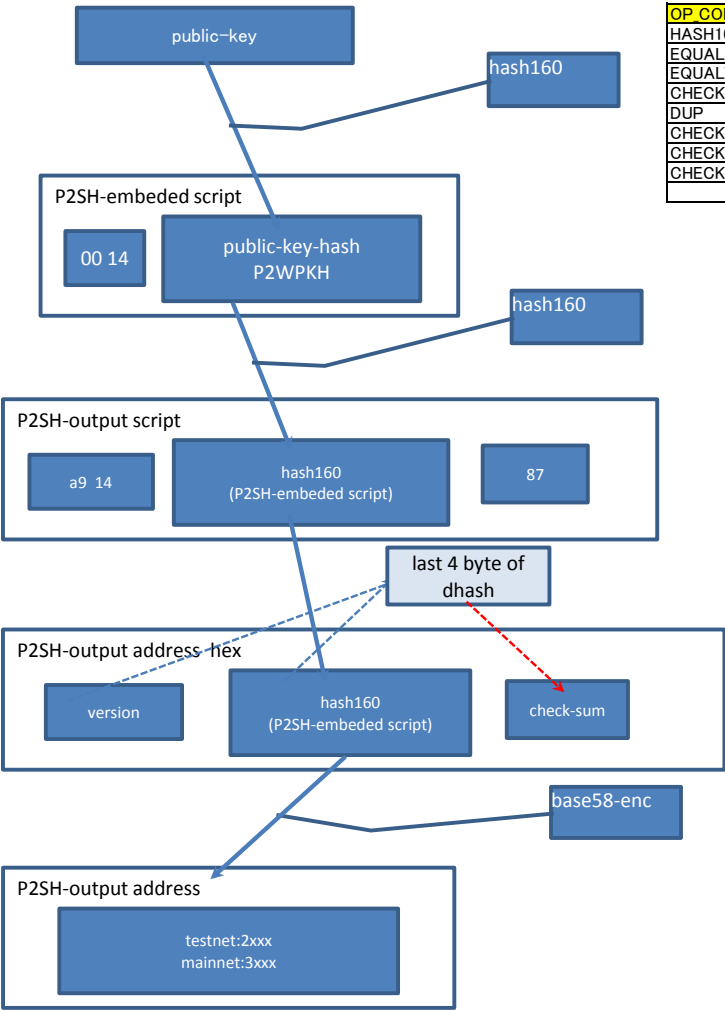


Sending to P2SH(P2WPKH) Output

Tx 構成	Script
Output Script	HASH160 [20-byte hash160(P2WPKH(public key hash))] EQUAL



OP CODE	HEX
HASH160	a9
EQUAL	87
EQUALVERIFY	88
CHECKSIG	ac
DUP	76
CHECKSIGVERIFY	ad
CHECKMULTISIG	ae
CHECKMULTISIGVERIFY	af

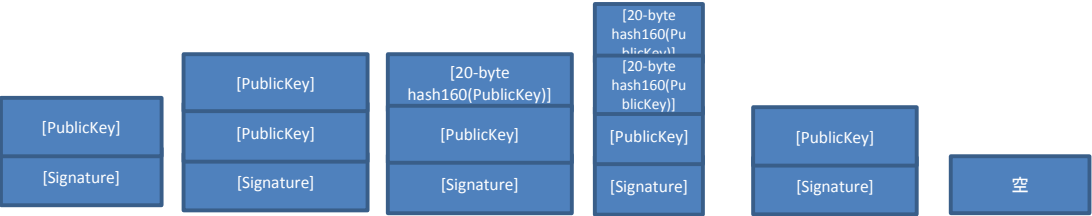
Redeem a P2SH(P2WPKH) Output

Tx 構成	Script
Output Script	指定先送金アドレス
Input Script	[00 14 <20-byte publicKeyHash>]
Script Code	DUP HASH160 [20-byte hash160(PublicKey)] EQUALVERIFY CHECKSIG
Witness	[Signature] [PublicKey]

hash160(Input Script) = previous P2SH-output script  
[Signature] [PublicKey] DUP HASH160 [20-byte hash160(PublicKey)] EQUALVERIFY CHECKSIG

スクリプトの検証順番は左から右へ行う

.....>



No.	Witness	構成
1		02 witness構成数
2		47 length [DER signature + sighash marker]
3		witness data [DER signature + sighash marker]
4		21 length [public key]
5		public key data [public key]