Openloop

Openloop ハードウェアウォレット
製品仕様書

バージョン v0.91.0 ｜ 最終更新 2026-04-02

株式会社ハウディ・クリプト　代表取締役社長　浅田 一憲

1. 製品概要

1.1 製品名

Openloop (オープンループ) - マルチチェーン対応ハードウェアウォレット

1.2 製品コンセプト

初心者でも使いやすく、高度なセキュリティを備えた商用レベルのハードウェアウォレット。既存の主要ウォレットアプリ（Sparrow　　Wallet、MetaMask等）との互換性を持ち、複数の通信方式（QRコード、USB、BLE）をサポートする。さらにFIDO2/CTAP2パスキー（セキュリティキー）機能を搭載し、暗号資産管理とWeb認証の両方を1台で実現する。

1.3 ターゲット市場

- **個人ユーザー**: 暗号資産の安全な保管を求める初心者〜中級者
- **企業ユーザー**: 社内資産管理やマルチシグ運用
- **販売チャネル**: Amazon等のECサイト

2. サポート資産

2.1 対応暗号通貨

資産タイプ	通貨/トークン	チェーン	実装状況
ネイティブ通貨	**Bitcoin (BTC)**	Bitcoin	✓ 実装済
ネイティブ通貨	**Ethereum (ETH)**	EVM互換チェーン	✓ 実装済

資産タイプ	通貨/トークン	チェーン	実装状況
ネイティブ通貨	**XRP**	XRP Ledger	✓ 実装済
ネイティブ通貨	**Solana (SOL)**	Solana	✓ 実装済
ネイティブ通貨	**TRON (TRX)**	TRON	✓ 実装済
トークン	**ERC-20トークン**	Ethereum/L2	✓ 実装済

2.2 対応Bitcoinスクリプトタイプ

スクリプトタイプ	説明	アドレス形式	対応状況
P2WPKH	Native SegWit (Bech32)	bc1q…	✓ 対応
P2PKH	Legacy	1…	✓ 対応
P2SH	Script Hash	3…	✓ 対応
P2SH-P2WPKH	Nested SegWit	3…	✓ 対応
P2WSH	Witness Script Hash (マルチシグ)	bc1q…	✓ 対応
P2TR	Taproot	bc1p…	▲ アドレス表示のみ

Bitcoin標準規格準拠:

- ✓ BIP39 - ニーモニック生成・復元 (12/24語)
- ✓ BIP32 - HD鍵導出
- ✓ BIP44 - マルチアカウント階層構造
- ✓ BIP84 - Native SegWit導出パス (m/84'/0'/0'/0/x)
- ✓ BIP143 - SegWit署名ハッシュ計算
- ✓ BIP174 - PSBT (Partially Signed Bitcoin Transaction)

受取アドレス機能:

受取画面で各通貨の代表アドレスを表示。カスタムパス機能でBIP32/BIP44準拠の任意の導出パスを指定可能。

通貨	標準導出パス（例）	ネットワーク切替	カスタムパス
Bitcoin	m/84'/0'/0'/0/0	Mainnet / Testnet	✓ secp256k1
Ethereum	m/44'/60'/0'/0/0	-	✓ secp256k1
XRP	m/44'/144'/0'/0/0	-	✓ secp256k1 / Ed25519
Solana	m/44'/501'/0'	-	✓ Ed25519
TRON	m/44'/195'/0'/0/0	-	✓ secp256k1

- オンデマンド導出（選択時に計算）
- 通貨別キャッシュ（BTC/ETH/XRP/SOL/TRX独立）
- Bitcoin選択時: Mainnet/Testnetドロップダウンでネットワーク切替可能（アドレスフォーマットが異なるため）

カスタムパス機能:

受取画面でBIP32導出パスの各要素を個別に指定可能。署名アルゴリズムごとに2エントリ: - **Custom Path (secp256k1)**: BIP32標準鍵導出。BTC/ETH/XRP等のアドレス生成 - **Custom Path (Ed25519)**: SLIP-0010準拠鍵導出。Solana/XRP Ed25519等のアドレス生成

パス要素	説明	選択可能値
Purpose	BIP規格	44 (Legacy) / 49 (Nested SegWit) / 84 (Native SegWit) / 86 (Taproot)
Coin Type	通貨識別子	0 (BTC) / 1 (BTC Test) / 60 (ETH) / 144 (XRP) / 195 (TRX) / 501 (SOL)
Account	アカウント番号	0〜9
Change	受取/お釣り/省略	(none) / 0 (受取) / 1 (お釣り)
Index	アドレスインデックス/省略	(none) / 0〜99

可変パス深さ: Change/Indexに`(none)`を指定するとそのレベルを省略できる（3〜5レベル）。 - 例: Solana標準 `m/44'/501'/0'` → Change=(none), Index=(none) で3レベル - 例: BTC標準 `m/84'/0'/0'/0/0` → 全指定で5レベル

Hardened導出ルール: - secp256k1: Purpose/CoinType/Accountはhardened、Change/Indexは非hardened（BIP44準拠） - Ed25519: 全レベルhardened（SLIP-0010準拠）

2.3 組み込み通貨・トークン、ネットワーク・チェーン総数

カテゴリ	通貨/トークン数	ネットワーク数	備考
Bitcoin	1 (BTC)	2	Mainnet + Testnet
Solana	1 (SOL)	3	Mainnet + Devnet + Testnet
TRON	1 (TRX)	3	Mainnet + Shasta + Nile
XRP Ledger	1 (XRP)	2	Mainnet + Testnet
EVM	2,599 (ERC-20)	215	129 Mainnet + 86 Testnet
合計	**2,603**	**225**	

2.4 組み込みEVMネットワーク - 215ネットワーク

Openloopは**すべてのEVMネットワーク**に対応しています。以下は、ネットワーク名がデバイス画面に表示される組み込み済みネットワークの一覧です。

非組み込みネットワーク:　一覧に含まれていないEVMネットワークも署名可能です。署名確認画面では「Chain ID: XXXXX」と表示されます。

EVMメインネット (129ネットワーク)

ネットワーク名	Chain ID	ネイティブ通貨
Ethereum	1	ETH
Optimism	10	ETH
Flare Network	14	FLR
Songbird	19	SGB
Elastos	20	ELA
KardiaChain	24	KAI
Cronos	25	CRO
Rootstock RSK	30	RBTC
Telos	40	TLOS
XDC Network	50	XDC
BNB Smart Chain	56	BNB
Syscoin NEVM	57	SYS

ネットワーク名	Chain ID	ネイティブ通貨
OKT Chain	66	OKT
Meter	82	MTR
Viction	88	VIC
Gnosis Chain	100	XDAI
Velas	106	VLX
Fuse	122	FUSE
Huobi ECO Chain	128	HT
Unichain	130	UNI
Polygon	137	POL
Monad	143	MON
Sonic	146	S
Manta Pacific	169	ETH
HashKey Chain	177	HSK
Mint	185	ETH
X Layer	196	OKB
BitTorrent	199	BTT
opBNB	204	BNB
Lens	232	GHO
TAC	239	TAC
Fantom	250	FTM
Fraxtal	252	frxETH
Kroma	255	ETH
Boba Network	288	ETH
Hedera	295	HBAR
zkSync Era	324	ETH
PulseChain	369	PLS
Cronos zkEVM	388	zkCRO
SX Network	416	SX
World Chain	480	ETH
Astar	592	ASTR

ネットワーク名	Chain ID	ネイティブ通貨
Flow EVM	747	FLOW
QL1	766	QOM
Bittensor EVM	964	TAO
Stable	988	FREE
HyperEVM	999	HYPE
Conflux eSpace	1030	CFX
Metis Andromeda	1088	METIS
Polygon zkEVM	1101	ETH
WEMIX	1111	WEMIX
Core	1116	CORE
Lisk	1135	ETH
Moonbeam	1284	GLMR
Moonriver	1285	MOVR
Glue	1300	GLUE
Sei	1329	SEI
Story	1514	IP
Gravity	1625	G
Soneium	1868	ETH
LightLink	1890	ETH
Swellchain	1923	ETH
Milkomeda C1	2001	milkADA
Ronin	2020	RON
Vanar	2040	VANRY
Kava	2222	KAVA
Goat	2345	BTC
Abstract	2741	ETH
Morph	2818	ETH
Peaq	3338	PEAQ
Botanix	3637	BTC
SX Rollup	4162	SX

