

LoRaWAN™ 端末番号の設定

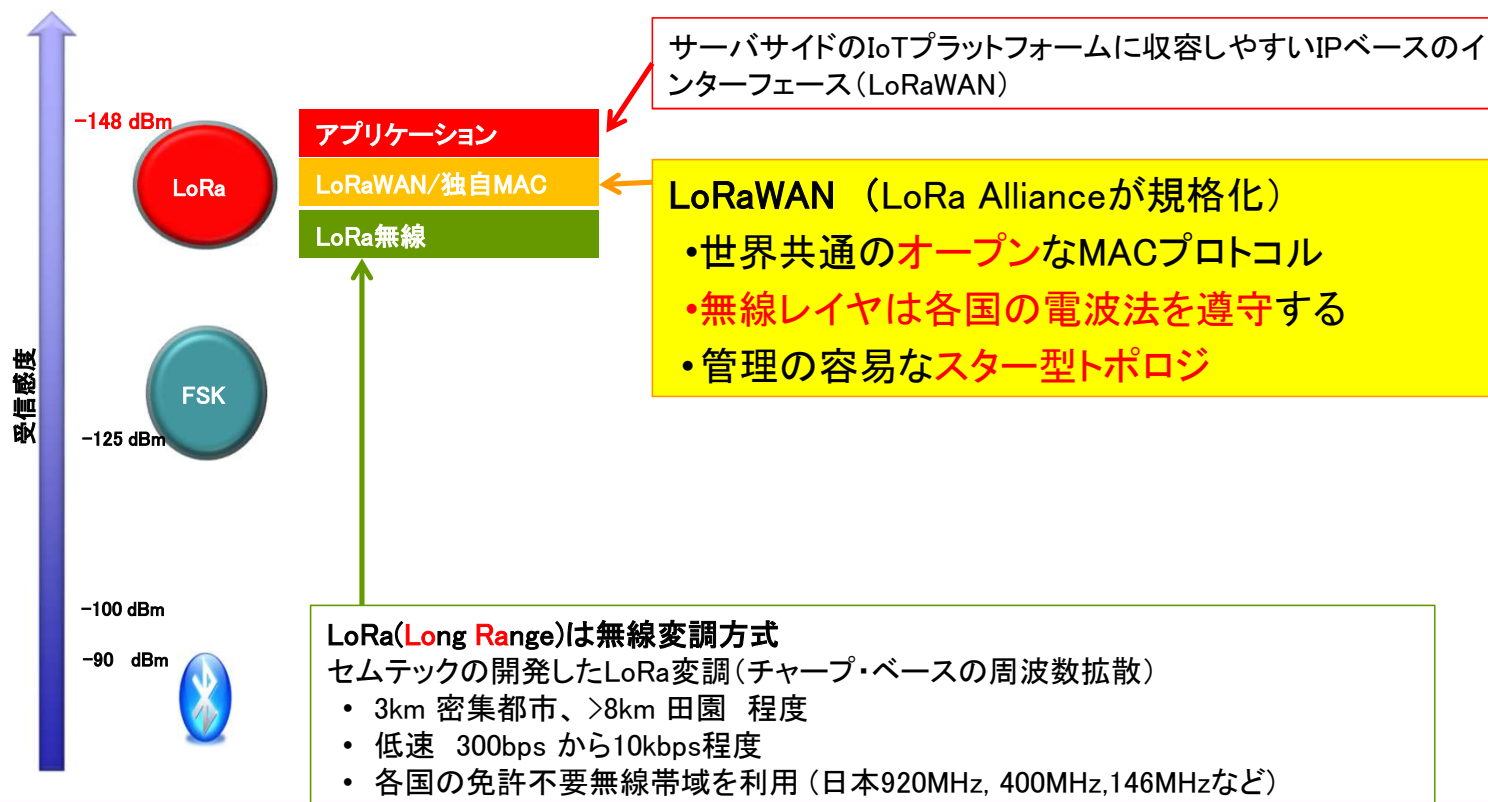
セムテック・ジャパン合同会社

LoRa 担当 技術課長 齋藤 城太郎

2019 Jan 28

LoRa® (変調方式)と LoRaWAN™

- LoRa=長距離無線変調方式(上り下り双方向)と無線IC
- LoRaWAN=スター型MACプロトコルと双方向無線システム



LPWAの比較



LoRaWAN:

