メモリマップ（低アドレス → 高アドレス）

【低：0x00000000...】

[.text / コード領域]
・内容：プログラムの命令 (main等)
・攻撃：ROPガジェットの探索
・権限：Read / Exec

[.rodata / 定数データ]
・内容：文字列 ("%d", "/bin/sh")
・攻撃：定数文字列の確認
・権限：Read Only

[.plt / 踏み台コード]
・内容：外部関数へのジャンプ台
・攻撃：ret2plt (systemの呼出)
・権限：Read / Exec

[.got.plt / 住所録] ★攻撃地点
・内容：関数の実アドレス格納場所
・攻撃：GOT Overwrite
・権限：Read / Write

[.data / 初期化済変数] ★攻撃地点
・内容：初期値ありグローバル変数
・攻撃：msgポインタの書き換え
・権限：Read / Write

[.bss / 未初期化変数] ★攻撃地点
・内容：初期値なし配列 (values[])
・攻撃：OOB / BoF の起点
・権限：Read / Write

[余白 / アライメント]

[ヒープ (Heap)]
・内容：malloc() 動的確保領域
・成長：(↓) 高アドレス方向へ伸びる
・攻撃：UAF / Heap Overflow
・権限：Read / Write

[:::::::::: 未使用領域 ::::::::::]

[ライブラリ (libc.so)]

・内容：system() 等の関数実体

・攻撃：Ret2Libc / One Gadget

・権限：Read / Exec

[:::::::::: 未使用領域 ::::::::::]

[スタック (Stack)]

・内容：ローカル変数 / 戻り先

・成長：(↑) 低アドレス方向へ伸びる

・攻撃：BoF / ROP の起点

・権限：Read / Write

[カーネル空間 (Kernel)]

・内容：OSの中枢領域

・制限：ユーザーアクセス不可

【高：0x7fffffffffff...】