ネットワーク名	Chain ID	ネイティブ通貨
Merlin Chain	4200	BTC
IoTeX	4689	IOTX
Mantle	5000	MNT
Somnia	5031	STT
Superseed	5330	ETH
Saga	5464	SAGA
DuckChain	5545	TON
Nibiru	6900	NIBI
ZetaChain	7000	ZETA
Cyber	7560	ETH
Canto	7700	CANTO
Kaia	8217	KAIA
Base	8453	ETH
IOTA EVM	8822	IOTA
Evmos	9001	EVMOS
Plasma	9745	FSN
SmartBCH	10000	BCH
BEVM	11501	BTC
Immutable zkEVM	13371	IMX
0G	16661	A0GI
Map Protocol	22776	MAPO
Oasis Sapphire	23294	ROSE
Mezo	31612	BTC
ApeChain	33139	APE
Mode	34443	ETH
Energi	39797	NRG
EDU Chain	41923	EDU
Arbitrum One	42161	ETH
Arbitrum Nova	42170	ETH
Celo	42220	CELO

ネットワーク名	Chain ID	ネイティブ通貨
Etherlink	42793	XTZ
Hemi	43111	ETH
Avalanche C-Chain	43114	AVAX
Zircuit	48900	ETH
Sophon	50104	SOPH
Superposition	55244	ETH
Ink	57073	ETH
Linea	59144	ETH
Henesys	68414	HNS
Berachain	80094	BERA
Blast	81457	ETH
Zedxion	83872	ZEDX
Plume	98866	ETH
Taiko	167000	ETH
Bitlayer	200901	BTC
Scroll	534352	ETH
Katana	747474	ETH
XRPL EVM	1440000	XRP
Zora	7777777	ETH
Corn	21000000	BTCN
Neon EVM	245022934	NEON
Degen	666666666	DEGEN
Ancient8	888888888	ETH
Aurora	1313161554	ETH
Rari Chain	1380012617	ETH
Harmony	1666600000	ONE
SKALE Europa	2046399126	sFUEL

EVMテストネット (86ネットワーク)

ネットワーク名	Chain ID	ネイティブ通貨
Ethereum Sepolia	11155111	ETH
Ethereum Holesky	17000	ETH
Optimism Sepolia	11155420	ETH
Arbitrum Sepolia	421614	ETH
Base Sepolia	84532	ETH
Polygon Amoy	80002	POL
zkSync Sepolia	300	ETH
Linea Sepolia	59141	ETH
Scroll Sepolia	534351	ETH
Polygon zkEVM Cardona	2442	ETH
BNB Testnet	97	tBNB
Avalanche Fuji	43113	AVAX
Fantom Testnet	4002	FTM
Cronos Testnet	338	TCRO
Flare Coston2	114	C2FLR
Songbird Coston	16	CFLR
Rootstock Testnet	31	tRBTC
Telos Testnet	41	TLOS
XDC Apothem	51	TXDC
OKT Chain Testnet	65	OKT
Meter Testnet	83	MTR
Viction Testnet	89	VIC
Gnosis Chiado	10200	XDAI
Fuse Sparknet	123	SPARK
Huobi ECO Testnet	256	HT
opBNB Testnet	5611	tBNB
Fraxtal Testnet	2522	frxETH
Kroma Sepolia	2358	ETH

ネットワーク名	Chain ID	ネイティブ通貨
Boba Sepolia	28882	ETH
Hedera Testnet	296	HBAR
PulseChain Testnet	943	tPLS
Cronos zkEVM Testnet	282	zkTCRO
Conflux eSpace Testnet	71	CFX
Metis Sepolia	59902	tMETIS
WEMIX Testnet	1112	tWEMIX
Core Testnet	1115	tCORE
Lisk Sepolia	4202	ETH
Moonbase Alpha	1287	DEV
Soneium Minato	1946	ETH
LightLink Pegasus	1891	ETH
Ronin Saigon	2021	RON
Kava Testnet	2221	TKAVA
Abstract Testnet	11124	ETH
Morph Holesky	2810	ETH
Merlin Testnet	686868	BTC
IoTeX Testnet	4690	IOTX
Mantle Sepolia	5003	MNT
ZetaChain Athens	7001	aZETA
Canto Testnet	7701	CANTO
Kaia Kairos	1001	KAIA
IOTA EVM Testnet	1075	IOTA
Evmos Testnet	9000	tEVMOS
SmartBCH Testnet	10001	BCHT
BEVM Testnet	11503	BTC
Immutable zkEVM Testnet	13473	tIMX
Oasis Sapphire Testnet	23295	TEST
ApeChain Curtis	33111	APE
Mode Sepolia	919	ETH

ネットワーク名	Chain ID	ネイティブ通貨
Energi Testnet	49797	tNRG
Celo Alfajores	44787	CELO
Zircuit Testnet	48899	ETH
Berachain Bartio	80084	BERA
Blast Sepolia	168587773	ETH
Taiko Hekla	167009	ETH
Bitlayer Testnet	200810	BTC
Zora Sepolia	999999999	ETH
Neon EVM Devnet	245022926	NEON
Aurora Testnet	1313161555	ETH
Harmony Testnet	1666700000	ONE
Flow EVM Testnet	545	FLOW
X Layer Testnet	195	OKB
BitTorrent Donau	1029	BTT
Sonic Blaze	57054	S
Lens Sepolia	37111	GHO
World Chain Sepolia	4801	ETH
Story Aeneid	1513	IP
Gravity Sepolia	13505	G
Unichain Sepolia	1301	ETH
Manta Pacific Sepolia	3441006	ETH
Mint Sepolia	1687	ETH
HashKey Testnet	133	HSK
Etherlink Testnet	128123	XTZ
Hemi Sepolia	743111	ETH
Ink Sepolia	763373	ETH
Plume Testnet	98864	ETH
XRPL EVM Devnet	1440002	XRP

2.5 組み込みERC-20トークン - 2,599トークン

Openloopは**すべてのERC-20トークン**に対応しています。ファームウェアにはCoinGecko時価総額Top 1000トークンのマルチチェーン展開を含む**2,599トークン**が組み込まれており、トークン情報（シンボル、デシマル、名前）が自動表示されます。

非組み込みトークン: 一覧に含まれていないERC-20トークンも署名可能です。署名確認画面では「ERC-20 Token」と表示され、コントラクトアドレスで識別できます。

トークンカテゴリ別内訳

カテゴリ	トークン数（概算）	代表例
ステーブルコイン	150+	USDT, USDC, DAI, JPYC, BUSD, TUSD, FRAX
DeFiトークン	400+	UNI, AAVE, LINK, CRV, MKR, COMP, SNX
ミームコイン	100+	SHIB, DOGE, PEPE, FLOKI, BONK
L2/インフラトークン	200+	ARB, OP, MATIC, IMX, LDO, BLUR
ゲーム/NFT	150+	AXS, SAND, MANA, ENJ, GALA, APE
AIトークン	50+	FET, AGIX, RNDR, OCEAN
その他	1,500+	各種プロジェクトトークン

主要ステーブルコイン (抜粋)

トークン名	シンボル	デシマル	対応チェーン数
Tether USD	USDT	6	15+
USD Coin	USDC	6	20+
Dai Stablecoin	DAI	18	10+
JPY Coin	JPYC	18	3
Binance USD	BUSD	18	5+
Frax	FRAX	18	5+

主要DeFiトークン (抜粋)

トークン名	シンボル	デシマル	対応チェーン数
Uniswap	UNI	18	5+
Chainlink	LINK	18	10+
Aave	AAVE	18	5+
Maker	MKR	18	1
Lido DAO	LDO	18	3
Arbitrum	ARB	18	1

注記:

- 上記以外のERC-20トークンも送金可能（コントラクトアドレスとして表示）
- トークンデータはCoinGecko APIから取得、Uniswap/1inch/CoinGeckoでdecimals検証済み（99.6%）
- トークンレジストリはファームウェア更新で拡張可能

2.6 Ethereum拡張機能

対応Ethereum標準規格:

