

# Link Key取得について

## Bluetoothログ解析方法

Bluetooth機器の通信は暗号化されており、解析時には暗号化を解く“Link Key”が必要となります。Sodera又はBPA600を使用したログ解析方法は以下の2通りです。

1. 測定機器のどちらかをSSP Debug Modeに設定する
2. Android端末の「btsnoop\_hci.log」ファイルから Link Key を取得する

---

## 【方法 1】 測定機器をSSP Debug Modeに設定する

Bluetooth機器は **SSP Debug Mode** と呼ばれる開発モードに設定可能です。  
Master/Slave機器のいずれかをSSPデバッグモードに設定すると、Link Key  
を入力せずに 暗号化以降の解析が可能になります。

### SSP Debug Mode とは

- ① Link Keyは通常、コネクション毎に毎回異なるKeyが生成されますが、Bluetooth機器を SSP Debug Mode に設定することにより、Link Key 構成要素の一部が固定になります。  
そのため、CPASソフトウェアは Link Keyを自動認識 (計算)することが可能になります。
- ② SSP Debug Modeへの切替方法は各セットメーカーにより異なり、  
また対応していないBluetooth機器もあるため、必ず各セットメーカーへ  
ご確認ください。

# 【方法1】 SSP Debug Modeに設定した場合の表示例

Master/SlaveのいずれかがSSP Debug Modeになっていると、Link keyを入力しなくても暗号化以降のタブが表示されます。

The image shows a Wireshark capture of Bluetooth LMP packets. The top pane shows a list of packets with columns for Frame#, LT\_Addr, Original Opcode, Opcode, Role, and Initiated by. A packet with opcode 'encapsulated\_payload' is highlighted, and its details pane is expanded. In the details pane, the 'Debug Key[X]' field is highlighted with a red box, showing the hexadecimal value 0x15207009984421a6586f9fc3fe7e4329d28. The bottom pane shows the raw data in binary, hexadecimal, and ASCII formats.

Frame#	LT_Addr	Original Opcode	Opcode	Role	Initiated by	Fram...
393	3	encapsulated_header	accepted	Slave	master	11
396	3	encapsulated_payload	encapsulated_payload	Master	master	26
407	3	encapsulated_payload	accepted	Slave	master	11
410	3	encapsulated_payload	encapsulated_payload	Master	master	26
415	3	encapsulated_payload	accepted	Slave	master	11
* 3			encapsulated_payload	* Master	* master	26
			encapsulated_payload	Slave	master	11
			preferred_rate	Slave	slave	11
	3		encapsulated_header	Slave	master	13

18: (Master) Len=26  
that the data were reconstructed.  
id:  
Role: Master  
\* Address: 3  
\* Opcode: LMP\_encapsulated\_payload  
\* Transaction ID: Initiated by master  
\* P-192 Public Key  
Debug Key[X]: 0x15207009984421a6586f9fc3fe7e4329d28  
\* Debug Key[Y]: 0x129142424151429872014594440057

Link key (Debug Key) は "encapsulated payload" パケット内で確認できます。

---

## 【方法2】 Android端末から Link Keyを抜き出す

Android端末との通信を解析する場合、Android端末内に記録される「btsnoop\_hci.log」ファイルから、Link Keyを抜き出すことが可能です。

