

技術ノート KGTN 2017090601

現象

[GGH5.1] HTML5 クライアントの通信のプロトコルは？

説明

HTML5 クライアントの通信プロトコルは **RXP over HTTP** で、より正確に言えば、**RXP over WebSocket protocol (ws://)** です。暗号化は、この **RXP** プロトコル上で **56-bit DES** または **SSL** で行われます。詳細については、下記説明をご覧ください。

The default protocol for the HTML5 client is RXP over HTTP. This is true, but it's a bit more accurate to say it's RXP over WebSocket protocol (ws://). By default, GO-Global hosts are configured to use the TCP Transport with 56-bit DES encryption. In this default configuration, the WebSocket packets transmitted between HTML5 clients and the host are not encrypted, but the RXP payloads of the WebSocket packets are encrypted using 56-bit DES encryption.

When an HTML5 client connects to a GO-Global host that is configured to use SSL, the HTML5 client must be configured to use the Secure WebSocket protocol. This can be done by specifying the WebSocket URL in the client's URL with the Secure WebSocket protocol as follows:

```
http[s]://[host_address]/goglobal/?WebSocketURL=wss://[host_address]:491/
```

When the Secure WebSocket (wss://) protocol is specified, the client then opens a Secure WebSocket connection to the specified port on the GO-Global host. In this case both the WebSocket packets and the RXP payloads are encrypted using OpenSSL and the cipher that is selected in the Cluster Manager.