規格	説明	対応状況
EIP-55	アドレスチェックサム (Mixed-case)	✓ 対応
EIP-155	リプレイ保護 (チェーンID署名)	✓ 対応
EIP-191	Personal Sign (メッセージ署名)	✓ 対応
EIP-712	Typed Structured Data署名	✓ 対応
EIP-1559	Type 2トランザクション (Priority Fee)	✓ 対応
EIP-2718	Typed Transaction Envelope	✓ 対応
EIP-2930	Access List Transactions (Type 1)	✓ 対応
EIP-4527	QR Code eth-sign-request	✓ 対応
EIP-7702	Set Code for EOAs (スマートアカウント委任)	✓ 対応
ERC-20	トークン標準	

規格	説明	対応状況
		✓ 対応

スマートコントラクト対応:

- ✓ **ERC-20トークン転送**: Transfer関数 (0xa9059cbb) 自動検出と金額表示
- ✓ **Contract Interaction**: 任意のスマートコントラクト呼び出し
- ✓ **Contract Creation**: コントラクトデプロイ

EIP-7702 スマートアカウント委任:

- ✓ **Authorization署名**: chain_id, delegate address, nonce を指定して署名
- ✓ **組み込み委任先レジストリ**: MetaMask, Coinbase, Uniswap, OKX の委任コントラクトを名前表示
- ✓ **未検証コントラクト警告**: 未登録の委任先に対して警告表示
- ✓ **委任解除 (Revoke Delegation)**: address(0) による委任解除 UI
- ✓ **chain_id=0 警告**: 全チェーン有効な委任に対して警告表示

マルチシグ対応:

- ✓ **EIP-712 Typed Data署名**: Safe (Gnosis Safe) マルチシグ対応
- ✓ **ドメインハッシュ/メッセージハッシュ表示**: ホストアプリでの検証用

トランザクションタイプの自動検出:

タイプ	表示名	検出条件
Send	“Send”	value > 0, data = empty
ERC-20 Transfer	“ERC-20 Transfer”	data = 0xa9059cbb…
Contract Interaction	“Contract Interaction”	data ≠ empty, methodSig ≠ transfer
Contract Creation	“Contract Creation”	to = null
Off-chain Signature	“Off-chain Signature”	EIP-712リクエスト
Smart Account Auth	“Smart Account Auth”	EIP-7702 Authorization署名

2.7 XRP Ledger対応

対応署名アルゴリズム:

規格	説明	対応状況
ECDSA secp256k1	secp256k1署名	✓ 対応
EdDSA Ed25519	Ed25519署名	✓ 対応

デュアル署名アルゴリズム:

XRP　Ledgerはsecp256k1とEd25519の2種類の署名アルゴリズムをサポート。Openloopはアドレスプレフィックスから自動判定: - `r` アドレス → アカウント情報から鍵タイプを判定 - カスタムパスで明示指定可能

トランザクション処理:

タイプ	表示名	検出条件
Payment	“XRP Payment”	TransactionType=0x0000
その他	“XRP Transaction”	上記以外

導出パス:

- 標準: m/44’/144’/0’/0/0 (secp256k1, BIP44準拠)
- Ed25519: m/44’/144’/0’/0/0 (SLIP-0010準拠、全hardened)
- アドレス形式: Base58Check (“r…” プレフィックス)

XRP技術仕様:

項目	値
トランザクションフォーマット	XRP Binary Format (バイナリ直接署名)
ハッシュプレフィックス	0x53545800 (“STX\0”)
署名ハッシュ	SHA-512 Half (先頭32バイト)
小数点	6桁 (1 XRP = 10^6 drops)

2.8 Solana対応

対応署名アルゴリズム:

規格	説明	対応状況
Ed25519	EdDSA署名 (RFC 8032)	

規格	説明	対応状況
		✓ 対応
Versioned Transaction	v0トランザクション (Address Lookup Table対応)	✓ 対応
Legacy Transaction	レガシートランザクション	✓ 対応

トランザクション解析:

タイプ	表示名	検出条件
SOL Transfer	“SOL Transfer”	System Program Transfer命令
SPL Token Transfer	“SPL Token Transfer”	Token Program Transfer命令
その他	“Solana Transaction”	上記以外

導出パス:

- WalletConnect/Solflare標準: m/44’/501’/0’/0’ (Ed25519, 全hardened, 4レベル)
- 受取画面デフォルト: m/44’/501’/0’ (3レベル)
- SLIP-0010準拠、2〜5レベルの可変パス深さに対応

2.9 TRON対応

対応インターフェース: USB, BLE（Air Gap QR非対応）

対応署名アルゴリズム:

規格	説明	対応状況
ECDSA secp256k1	secp256k1署名	✓ 対応

TRON技術仕様:

項目	値
カーブ	secp256k1 (Ethereumと同一)
アドレス生成	keccak256 → 0x41プレフィックス → Base58Check(SHA256D) → “T…”アドレス
TX署名ハッシュ	SHA-256（Ethereumのkeccak-256とは異なる）
V値	27 + recovery_id（固定、EIP-155なし）
BIP44パス	m/44’/195’/0’/0/0
小数点	6桁 (1 TRX = 10^6 SUN)

トランザクション解析:

タイプ	表示名	検出条件
TRX Transfer	“TRX Transfer”	TransferContract
TRC-20 Transfer	“TRC-20 Transfer”	TriggerSmartContract + transfer()
その他	“TRON Transaction”	上記以外

導出パス:

- 標準: m/44’/195’/0’/0/0 (secp256k1, BIP44準拠)
- アドレス形式: Base58Check (“T…” プレフィックス)

Ethereum互換性と差異:

TRONはEthereum派生のため多くの共通点があるが、重要な差異がある:

項目	Ethereum	TRON
カーブ	secp256k1	secp256k1 (同一)
アドレスハッシュ	keccak256	keccak256 (同一)
アドレスプレフィックス	0x (16進)	0x41 → Base58Check → “T…”
TX署名ハッシュ	keccak-256	**SHA-256**
V値	EIP-155 (chainId依存)	**27 + recovery_id (固定)**
Coin Type (BIP44)	60	195

2.10 対応署名メソッド

署名タイプ	BTC	ETH	XRP	SOL	TRX	対応インターフェース
トランザクション署名	✓	✓	✓	✓	✓ *1	USB, BLE, Air Gap *1
メッセージ署名 (personal_sign)	✓	✓	-	✓	✓	USB, BLE
型付きデータ署名 (EIP-712)	-	✓	-	-	-	USB, BLE
PSBT署名		-	-	-	-	

署名タイプ	BTC	ETH	XRP	SOL	TRX	対応インターフェース
	✓					USB, BLE, Air Gap
Authorization署名 (EIP-7702)	-	✓	-	-	-	USB, BLE
バッチ署名 (signAllTransactions)	-	-	-	✓	-	USB, BLE
署名+ブロードキャスト	✓	✓	-	✓	✓	USB, BLE

*1 TRXはUSB/BLEのみ対応（Air Gap QR非対応。コンパニオンウォレットが未整備のため）

ブロードキャスト（トランザクション送信）：

署名後のトランザクションブロードキャストはOpenloop Connect経由で実行:

通貨	メソッド	ブロードキャスト方式	対応ネットワーク
BTC	sendTransfer	Blockstream/ mempool.space API	Mainnet, Testnet
ETH	eth_sendTransaction	dApp経由（WalletConnect）	全EVMチェーン
SOL	solana_signAndSendTransaction	Solana JSON-RPC sendTransaction	Mainnet, Devnet, Testnet
TRX	tron_signAndSendTransaction	TronGrid API broadcastTransaction	Mainnet, Shasta, Nile

3. FIDO2/CTAP2 パスキー機能

OpenloopはFIDO2/CTAP2準拠のセキュリティキーとしても動作します。

3.1 概要

項目	仕様
プロトコル	CTAP2 (FIDO_2_0)
後方互換	U2F (FIDO U2F V2)

項目	仕様
通信	USB HID (FIDO Alliance Usage Page 0xF1D0)
署名アルゴリズム	ES256 (P-256/NIST) / EdDSA (Ed25519)
Discoverable Credentials	✓ 対応
User Presence (UP)	✓ デバイス画面での確認ダイアログ
User Verification (UV)	✓ デバイスPINによる認証
最大クレデンシャル数	100
クレデンシャルID長	32バイト