* 免許不要の周波数帯

* 使用者が独自に運用する自営網 (Private)、電気通信事業者が運用する公衆網 (Public) どちらも可能

	LoRaWAN	Sigfox	NB-IoT	LTE-M	SONY LPWA
形式	非免許	非免許	免許	免許	非免許
ネットワーク	公衆、自営	公衆	公衆	公衆	公衆
転送速度	~11kbps (LoRa) 50kbps (FSK)	100bps (UL) 600bps (DL)	~62.5kbps	~300kbps	~80bps
接続形態	スター型	スター型	1:1	1:1	スター型
帯域	7.8kHz ~500kHz	100Hz (UL) 800Hz (DL)	200 kHz	~ 1.4MHz	200kHz
変調	CSS	BPSK UL GFSK DL	QPSK, BPSK	PSK, QPSK, 16QAM	Chirp BPSK
RF 出力	~13dBm ~24dBm	~13dBm UL ~24dBm DL	~ 23dBm	~23dBm	~13dBm

LoRa Alliance™ には世界で300社以上が参加

□ Sponsor (W/W):

- Actility
- Alibaba Group
- CISCO
- ER-Telecom
- Google Cloud
- Hangzhou Lowan Information Technology Co
- IBM
- JD Cloud
- Kerlink
- Kpn
- Machine Q
- Bouygues
- Orange
- Proximus
- Sagemcom
- SEMTECH
- Shenzhen Tencent Computer Systems Company Limited
- SK telecom
- STMicroelectronics
- ZTE CORPORATION

□ Contributor (Japan):

- Renesas
- M2B
- Murata
- NEC
- Nextfield
- NTT
- Senseway
- Softbank

□ Adopter (Japan):

- ACCESS
- Automagi
- Braveridge
- EASEL
- Green House
- Macnica
- Oki
- Oi Electric
- Seiryō
- TDK
- SMK
- Yokogawa

オープンな規格 IoTエコシステムの中で得意な分野に参入可能



□ Chipset:

- SEMTECH
- Microchip
- STmicro 等

□ Module:

- muRata
- EASEL
- Green House
- Braveridge
- Microchip 等

□ Device:

- ABIT
- Braveridge
- EASEL
- Green House
- GEMTEK
- Oki
- Oi Electric
- Yokogawa 等

□ Base Station:

- Oi Electric
- CISCO
- Kerlink
- GEMTEK 等

□ Network Server:

- Actility
- NEC 等

□ Network Operator:

- NTT
- SENSEWAY
- SOFTBANK
- M2B 等

LoRaWANの特徴

□ LoRaWANは、LoRa Alliance™が技術仕様を作成し公開している MACレイヤのオープンな規格

- 仕様はLoRa Allianceホームページから、非会員でもダウンロード可能
- <https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers>

□ LoRaWAN特長

- 双方向、アクリッジ・ベースの通信
- 単純なスター型トポロジ、長距離飛ぶのでリピータ、メッシュ・ルーチングは不要
- 残念ながら低速
- 低コスト
- 長距離
- 低消費電力のため、電池駆動型ノードに最適
- 物理層は、LoRaもしくはFSKを利用し、各国の電波法に準拠
- 各国別の仕様。日本はAS923