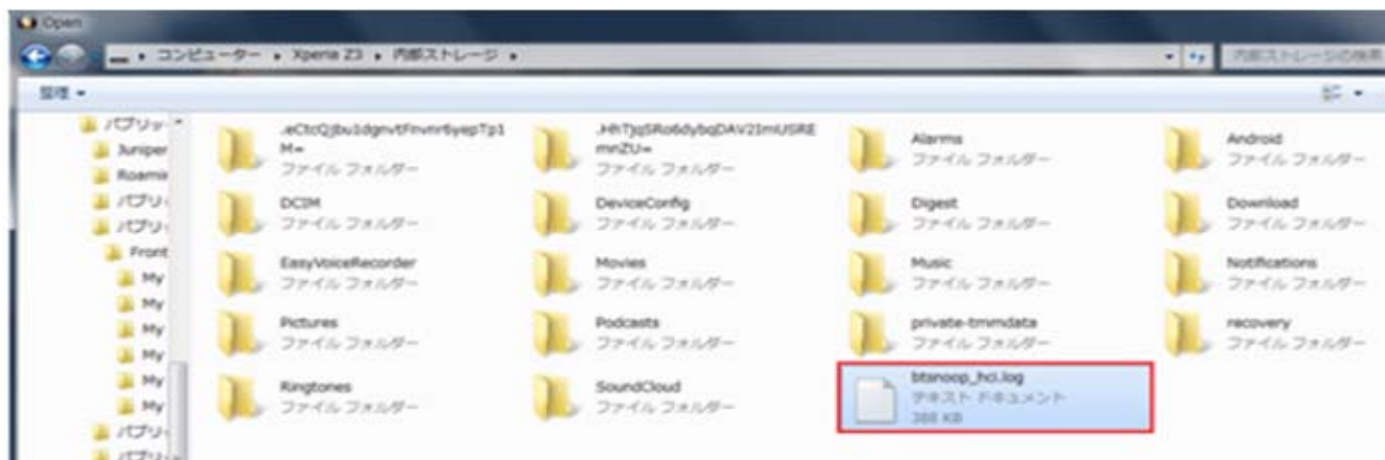
抜き出したLink KeyをCPASソフトウェアに入力することで暗号化以降のプロトコル解析も可能になります。

※本手法はAndroid端末(OS ver 4.4以降)のみ有効であり、**iPhone端末は非対応**です。

# btsnoop\_hci.log 取得方法 (1)

## <ログ取得前の確認事項>

- ① CPASソフトウェアが最新バージョンであることを確認する
- ① Android端末のペアリング履歴・デバイス情報を完全削除する
- ① 一度端末をPCに接続し、古い「btsnoop\_hci.log」が残っていないかを確認する  
⇒残っている場合は、削除する