3.2 セキュリティ設計

- 秘密鍵はデバイスに一切保存しない（使用時にHW保護シードから導出、即消去）
- DualSecure保護: SE050 (ECDH) + ESP32 二重鍵
- SE050ハードウェアバインド: HMACマスターキー（読み出し不可）
- ウォレットとは独立したシード > 詳細は「パスキー DualSecure セキュリティアーキテクチャ」仕様書参照

3.3 対応ブラウザ・プラットフォーム

プラットフォーム	Chrome	Edge	Firefox	Safari
Windows	✓	✓	✓	-
macOS	✓	-	△	△

動作詳細:

- **Windows**: 全ブラウザでWebAuthn登録・認証・ユーザー拒否が正常動作（OS標準webauthn.dll経由）
- **macOS Chrome**: 登録・認証は正常動作。ユーザー拒否時はNotAllowedErrorとして正常処理
- **macOS Safari/Firefox**: 登録・認証は正常動作。ユーザーがデバイス側で承認しなかった場合、エラーにならずブラウザが応答待ちを続ける（プラットフォーム側の制限）。ブラウザの「キャンセル」ボタンで復帰可能

> 注: macOS Safari/Firefoxの応答待ち動作はOS側のAuthenticationServices/authenticator-rsフレームワークの制限であり、Openloopデバイス側の問題ではありません。CTAPHID_CANCELによるキャンセルは全プラットフォームで正常動作します。

3.4 SE050要件

SE050必須。未搭載時は自動無効化（UIからON不可）

3.5 ユーザーインターフェース

- ON/OFF切替、クレデンシャル一覧（仮想スクロール、最大100件）
- 個別削除、一括リセット
- 登録/認証時にRP名・ユーザー名を表示し承認/拒否を選択

3.6 U2F後方互換

U2F_REGISTER, U2F_AUTHENTICATE, U2F_VERSION対応

3.7 PIV/PKCS#11機能

OpenloopはPIV (Personal Identity Verification) 準拠のAPDUインターフェースを搭載し、PKCS#11ライブラリ経由でSSH認証やFirefoxクライアント証明書認証に使用できます。

項目	仕様
プロトコル	PIV (NIST SP 800-73互換サブセット)
通信	USB HID (Ledger HIDプロトコル)
署名アルゴリズム	ECDSA P-256 / Ed25519 / RSA-2048*
スロット	9A (Authentication), 9C (Digital Signature), 9D (Key Management), 9E (Card Authentication)
PIV ON/OFF	✓ デバイス設定画面で切替可能
PIV PIN	✓ オプション (6-8桁ASCII、SHA-256ハッシュ保存)

デュアルモード署名:

条件	動作	用途
USB経由でPIN認証済み	ブラインド署名（確認画面なし）	自動化・CI/CD
PIN未送信	デバイス確認画面表示	対話的利用

*RSA-2048はSE050C1/C2バリアントのみ対応。E2バリアントではEC鍵のみ使用可能。チップ対応は起動時に自動判定。

PKCS#11ライブラリ:

- macOS / Windows / Linux対応 (.dylib / .dll / .so)

- Openloop Connectアプリ経由でデバイスと通信
- SSH (`ssh -I`)、GPG (`gnupg-pkcs11-scd`)、PDF署名 (`pyHanko`)、Firefox、 `pkcs11-tool` 等のPKCS#11対応アプリケーションで使用可能

3.8 ファクトリーリセット時の動作

パスキー関連データ・PIVデータも全消去

---

4. 通信方式

4.1 QRコード通信 ✓ 実装済

用途: Sparrow Wallet等のデスクトップアプリとの連携（エアギャップ動作）

入力対応フォーマット:

フォーマット	説明	対応状況
BBQr V0/V1	マルチフレーム・マルチパート (Bitcoin)	✓ 対応
UR crypto-psbt	Bitcoin PSBT (Blockchain Commons)	✓ 対応
UR eth-sign-request	Ethereum署名リクエスト (EIP-4527)	✓ 対応
UR sol-sign-request	Solana署名リクエスト (Keystone互換)	✓ 対応
UR xrp-sign-request	XRP署名リクエスト	✓ 対応
Base64 PSBT	単一QR (Bitcoin)	✓ 対応
ZLIB圧縮	wbits=-10 (BBQr)	✓ 対応

出力対応フォーマット (設定で切替可能):

フォーマット	説明	推奨用途
BBQr	ZLIB圧縮、QR v4-5	Sparrow Wallet（推奨）
UR	Fountain codes	Keystone, AirGap Vault, Solflare
Base64	単一QR、非圧縮	汎用・デバッグ

QRコード仕様:

- QRバージョン: 4-5 (25×25〜27×27モジュール)
- エラー訂正: Level L
- 画面適合: Openloop (320×240)

4.2 USB通信 ✓ 実装済

プロトコル: USB HID

USBモード選択:

設定画面からUSBモードを選択可能。モード変更は即座に反映され、再起動不要。

モード	VID	PID	説明
独自	0x303A	0x8341	デフォルト。Espressif VID + Openloop PID（公式割当）
互換	0x2C97	0x1011	既存ウォレットアプリとの互換性が必要な場合

共通設定:

項目	値
Manufacturer	“Openloop”
Product	“Openloop Wallet”
インターフェース	HID + FIDO HID + CDC (複合デバイス、最大4インターフェース)
HIDパケットサイズ	64バイト

USB構成の3段階切替:

モード	USB設定	パスキー設定	インターフェース構成
CDC のみ	OFF	-	CDC (2インターフェース)
HID + CDC	ON	OFF	Ledger HID + CDC (3インターフェース)
HID + FIDO HID + CDC	ON	ON	Ledger HID + FIDO HID + CDC (4インターフェース)

USB識別子:

- ✓ Manufacturer文字列: “Openloop”
- ✓ Product文字列: “Openloop Wallet” (Chrome HIDダイアログに表示)
- ✓ VID/PID: ユーザー選択可能（Native/Compatible）

対応アプリケーション:

- ✓ **Sparrow Wallet**: Bitcoin対応
- ✓ **MetaMask**: Ethereum/ERC-20対応
- ✓ **Safe (Gnosis Safe)**: EIP-712マルチシグ対応
- ✓ **Rabby Wallet**: EVM対応
- ✓ **Solflare**: Solana対応
- ▲ **Ledger Live**: 非対応（デバイス認証チェックあり）

USB設定:

- Settings画面からUSB有効/無効を切替可能
- CDC (シリアルログ) は常時有効

USB OTA更新 (CBOR-RPC):

トランスポート	プロトコル	用途
CDC (シリアル)	Raw CBOR-RPC	OTA更新、シリアルログ、スクリーンキャプチャ
HID	TAG 0x06 CBOR over HID	OTA更新（Openloop Connect経由）

- OTAコマンド: “ota”, “ota_data”, “ota_complete”, “openloop_get_version”
- ZLIB圧縮対応、CRC32チャンク検証、SHA256ハッシュ検証
- Delta OTA対応 (差分更新)
- RSA-3072署名検証（後述）

スクリーンキャプチャー機能:

APDU (CLA=0xE0)	コマンド	説明
INS 0xF0	SNAP_MODE_ENTER	スナップモード開始
INS 0xF1	SNAP_MODE_EXIT	スナップモード終了
INS 0xF2	CAPTURE	画面キャプチャ

APDU (CLA=0xE0)	コマンド	説明
INS 0xF3	GET_CHUNK	データ取得 (480バイト/チャンク)
INS 0xF5	STREAM	全データストリーム送信

- 形式: RGB565 (320×240, 153,600バイト)
- 用途: ドキュメント作成、デバッグ

4.3 BLE通信 ✓ 実装済

プロトコル: Ledger Nano X互換GATT

項目	値
Service UUID	13D63400-2C97-0004-0000-4C6564676572
Notify Characteristic	13D63400-2C97-0004-0001-4C6564676572
Write Characteristic	13D63400-2C97-0004-0002-4C6564676572
デバイス名	“Openloop”
MTU	247バイト

セキュリティ:

項目	設定
ペアリング方式	Secure Connections (LE SC)
セキュリティレベル	Level 2 (MITM保護)
認証方式	Numeric Comparison (6桁コード)
暗号化	AES-CCM (128-bit)
ボンディング	NVS永続化 (最大3デバイス)

ペアリング:

- ✓ Numeric Comparison (6桁PIN表示)
- ✓ ボンディング情報のNVS保存
- ✓ ペアリング解除機能
- ✓ 無通信60秒で自動切断

対応アプリケーション:

- ✓ **MetaMask Mobile**: iOS/Android（動作確認済）
- ✓ **Rabby Wallet (モバイル)**: iOS/Android
- ▲ **Ledger Live Mobile**: 非対応（デバイス認証チェックあり）

BLE OTA更新 (Openloop専用サービス):

項目	値
OTA Service UUID	14b08099-71e4-4454-aeb1-23a8852e5d9e
RX Characteristic	32ea69e7-7cdf-4625-ae32-abbf9bf0e137
TX Characteristic	59db6df7-d86d-4316-90ca-5d3763e82d5d

- プロトコル: CBOR-RPC (USB CDCと共通)
- OTAコマンド: “ota”, “ota_data”, “ota_complete”, “openloop_get_version”
- ZLIB圧縮対応、SHA256ハッシュ検証
- セキュリティ: 独自UUID (他ウォレットツールと非互換)
- ハイブリッドアーキテクチャ: Ledger互換(支払) + Openloop独自(OTA)

対応OTAツール:

- ✓ `haulet_ble_ota.py` (Python CLI)
- ✓ Openloop Connect (iOS/Android モバイルアプリ)

4.4 APDUプロトコル (USB/BLE共通) ✓ 実装済

APDUコマンド処理は `apdu_handler` コンポーネントで実装され、USB HIDとBLE両方のトランスポート層から共通で使用されます。ウォレットアプリケーションはUSBまたはBLEどちらで接続しても同一の機能が利用可能です。

Ledger互換性レベル:

プロトコル	互換性	備考
CLA=0xE0 (Legacy)	✓ 部分対応	Bitcoin/Ethereum/XRP/Solana/TRON 主要コマンド
CLA=0xE1 (Bitcoin v2)	▲ 最小限	GET_EXTENDED_PUBKEY, GET_MASTER_FINGERPRINT のみ
CLA=0xB0 (Common)	✓ 対応	OPEN_APP, GET_BATTERY_STATUS

プロトコル	互換性	備考
CLA=0xF0 (Openloop)	✓ 独自	BTC PSBT署名、chain_id付き署名

エミュレートアプリバージョン:

アプリ	バージョン	備考
Dashboard (BOLOS)	2.0.6	Ledger Liveダッシュボード認識用
Bitcoin	2.0.6	Legacy Protocol (CLA=0xE0)使用のため
Ethereum	1.17.0	MetaMask/Safe/Rabby互換 (EIP-7702対応)
XRP	2.0.1	XRP Toolkit 2.0.0+要件を満たす
Solana	1.0.0	hw-app-solana互換
TRON	1.0.0	TronScan互換

- GET_VERSION (INS=0x01): Target ID=0x31100004 (Nano S), SE Version="1.6.1", MCU Version="1.0"
- GET_APP_CONFIGURATION (INS=0x06): バージョン 2.5.2 を返す

アプリ自動切替機能:

Openloopは接続されたウォレットのコマンドに基づいて自動的にアプリモードを切り替えます：

トリガー	動作
OPEN_APP "Bitcoin" (CLA=0xB0, INS=0x01)	→ Bitcoinモード
OPEN_APP "Ethereum"	→ Ethereumモード
OPEN_APP "XRP"	→ XRPモード
OPEN_APP "Solana"	→ Solanaモード
OPEN_APP "Tron"	→ TRONモード
closeApp (INS=0xA7)	→ Dashboardモード
Bitcoin専用INS (0x40, 0x42, 0x44, 0x48, 0x4A)	→ 自動でBitcoinモード
BIP32パス m/44'/0'/…	→ 自動でBitcoinモード
BIP32パス m/44'/60'/…	→ 自動でEthereumモード
BIP32パス m/44'/144'/…	→ 自動でXRPモード
BIP32パス m/44'/501'/…	→ 自動でSolanaモード

トリガー	動作
BIP32パス m/44'/195'/…	→ 自動でTRONモード

・初期状態: Ethereumモード (MetaMask BLE互換性のため)

・BIP32パス検出はINS=0x02, 0x04, 0x0C (EIP-712) で動作

対応APDUコマンド - CLA=0xE0 (Bitcoin Legacy Protocol):

INS	コマンド	状態	説明
0x40	GET_WALLET_PUBLIC_KEY	✓	公開鍵・アドレス取得
0x42	GET_TRUSTED_INPUT	✓	前トランザクション処理
0x44	UNTRUSTED_HASH_TX_INPUT_START	✓	入力ハッシュ開始
0x48	UNTRUSTED_HASH_SIGN	✓	トランザクション署名
0x4A	UNTRUSTED_HASH_TX_INPUT_FINALIZE	✓	出力ハッシュ確定

対応APDUコマンド - CLA=0xE1 (Bitcoin v2 Protocol):

INS	コマンド	状態	説明
0x00	GET_EXTENDED_PUBKEY	✓	xpub取得　(Sparrow対応)
0x01	REGISTER_WALLET	✗	ウォレットポリシー登録
0x02	GET_WALLET_ADDRESS	✗	ポリシーベースアドレス
0x03	SIGN_PSBT	✗	PSBT署名 (※CLA=0xF0またはQR経由で対応)
0x05	GET_MASTER_FINGERPRINT	✓	4バイトマスター指紋

対応APDUコマンド - CLA=0xE0 (Ethereum Protocol):

INS	コマンド	状態	説明
0x02	GET_PUBLIC_KEY	✓	公開鍵・アドレス取得
0x04	SIGN	✓	トランザクション署名

INS	コマンド	状態	説明
0x06	GET_APP_CONFIGURATION	✓	アプリ情報取得
0x08	SIGN_PERSONAL_MESSAGE	✓	メッセージ署名 (EIP-191)
0x0A	PROVIDE_ERC20_TOKEN_INFO	✗	トークン情報設定
0x0C	SIGN_EIP712	✓	EIP-712署名 (Safe対応)
0x34	SIGN_AUTH_7702	✓	EIP-7702 Authorization署名
0x14〜	その他	✗	NFT, Plugin等

対応APDUコマンド - CLA=0xE0 (XRP Protocol):

INS	コマンド	状態	説明
0x02	GET_ADDRESS	✓	XRPアドレス取得
0x04	SIGN_TX	✓	トランザクション署名

対応APDUコマンド - CLA=0xE0 (Solana Protocol, Ledger Solana互換):

INS	コマンド	状態	説明
0x05	GET_PUBKEY	✓	公開鍵取得 (生32バイトEd25519)
0x06	SIGN_MESSAGE	✓	トランザクション署名 (P2チャンキング対応)
0x07	SIGN_OFFCHAIN_MESSAGE	✓	オフチェーンメッセージ署名

・Ledger hw-app-solana互換: P2チャンキングプロトコル (P2_EXTEND=0x01, P2_MORE=0x02)
・pathsCountバイト自動検出・スキップ

対応APDUコマンド - CLA=0xE0 (TRON Protocol, coin_type=195'でルーティング):

INS	コマンド	状態	説明
0x02	GET_ADDRESS	✓	TRONアドレス取得 (Base58Check "T…")
0x04	SIGN_TX	✓	トランザクション署名 (SHA-256ハッシュ)

INS	コマンド	状態	説明
0x08	SIGN_MESSAGE	✓	メッセージ署名 (personal_sign)

- Ethereum Protocol (CLA=0xE0) と同じINSコードを共用。BIP32パスのcoin_type=195'で自動ルーティング
- INS=0x08は自動判定: coin_type=195'→TRONモード、それ以外→Ethereumモード

対応APDUコマンド - CLA=0xF0 (Openloop独自プロトコル):

