なし	mbms_session_id	該当なし
166	該当なし	mbms_2g3g_indicator	該当なし
167	該当なし	enhanced_nsapi	該当なし
168	該当なし	mbms_session_duration	該当なし
169	該当なし	addi_mbms_trace_info	該当なし
170	該当なし	mbms_session_repetition_num	該当なし
171	該当なし	mbms_time_to_data	該当なし
173	該当なし	bss	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
174	該当なし	cell_id	該当なし
175	該当なし	pdu_num	該当なし
177	該当なし	mbms_bearer_capab	該当なし
178	該当なし	rim_routing_disc	該当なし
179	該当なし	list_pfc	該当なし
180	該当なし	ps_xid	該当なし
181	該当なし	ms_info_change_report	該当なし
182	該当なし	direct_tunnel_flags	該当なし
183	該当なし	correlation_id	該当なし
184	該当なし	bearer_control_mode	該当なし
185	該当なし	mbms_flow_id	該当なし
186	該当なし	mbms_ip_multicast	該当なし
187	該当なし	mbms_distribution_ack	該当なし
188	該当なし	reliable_inter_rat_handover	該当なし
189	該当なし	rfsp_index	該当なし
190	該当なし	fqdn	該当なし
191	該当なし	evolved_allocation1	該当なし
192	該当なし	evolved_allocation2	該当なし
193	該当なし	extended_flags	該当なし
194	該当なし	uci	該当なし
195	該当なし	csg_info	該当なし
196	該当なし	csg_id	該当なし
197	該当なし	cmi	該当なし
198	該当なし	apn_ambr	該当なし
199	該当なし	ue_network	該当なし
200	該当なし	ue_ambr	該当なし

タイプ	バージョン 0 の名前	バージョン 1 の名前	バージョン 2 の名前
201	該当なし	apn_ambr_nsapi	該当なし
202	該当なし	ggsn_backoff_timer	該当なし
203	該当なし	signalling_priority_indication	該当なし
204	該当なし	signalling_priority_indication_nsapi	該当なし
205	該当なし	high_bitrate	該当なし
206	該当なし	max_mbr	該当なし
251	charging_gateway_addr	charging_gateway_addr	該当なし
255	private_extension	private_extension	private_extension

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。