□ 3つの通信クラス

- Class A LoRaの基本通信。センサーからデータを送信
- Class B ビーコンモード
- Class C レイテンシなし

エンドデバイスのアクティベーション方法



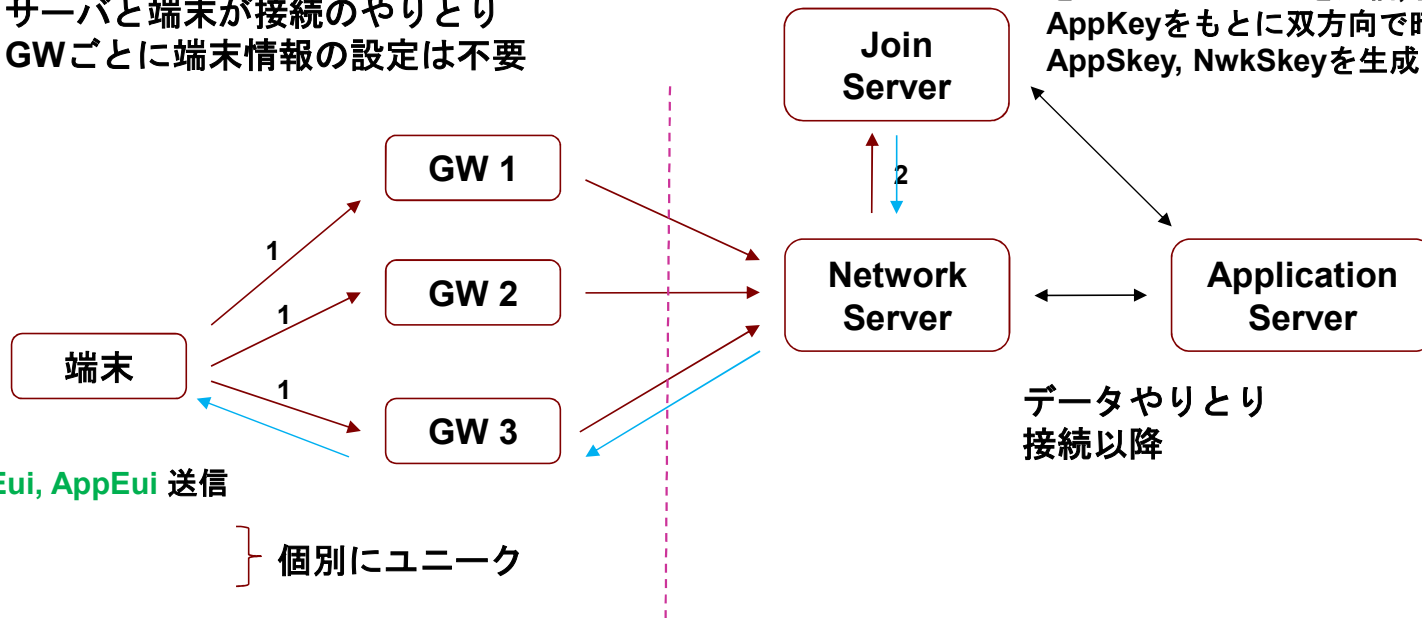
□ 2つのアクティベーション方法が用意

- OTAA (Over The Air Activation) エンドデバイスがネットワークに最初に接続したときに接続要求を行う。エンドデバイスはグローバルなデバイス識別子DevEUIをサーバに送り、DevAddrの払い出しを受ける。DevAddrは使いまわし可能
- ABP (Activation By Personalization): DevAddrなどを工場出荷時にエンドデバイスに設定する。DevAddrは端末固有値

ネットワークとの接続 (OTAA)

- ✓ 各無線ネットワークは、LoRaAllianceから割り当てられる24bitのNetIDを持つ。
- ✓ LoRaネットワーク上で端末を一意に識別するIDとしてDevAddrが使用される。
- ✓ DevAddrは、初回接続時に、端末のDevEUI、AppEUI及びAppKeyをサーバに対して送信し、サーバから受取る

サーバと端末が接続のやりとり
GWごとに端末情報の設定は不要



OTAA : 接続時 DevEui, AppEui 送信

- DevEui (8B)
- AppEui (8B)
- AppKey (AES128)

} 個別にユニーク

DevEUI, AppEUIはIEEEより入手

用語

□ DevEUI

- IEEE が発行したEUI-64。グローバルにユニーク。端末メーカーが設定

□ AppEUI (=>JoinEUI @R1.1)

- EUI-64。Join ServerのID。Join Serverもしくはオペレータがアサイン。端末はネットワーク接続時に指定

□ Device Address (DevAddr)

- 32ビット識別子、デバイスをネットワーク内で識別
- 初回接続時(OTAA)にJoin Serverより振出し。その後、各データフレームに付随し通信
- エンドデバイス、ネットワークサーバ、アプリケーションサーバ間で共有