## btsnoop\_hci.log 取得方法 (2)

- ① 端末の「設定」画面を開く  
→最下層の「端末情報」  
→「ビルド番号」を7回タップ



- ② ①で開発者モードになり  
「設定」画面に開発者向けオプションが  
表示される

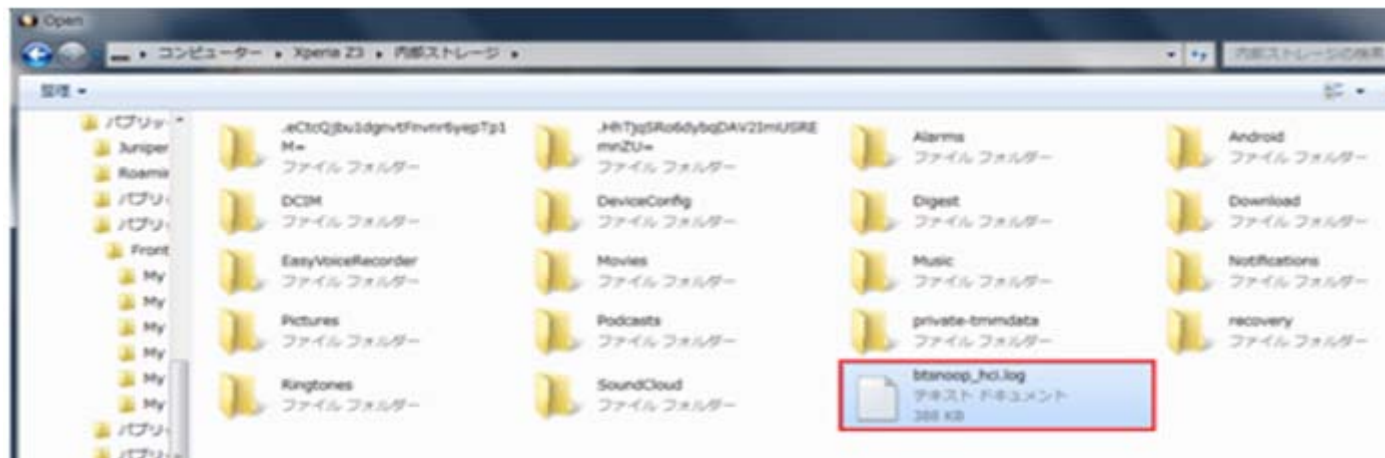


- ③ 開発者向けオプションをONに変更し、  
Bluetooth HCIスヌープログを  
「有効にする」をチェック



## btsnoop\_hci.log 取得方法 (3)

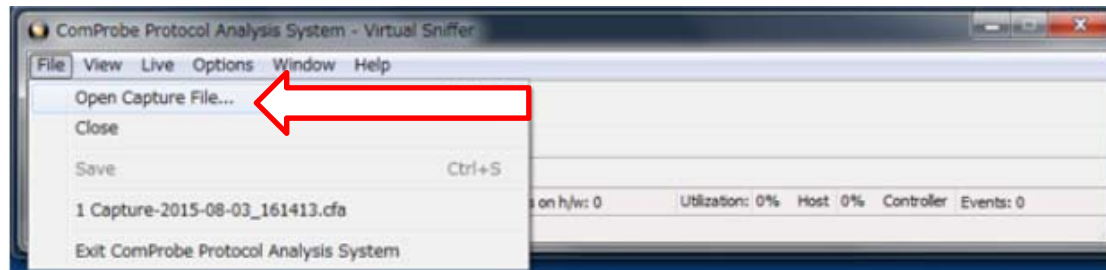
- ④ 端末とペアリングを行う
- ⑤ 端末を再起動
- ⑥ 再度端末をPCに接続し、「btsnoop\_hci.log」をPCに保存



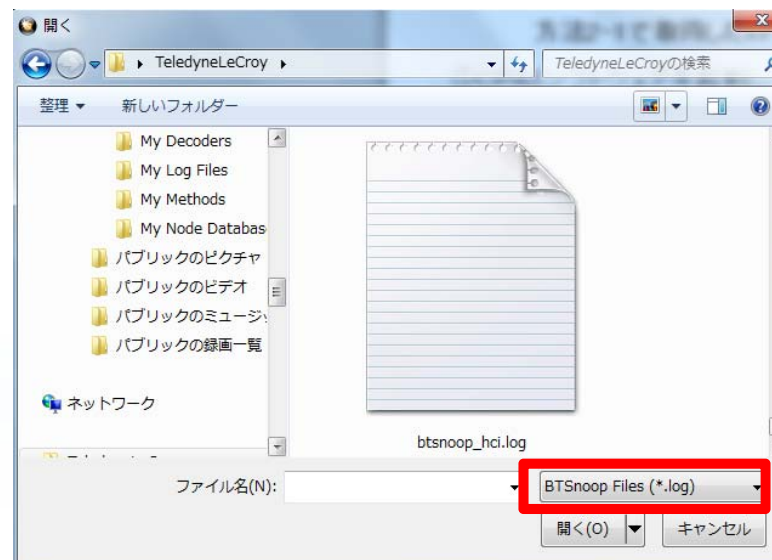


# 取得した btsnoop\_hci.log から Link Keyを確認

- ① CPASソフトウェアを起動し、「Open Capture File...」を選択



- ② 拡張子を「BT Snoop Files.log」に変更し、PCに保存した「btsnoop\_hci.log」ファイルを開く



# 抜き出したLink Keyの表示例 (1)

## \* 成功例 \*

“Link key”を検索すると、以下の通り表示されます。

The screenshot shows the Wireshark interface with the following details:

- Frame 942: (Controller) Len=26
- HCI UART: HCI Packet Type: Event Packet
- HCI: Packet from: Controller
- HCI Event: Event: Link Key Notification
- Total Length: 23
- Bluetooth Device Address: 0x8c-de-52-24-3d-8b
- LAP: 0x24-3d-8b
- UAP: 0x52
- NAP: 0x8c-de
- Link Key: 0xd3 7e 8b 5b 60 8f be 34 fe 61 be f7 dc 23 84 43
- Link Key Types: Unauthenticated Combination Key

The search bar at the top right contains the text "link key".