INS	コマンド	状態	説明
0x70	BTC_SIGN_PSBT	✓	PSBT受信・署名
0x71	BTC_GET_SIGNED_PSBT	✓	署名済みPSBT取得
0x72	BTC_GET_ACCOUNT_XPUB	✓	アカウントxpub取得 (BIP32導出)
0x73	BTC_SIGN_MESSAGE	✓	Bitcoinメッセージ署名 (BIP-137)
0x08	ETH_SIGN_MESSAGE	✓	chain_id付きメッセージ署名
0x0C	ETH_SIGN_EIP712	✓	chain_id付きEIP-712署名

- Openloop Connect専用。chain_idパラメータにより正確なネットワーク名を確認画面に表示
- BTC PSBT署名: Ledger互換プロトコルでは対応できないPSBT直接署名をサポート
- BTC SIGN_MESSAGE: Bitcoin固有のメッセージ署名 (BIP-137形式)

---

5. ユーザーインターフェース

5.1 ハードウェア仕様

項目	仕様
デバイス	Openloop
画面サイズ	2.0インチ IPS LCD
解像度	320 × 240ピクセル
タッチ入力	静電容量方式タッチパネル

項目	仕様
カメラ	GC0308 (30万画素) QRスキャン用
スピーカー	AW88298 (I2Sオーディオ)

5.2 画面構成

スワイプナビゲーション（8画面）：

画面	機能
ホーム	受取アドレス表示
送金	カメラプレビュー、PSBT/トランザクションスキャン、確認・署名
受取	アドレスQRコード表示
ウォレット	新規ウォレット、ウォレット連携、ウォレット削除、リカバリーフレーズ
パスキー・PIV	パスキー　ON/OFF、クレデンシャル一覧・削除・リセット、PIV ON/OFF、PIV PIN管理
セキュリティ	PIN設定・変更・削除
通貨	サポートネットワーク・サポートトークンの表示、BTC Air Gap QR方式切替
設定	オーディオ、言語設定、USB設定、BLE設定、ファクトリーリセット、本製品について

- スクロール可能ナビバー（86px幅、90px間隔）
- 左右スワイプで画面切替
- “About”（バージョン、コピーライト、ライセンス）はSETTINGS内サブメニュー

その他の機能画面:

画面	アクセス方法
QRスキャン	SEND画面でカメラプレビュー・署名フロー
アニメーションQR表示	署名後に署名済みデータをQRコード表示
署名済みトランザクション表示	署名結果の詳細確認

5.3 多言語対応

- ✓ **日本語**: サポート (Noto Sans CJK JP)
- ✓ **英語**: サポート

・設定はNVSに永続化

5.4 音声フィードバック

音声	タイミング
起動音	アプリ起動時
クリック音	ボタンタップ時
進行音	QRフレーム読取時
成功音	操作成功時
エラー音	認証失敗、操作失敗時
決済音	トランザクション署名成功時

・音量調整: 0-100% (Settings画面)
・Click Sound: ON/OFF切替可能

---

6. セキュリティ

6.1 現在の実装 - Phase 2: SE050 DualSecure

セキュアエレメント SE050:

項目	仕様
チップ	NXP SE050 (EAL6+ 認証)
接続	I2C (400kHz)
鍵容量	50KB動的メモリ
署名鍵	ECDSA secp256k1 / EdDSA Ed25519

DualSecure暗号化:

entropy（ニーモニックの元データ）を**二重鍵**で保護:

鍵	保存場所	用途
K_esp	ESP32 NVS	ESP32側のHMAC派生鍵
A.priv	SE050内部	ECDH共有秘密生成用

両方の鍵が必要で初めてentropyを復号可能。

SE050署名鍵管理 (Key Cache V2):

項目	仕様
キャッシュ方式	Key Cache V2（統合50スロット）
ハッシュアルゴリズム	FNV-1a
衝突解決	オープンアドレッシング
退避方式	LRU (Least Recently Used)
導出タイミング	オンデマンド（署名時に必要な鍵のみ導出）

鍵タイプ	対応通貨
secp256k1	Bitcoin, Ethereum
EdDSA Ed25519	XRP, Solana

署名処理:

- **キャッシュヒット時**: SE050内でハードウェア署名（秘密鍵がRAMに出ない）
- **キャッシュミス時**: ソフトウェア署名（オンデマンド鍵導出）

暗号化ストレージ:

項目	仕様
entropy暗号化	AES-256-GCM
鍵派生	HMAC-SHA256 + ECDH
認証タグ	16バイト (改竄検知)
メモリ保護	memzero_explicit() によるRAMクリア

PIN認証:

- 4〜6桁のPINコード
- 段階的ロックアウト:
  - 0-2回失敗: ロックアウトなし
  - 3回失敗: 30秒ロックアウト
  - 4回失敗: 1分ロックアウト
  - 5回失敗: 5分ロックアウト
  - 6回以上失敗: 10分ロックアウト
  - 10回以上失敗: 永久ロックアウト
- PIN設定時は確認入力必須
- リセット時刻不整合攻撃対策実装済

物理的確認:

- トランザクション内容を画面で確認後に署名
- 署名/キャンセルボタンによる明示的な承認

6.2 セキュリティアーキテクチャ

3フェーズ戦略:

Phase	状態	ESP32	SE050	署名処理
Phase 1	完了	ソフトウェア暗号化	不使用	ソフトウェア
Phase 2	**現在**	DualSecure暗号化	**使用**	**SE050内**
Phase 3	将来	eFuse + DualSecure	使用	SE050内

Phase 2の特徴 (現在の実装):

- ✓ **署名鍵はSE050内でキャッシュ管理**: 50スロットのキャッシュに保存
- ✓ **キャッシュヒット時**: SE050内でハードウェア署名（秘密鍵がRAMに出ない）
- ✓ **キャッシュミス時**: ソフトウェア署名（オンデマンド鍵導出）
- ✓ **entropyはDualSecure保護**: ESP32 + SE050の両方が必要
- ✓ **Seedless署名**: キャッシュヒット時はseedすらロードしない

6.3 商用ウォレットとの比較

ウォレット	署名方式	セキュリティレベル
Openloop	**SE050内でハードウェア署名（キャッシュヒット時）**	**高**
Ledger Nano	SE内で署名	高
Trezor	MCU内ソフトウェア署名	中
Keystone	SE内で署名	高
Jade	MCU内ソフトウェア署名	中

6.4 セキュリティベストプラクティス

- **オフライン動作**: インターネット接続不要（Wi-Fi機能は使用しない）
- **ファームウェア署名検証**: OTA更新時にRSA-3072署名 + SHA256検証を実施

- **署名アルゴリズム**:
  - Bitcoin: ECDSA secp256k1 (RFC 6979準拠 決定論的署名)
  - Ethereum: ECDSA secp256k1 (EIP-155 リプレイ保護)
  - XRP: EdDSA Ed25519 / ECDSA secp256k1 (アドレスから自動判定)
  - Solana: EdDSA Ed25519 (RFC 8032準拠)
  - TRON: ECDSA secp256k1 (SHA-256ハッシュ、V=27+recovery_id)
- **乱数生成**: SE050 TRNG (True Random Number Generator)

OTAファームウェア署名検証:

項目	仕様
アルゴリズム	RSA-3072 + SHA-256 (RSA-PSS)
検証タイミング	OTA完了時 (esp_ota_end() 内部)
検証失敗時	OTAエラー（現FW維持）

7. ハードウェア仕様

7.1 ハードウェア仕様

項目	仕様
CPU	ESP32-S3 Dual-core Xtensa LX7 (240MHz)
RAM	512KB SRAM + 8MB PSRAM
Flash	16MB
ディスプレイ	2.0インチ IPS LCD (320×240) タッチ対応
カメラ	GC0308 (30万画素) QRスキャン用
スピーカー	AW88298 I2Sオーディオアンプ (22.05kHz/16bit)
USB	USB Type-C (OTG対応)
Bluetooth	BLE 5.0 (NimBLE)
Wi-Fi	2.4GHz 802.11 b/g/n（使用しない）
電源	USB給電 / 内蔵バッテリー（350mAh）