□ AppKey

- AppKeyは、エンドデバイスに固有のAES-128ルートキー。NwkSKey, AppSKeyを引き出すために使用

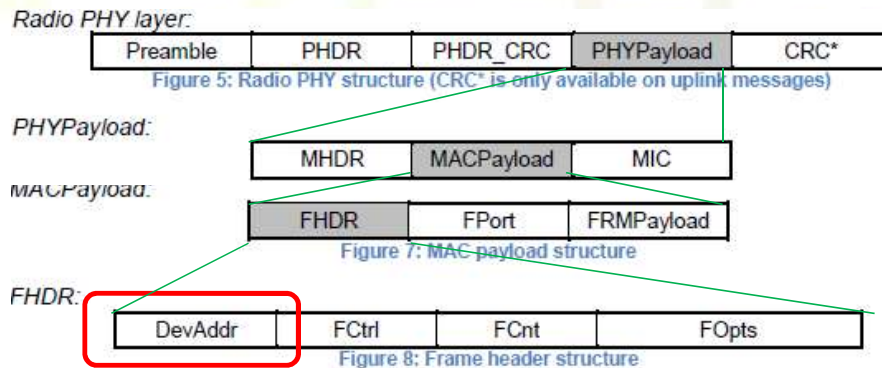
□ Network Session Key (NwkSKey)

- 128bit AES暗号鍵
- エンドデバイスとネットワークサーバ間で共有
- メッセージの保全とエンドデバイスとネットワークサーバ間のセキュリティ

□ Application Session Key (AppSKey)

- 128bit AES暗号鍵
- エンドデバイスとアプリケーションサーバ間で共有
- アプリケーションデータ、メッセージの暗号化復号化に使われる
- アプリケーションペイロードのセキュリティ

送信パケット例 DevAddr はFHDRの中で暗号化されずに送信



Mode	PHYPayload																			
	MHDR	MACPayload (or Join-Request/Response)							FRMPayload (Encryption)				MIC (Message Integrity Code)							
	40	DevAddr				FCtrl	FCnt (Frame counter)		FOpts	Fport										
	1 Byte	4 Bytes				1 Byte	2 Bytes		1 Byte											4 Bytes
Rx	40	00	00	00	11	00	71	00	02	9	FB	AB	64	F1	A1	72	AB	D3		
Rx	40	00	00	00	11	00	72	00	02	68	15	E7	9D	37	F7	8	A3	O6		
Rx	40	00	00	00	11	00	75	00	02	1	0A	BB	D9	48	8B	6E	28	D1		
Rx	40	00	00	00	11	00	76	00	02	58	59	3F	83	E3	1E	3E	16	D6		
						00	77	00		C0	3D	3F	94	O6	F6	FA	38	6		
						00	78	00		1E	77	BB	A7	24	1D	A0	AC	2B		
						00	79	00		88	9E	78	AE	35	46	CE	EF	47		
						00	7B	00		83	70	0A	43	30	E4	EB	4D	9C		
						00	7C	00	02	B6	AC	76	AE	43	26	AA	E2	FF		
						00	7D	00	02	8A	89	98	80	33	60	47	64	D0		

00:Join Request
 10: Join Accept
 20: Unconfirmed UL
 30: Unconfirmed DL
 40: Confirmed UL
 50: Confirmed DL
 60: Rejoin Request
 7x: Proprietary

Bit# 7: ADR, 6: ADRACKReq,
 5:ACK, 4: RFU, 3-0:
 FoptLen, If FoptLen ="0",
 the Fopts field is absent

(MAC command up to 15 Byte)

If 0, PL contains
 MAC commands
 only, Others
 depend on apps

LoRa Alliance メンバーグレードでのDevAddrの割当数

- ✓ Dev Addrは、プレフィックス (1~7bit) + Net ID (6~15bit) + Net Addr (10~25bit) の合計32bitで構成
- ✓ メンバーのクラス (スポンサー、コントリビューター、アダプター) に応じて、Dev Addrの番号容量が異なる。

【Dev Addrの構造・割当】

Assigned to:		24bit NetID			32bit DevAddr			番号容量
Type	Type (3 bits)	RFU	ID	Type prefix binary value	Number of NwkID bits	Number of NwkAddr bits		
Sponsor members	0	000	0000000000000000 (15 bits)	xxxxxx (6 bits) ▶	0 (1 bit)	6	25	約3,300万端末分
Contributor members	3	011	<none>	xxxxxxxxxxxxxxxxxxxx (21 bits) ▶	1110 (4 bits)	10	18	約26万端末分
Adopter/Institutional	6	110	<none>	xxxxxxxxxxxxxxxxxx (21 bits) ▶	1111110 (7 bits)	15	10	約1000端末分