B...	Frame#	HCI Packet Type	Fram...	Delta	Timestamp
	942	Event	26	00:00:00.3...	2017/05/18 7:55:45.401328
	943	Event	6	00:00:00.0...	2017/05/18 7:55:45.403720
	944	ACL Data	17	00:00:00.0...	2017/05/18 7:55:45.442433
	945	ACL Data	21	00:00:00.0...	2017/05/18 7:55:45.538386
	946	ACL Data	21	00:00:00.0...	2017/05/18 7:55:45.540721
	947	ACL Data	21	00:00:00.0...	2017/05/18 7:55:45.605164
	948	Event	8	00:00:00.0...	2017/05/18 7:55:45.605945
	949	ACL Data	19	00:00:00.0...	2017/05/18 7:55:45.607329
	950	ACL Data	19	00:00:00.0...	2017/05/18 7:55:45.607784
	951	ACL Data	29	00:00:00.0...	2017/05/18 7:55:45.609120
	952	Event	8	00:00:00.0...	2017/05/18 7:55:45.674843
	953	ACL Data	22	00:00:00.0...	2017/05/18 7:55:45.742211
	954	ACL Data	119	00:00:00.3...	2017/05/18 7:55:46.078505
	955	ACL Data	17	00:00:00.0...	2017/05/18 7:55:46.080891

※検証機器：Android OS 6.0.1のXperiaとスマートスピーカーとの接続

## 抜き出したLink Keyの表示例 (2)

### \* 失敗例 \*

エラー表示となり、Link Keyが表示されない

The screenshot shows a software interface for displaying Bluetooth HCI log data. The left pane shows a tree view of the log data for Frame 933. Under 'HCI Event', there is an 'Event: Link Key Request' with a 'Total Length: 6'. Below it, a red box highlights the error message: 'Bluetooth Device Address: Field Truncated or Not Present'. The right pane shows a table of HCI packets. A search bar at the top right contains the text 'link key'. The table has columns for 'B...', 'Frame#', 'HCI Packet Type', 'Fram...', 'Delta', and 'Timestamp'. The following table represents the data shown in the screenshot:

B...	Frame#	HCI Packet Type	Fram...	Delta	Timestamp
	913	Event	7	00:00:00.0...	2018/01/05 5:10:25.735459
	914	Command	8	00:00:00.0...	2018/01/05 5:10:25.735706
	915	Event	9	00:00:00.0...	2018/01/05 5:10:25.736239
	916	Command	8	00:00:00.0...	2018/01/05 5:10:25.736527
	917	Event	9	00:00:00.0...	2018/01/05 5:10:25.737061
	918	Event	6	00:00:00.0...	2018/01/05 5:10:25.737293
	919	ACL Data	21	00:00:00.0...	2018/01/05 5:10:25.738366
	920	Event	8	00:00:00.0...	2018/01/05 5:10:25.744679

※以下の場合はセットメーカー様へお問合せ下さい。

- 複数回試してもエラー表示が続いた場合
- 「btsnoop\_hci.log」ファイル自体が取得できない場合

---

ご不明点などございましたら、お気軽にご連絡ください

お問い合わせ先

〒105-0014  
東京都港区芝3丁目5番1号コーンズハウス  
コーンズテクノロジー株式会社  
電子通信ソリューション営業部  
TEL : 03-5427-7566  
Email : [ctl-comm@cornes.jp](mailto:ctl-comm@cornes.jp)