7.2 フラッシュパーティション構成

パーティション	タイプ	オフセット	サイズ	用途
nvs	data (nvs)	0x9000	32KB	設定データ保存
nvs_secure	data (nvs)	0x11000	32KB	ウォレットデータ(暗号化)
otadata	data (ota)	0x19000	8KB	OTAブート情報
phy_init	data (phy)	0x1B000	4KB	無線キャリブレーション
factory	app (factory)	0x20000	4MB	OTA Recovery Mini (リカバリーFW)
ota_0	app (ota_0)	0x420000	4MB	メインファームウェア スロット1
ota_1	app (ota_1)	0x820000	4MB	メインファームウェア スロット2
nvs_data	data (nvs)	0xC30000	256KB	CTAP2クレデンシャル、レジストリデータ
coredump	data (coredump)	0xC20000	64KB	クラッシュダンプ保存

OTA更新:

- 3スロット構成 (factory + ota_0 + ota_1)
- A/Bパーティション切替による安全な更新
- CBOR-RPC OTAプロトコル

7.3 リカバリーモード

メインファームウェアが起動できない場合の緊急復旧機能。

リカバリーモードに入る3つの条件:

条件	トリガー	保護レベル
電源ボタン長押し	起動音中に電源ボタンを離す	ユーザー操作
3回連続クラッシュ	メインFWが3回続けてクラッシュ	アプリケーションレベル
APP ROLLBACK	パーティションが破損/無効	ブートローダーレベル

電源ボタン操作: 1. デバイスの電源をOFFにする 2. 電源ボタンを押し続けて電源ON 3. 起動音（約1秒後）が鳴ったら電源ボタンを離す 4. 3秒以内に離すとリカバリーモードに移行

OTA Recovery Mini 機能:

機能	説明
USB OTA	HID + CDC 複合USBデバイス（両トランスポート同時対応）
BLE OTA	Openloop専用BLEサービス経由
設定画面	言語切替、USB/BLE有効化、BLEペアリング
メインFW起動	「メイン起動」ボタン（ota_0 → ota_1 フォールバック）
自動電源OFF	USB/BLE未接続で5分無操作時に自動シャットダウン
RSA署名検証	メインFW更新時にRSA-3072 + SHA256で署名検証

> 注: リカバリーFWはメインFWの更新のみ対応。リカバリーFW自体のOTA更新はできません。

対応OTAツール:

- ✓ Openloop Connect (iOS/Android)
- ✓ `openloop_ota.py` (Python CLI)

7.4 クラッシュダンプ (Coredump)

デバイスがクラッシュした際のデバッグ情報を自動保存。

項目	仕様
保存先	coredump パーティション (64KB)
保存タイミング	panic/abort 発生時
保存内容	スタックトレース、レジスタ状態
読み出し	`idf.py coredump-info` (開発者用)

8. ソフトウェア構成

8.1 技術スタック

コンポーネント	バージョン
ESP-IDF	v5.4
LVGL	9.4.0-dev
ESP-BSP	Openloop独自BSP
mbedTLS	3.6.2
NimBLE	ESP-IDF内蔵版
TinyUSB	ESP-IDF内蔵版
secp256k1	Bitcoin Core (サブモジュール)
trezor_crypto	trezor-crypto fork (PSRAM最適化版)

8.2 主要コンポーネント

コンポーネント	機能
apdu_handler	APDUプロトコル処理 (Ledger互換 + Openloop独自)
usb_hid	USB HIDトランスポート
usb_cdc	USB CDCトランスポート (OTA/スクリーンキャプチャ/シリアルログ)
ble_comm	BLE GATTトランスポート
wire_protocol	統合ワイヤプロトコル
psbt	Bitcoin PSBTパーサー/シリアライザー
bbqr / bbqr_wrapper	BBQrエンコード/デコード
esp32_bc-ur	UR (Uniform Resources) 処理
secure_storage	DualSecure暗号化ストレージ
nvs_wallet	ウォレット設定NVS管理
se050	SE050セキュアエレメント制御
network_registry	EVMネットワーク管理 (215チェーン)
token_registry	ERC-20トークン管理 (2,599トークン)
delegate_registry	EIP-7702委任先コントラクト管理

コンポーネント	機能
ethereum	ETH/ERC-20トランザクション処理
xrp	XRPトランザクション処理
solana	Solanaトランザクション処理・AirGap UR
bitcoin_utils	Bitcoin関連ユーティリティ
currency_abstraction	マルチ通貨抽象化層 (BTC/ETH/XRP/SOL/TRX)
aes_gcm	AES-256-GCM暗号化
cbor_rpc	CBOR-RPCプロトコル (OTA/スクリーンキャプチャ)
operation_lock	操作排他制御
screenshot_manager	スクリーンキャプチャ管理
audio_manager	オーディオフィードバック
language	多言語サポート (EN/JA)
ui_common	共通UIコンポーネント
ctap2	FIDO2/CTAP2プロトコルスタック (MakeCredential, GetAssertion, U2F)
ctaphid	CTAPHIDパケットフレーミング (HIDトランスポート層)
usb_hid_cbor	FIDO HIDパケット転送 + CBOR処理
ota_manager	OTA更新管理 (USB/BLE)
trezor_crypto	暗号ライブラリ (ed25519, secp256k1, SHA, HMAC等)

8.3 バイナリサイズ

- **ファームウェアサイズ**: 約2.6MB
- **利用可能スロットサイズ**: 4MB/スロット
- **空き容量**: 約1.4MB (35%)

9. 既存ウォレットとの互換性

9.1 対応ウォレットアプリ

アプリ	通信方式	BTC	ETH	XRP	SOL	TRX	備考
MetaMask Mobile	BLE	-	✓	-	-	-	iOS/Android、推奨
MetaMask (PC)	USB	-	✓	-	-	-	WebHID、EIP-712対応
Sparrow Wallet	QR / USB	✓	-	-	-	-	P2WSHマルチシグ対応
Safe (Gnosis Safe)	USB	-	✓	-	-	-	EIP-712マルチシグ対応
Rabby Wallet	USB / BLE	-	✓	-	-	-	マルチチェーン対応
XRP Toolkit	USB	-	-	✓	-	-	XRP専用
Solflare	USB / BLE	-	-	-	✓	-	Solana専用、Ledger互換
TronScan	USB	-	-	-	-	✓	Ledger HID互換、Shasta/Mainnet
WalletConnect dApps	WalletConnect	-	✓	-	✓	✓	Openloop Connect経由、600+ dApps
FIDO2 Webサイト	USB HID	-	-	-	-	-	パスキー登録・認証 (Windows/macOS)

アプリ	通信方式	BTC	ETH	XRP	SOL	TRX	備考
AirGap Vault	QR	✓	✓	✓	✓	-	UR互換
Keystone	QR	✓	✓	-	✓	-	UR互換
Ledger Live	-	✗	✗	✗	✗	✗	非対応（デバイス認証）

9.2 プロトコル互換性

プロトコル	互換性	対応通貨
Ledger Bitcoin App (CLA=0xE0)	✓ 互換性あり	BTC
Ledger Bitcoin v2 (CLA=0xE1)	▲ 部分対応	BTC (xpub/fingerprint)
Ledger Ethereum App (CLA=0xE0)	✓ 互換性あり	ETH/EVM/TRX
Ledger XRP App (CLA=0xE0)	✓ 互換性あり	XRP
Ledger Solana App (CLA=0xE0)	✓ 互換性あり	SOL
Ledger TRON App (CLA=0xE0)	✓ 互換性あり	TRX
BIP174 (PSBT)	✓ 互換性あり	BTC
UR crypto-psbt	✓ 互換性あり	BTC
UR sol-sign-request/sol-signature	✓ 互換性あり	SOL
UR xrp-sign-request	✓ 互換性あり	XRP
BBQr V0/V1	✓ 互換性あり	BTC
EIP-191 (personal_sign)	✓ 互換性あり	ETH/TRX
EIP-712 (Typed Data)	✓ 互換性あり	ETH
CTAP2 (FIDO2)	✓ 互換性あり	パスキー
U2F (FIDO)	✓ 互換性あり	パスキー (後方互換)
WalletConnect v2		ETH/SOL/TRX

プロトコル	互換性	対応通貨
	✓ 互換性あり	

9.3 競合製品との比較

表1: 基本仕様

製品	セキュアエレメント	画面	通信方式
Openloop	✓ **SE050 EAL6+**	**タッチ**	**Air Gap, USB, BLE**
Ledger Nano X	✓ EAL5+	ボタン操作	USB, BLE
Ledger Stax	✓ EAL6+	タッチ (E-Ink)	USB, BLE
Trezor Safe 5	✓ EAL6+	タッチ	USB
Trezor Safe 7	✓ TROPIC01	タッチ	USB, BLE
Keystone 3 Pro	✓ EAL5+ ×3	タッチ	Air Gap
Jade Plus	✗ 仮想SE	ボタン操作	Air Gap, USB, BLE

表2: 対応エコシステム

製品	Bitcoin	EVM	XRP	Solana	TRON	通貨/トークン数
Openloop	✓	✓ **(215チェーン)**	✓ **Ed25519/secp256k1**	✓	✓	**2,603**
Ledger	✓	✓	✓ secp256k1	✓	✓	5,500+
Trezor	✓	✓	✓	✓	✓	9,000+
Keystone	✓	✓	✓	✓	✗	5,500+
Jade	✓	✗	✗	✗	✗	BTCのみ

表3: 機能比較

機能	Openloop	Ledger Nano X	Keystone	Jade
Air Gap	✓	✗	✓	✓
USB	✓	✓	✗	✓
Bluetooth	✓	✓	✗	✓
タッチスクリーン	✓	✗	✓	✗
チェーン/トークン名表示	✓	✗	✓	✓
パスキー (FIDO2)	✓	✗	✗	✗
マルチチェーン	✓	✓	✓	✗

Openloopの特長:

- **3つの通信方式すべてに対応**: Air Gap、USB、Bluetooth
- **SE + タッチスクリーン + マルチチェーン**: この組み合わせは希少
- **XRP Ed25519署名対応**: アドレスから自動判定
- **TRON完全対応**: トランザクション署名 + メッセージ署名 + ブロードキャスト
- **充実したトランザクション確認画面**: チェーン/トークン名、トランザクション内容表示
- **FIDO2/CTAP2パスキー対応**: ハードウェアウォレットとセキュリティキーを1台で実現

9.4 独自モード戦略

Openloopは「**互換モード**」と「**独自モード**」の2つの動作モードを持つ。

モード	VID/PID	用途
独自モード	0x303A / 0x8341	Openloop Connect、Web SDK等で使用（デフォルト）
互換モード	0x2C97 / 0x1011	既存ウォレットアプリ（Sparrow、Rabby等）で使用

独自モードで動作する接続手段は拡大を続けており、互換モードへの依存度は低下している。

独自モード対応の接続手段:

接続手段	経路	プラットフォーム
WalletConnect	Openloop Connect経由	全プラットフォーム

接続手段	経路	プラットフォーム
LocalWebSocket	Openloop Connect経由	Desktop / Android
Safari Web Extension	Openloop Connect経由	iOS
WebHID	ブラウザから直接接続	Desktop (Chrome等)

独自モードの利点: - **自由な機能追加**: 互換性を気にせず、革新的な機能を実装可能 - **最適化されたUX**: Openloopハードウェアに特化したユーザー体験 - **迅速な開発**: 他社仕様への追従が不要、独自のロードマップで開発

WalletConnect対応dApp（600以上）、WebHID対応Webアプリ、ブラウザ拡張経由のWeb3　dAppなど、**独自モードだけで実用的なウォレットとして十分に機能する**環境が整いつつある。

---

10. 参考資料

10.1 Bitcoin技術標準 (BIP)

規格	説明	URL
BIP-39	ニーモニックコード	https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
BIP-32	HD Wallets	https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
BIP-44	マルチアカウント階層	https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki
BIP-84	Native SegWit導出パス	https://github.com/bitcoin/bips/blob/master/bip-0084.mediawiki
BIP-143	SegWit Sighash	https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki
BIP-174	PSBT	https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki

10.2 Ethereum技術標準 (EIP/ERC)

規格	説明	URL
EIP-155	リプレイ保護	https://eips.ethereum.org/EIPS/eip-155
EIP-712	Typed Structured Data	https://eips.ethereum.org/EIPS/eip-712

規格	説明	URL
EIP-1559	Fee Market Change	https://eips.ethereum.org/EIPS/eip-1559
EIP-2718	Typed Transaction	https://eips.ethereum.org/EIPS/eip-2718
EIP-4527	QR Code Data	https://eips.ethereum.org/EIPS/eip-4527
EIP-7702	Set Code for EOAs	https://eips.ethereum.org/EIPS/eip-7702
ERC-20	トークン標準	https://eips.ethereum.org/EIPS/eip-20

10.3 XRP Ledger技術標準

規格	説明	URL
XLS-11d	Secret Numbers	https://github.com/XRPLF/XRPL-Standards/tree/master/XLS-0011d-secret-numbers
XLS-12d	Secp256k1 Keys	https://github.com/XRPLF/XRPL-Standards/tree/master/XLS-0012d-secp256k1-keys
XRP Binary Format	トランザクションシリアライズ	https://xrpl.org/docs/references/protocol/binary-format
XRP Signing	署名アルゴリズム	https://xrpl.org/docs/concepts/transactions/finality-of-results/sign-the-transaction
XRP Address	アドレス形式 (Base58Check)	https://xrpl.org/docs/concepts/accounts/addresses
Payment Tx	基本送金トランザクション	https://xrpl.org/docs/references/protocol/transactions/types/payment

Openloop実装詳細:

- 鍵導出: BIP-44 (m/44’/144’/0’/0/0)
- 署名: ECDSA secp256k1
- アドレス: rXXX… 形式 (Base58Check + “r”プレフィックス)
- トランザクション: バイナリフォーマット直接署名

10.4 Solana技術標準

規格	説明	URL
Ed25519	EdDSA署名	https://ed25519.cr.yp.to/
Solana Transaction	トランザクションフォーマット	https://solana.com/docs/core/transactions
sol-sign-request	Keystone互換QR署名リクエスト	

規格	説明	URL
		https://github.com/KeystoneHQ/Keystone-developer-hub/blob/main/research/solana-qr-data-protocol.md
Solana JSON-RPC	RPC API	https://solana.com/docs/rpc

Openloop実装詳細:

- 鍵導出: SLIP-0010 Ed25519準拠、可変パス深さ (2〜5レベル)
  - WalletConnect/Solflare標準: m/44'/501'/0'/0' (4レベル、全hardened)
  - 受取画面デフォルト: m/44'/501'/0' (3レベル)
  - アプリにより導出パスの深さが異なるため、2〜5レベルの可変パス深さに対応
- 署名: EdDSA Ed25519 (RFC 8032)
- アドレス: Base58 (32バイト公開鍵のBase58エンコード)
- トランザクション: Legacy / Versioned (v0) 両対応

10.5 TRON技術標準

規格	説明	URL
TIP-1	TRON Address Standard	https://github.com/tronprotocol/tips/blob/master/tip-1.md
TRON Protocol	Protocol Buffers定義	https://github.com/tronprotocol/protocol
TronGrid API	TRON HTTP/JSON-RPC API	https://www.trongrid.io/

Openloop実装詳細:

- 鍵導出: BIP-44準拠 (標準パス m/44'/195'/0'/0/0)
- 署名: ECDSA secp256k1 (SHA-256ハッシュ、V=27+recovery_id)
- アドレス: T… 形式 (keccak256 → 0x41プレフィックス → Base58Check)
- トランザクション: Protocol Buffers形式のrawDataをSHA-256ハッシュして署名

10.6 FIDO2/CTAP2技術標準

規格	説明	URL
CTAP2	Client to Authenticator Protocol	https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html
WebAuthn	Web Authentication API	https://www.w3.org/TR/webauthn-2/

規格	説明	URL
U2F	Universal 2nd Factor	https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/
CTAPHID	HID Protocol	https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.html#usb

10.7 QRコード/エアギャップ通信規格

規格	説明	URL
UR	Uniform Resources	https://github.com/BlockchainCommons/Research/blob/master/papers/bcr-2020-005-ur.md
BBQr	Bitcoin Efficient QR	https://bbqr.org/
crypto-psbt	PSBT UR Type	https://github.com/BlockchainCommons/Research/blob/master/papers/bcr-2020-006-urtypes.md