

# OSB-Edge（Base版）自律防衛実演デモUI 一般取扱説明書

## 1. 本書の目的および実演デモUIの概要

本書は、株式会社オリビアが提供する次世代エッジセキュリティ基盤「OSB-Edge（Base版：特許出願 特願2026-200234）」の自律防衛機能を、Webブラウザ上で直感的に体感・検証できる「実演デモコンソール」の操作手順および機能解説をまとめた一般取扱説明書です。

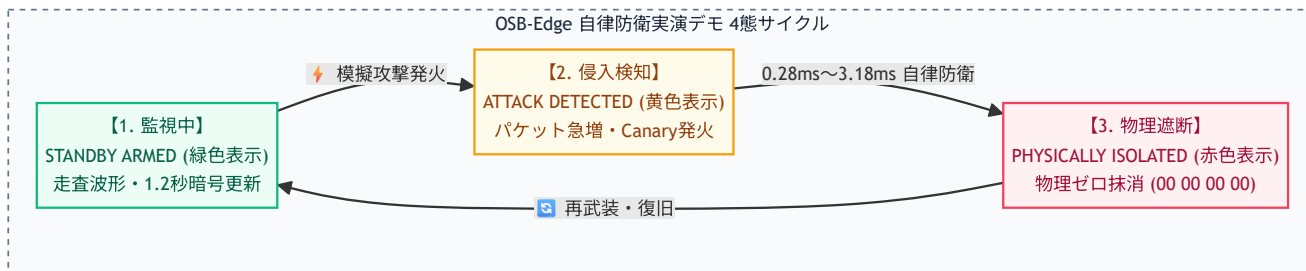
本デモコンソールは、外部ネットワークから切り離された環境や重要インフラ現場における「侵入検知」「暗号鍵即時抹消」「物理通信遮断」「安全復旧」の自律防衛サイクル（ミリ秒単位的高速隔離）を、特別なハードウェア接続を要することなくブラウザ上で何度でも実演・検証いただけるよう設計されています。

## 2. 4大自律防衛機能の基本概要

本実演デモUIでは、OSB-Edgeを構成する以下の4大自律防衛エージェントの連動動作を可視化しています：

- ①「侵入検知エッジ A I」（OSB-Canary）：ユーザー空間のおとりメモリ（Decoy Page）により、未知の侵入やメモリダンプ攻撃を0.28ms未満で予兆検知。
- ②「制御中枢エッジ A I」（OSB-Kernel）：特権カーネル空間（Ring 0）で動作し、侵入検知時に自律防衛・物理隔離を即時発令。
- ③「物理遮断器」（OSB-Axon）：MMIOレジスタ直接書き込みやリレー制御により、VRAM画面ロックおよびNIC外部通信を1～4ms以内で物理遮断。
- ④「暗号鍵物理消去器」（OSB-KMS）：侵害検知と同時にSRAM物理メモリ上の耐量子暗号鍵（ML-KEM-768等）や認証トークンを0.001ms（0.19μs）でゼロクリア上書き抹消。

## 3. 実演デモコンソールの4態サイクルと主要操作方法



### 3.1 主な操作機能

#### 1. 手動ワンクリック実演ボタン:

- 「⚡ 模擬攻撃を発火 (ATTACK)」：ボタンを押すと模擬攻撃パケットが着弾し、侵入検知エッジ A I（0.28ms）→ 暗号鍵物理消去器（0.19μs）→ 物理遮断器（3.18ms）が連動発火し、瞬時に画面ロック・通信遮断・SRAM完全ゼロ抹消（00 00 00 00）へ遷移します。
- 「🔄 再武装・復旧 (RE-ARM)」：遮断状態から平時待機モード（STANDBY ARMED / 緑色表示）へ即座に復帰し、暗号データの動的更新（1.2秒周期）を再開します。

## 2. 模擬攻撃シナリオ選択 & 実演実施:

- ① LSASSメモリダンプ: ※パソコン内のパスワード保管庫 (LSASS) を覗き見して暗号を盗み出す攻撃です。侵入された瞬間に画面ロックとネット通信を物理遮断して流出を防ぎます。代表例: Mimikatz、LockBit、Qilin (病院等を襲う身代金ウイルス)、TrickBot
- ② BYOVDドライバ悪用: ※正規の安全な部品 (ドライバ) の隙を突き、パソコンの心臓部 (カーネル) を乗っ取る攻撃です。セキュリティ機能を無理やり停止される前に即座に遮断します。代表例: BlackCat/ALPHV、Qilin (防衛無効化ランサムウェア)、RobbinHood
- ③ コンテナ脱獄&root: ※隔離された安全な小部屋 (コンテナ) の壁を突き破り、サーバー全体の最高管理者 (root) を奪う攻撃です。物理リレースイッチを作動させて回線を強制遮断します。代表例: Kinsing (仮想通貨を勝手に掘らせるウイルス)、Siloscape (脱獄マルウェア)、Doki
- ④ ASM外部露出ポート悪用: ※ネット上にうっかり開きっぱなしになった通信ドア (ポート) を探し出し、外から一気に侵入する攻撃です。おとり罠で即座に検知し、侵入ルートを瞬時に封鎖します。代表例: WannaCry (世界中で猛威を振るった身代金ウイルス)、Emotet、Mirai (IoT乗っ取り)
- ⑤ AIエージェント乗っ取り&MCP注入: ※仕事を手伝うAIを言葉の罠 (悪意ある指示) で騙し、社内の秘密データや暗号鍵を勝手に盗ませる最新の攻撃です。不正な指示を検知しAIの外部通信を遮断します。代表例: Prompt Injection (AI騙し攻撃)、Morris II (AI感染ワーム)、PoisonGPT

## 3. 主要5大OS切り替え実演:

- Linux (コンテナエスケープ)、Windows 11 (LSASSダンプ)、macOS (Mach-Oインジェクション)、μT-Kernel (CANバス改ざん)、Android (HAL不正アクセス) の各シナリオをタブ切り替えで即座に実演・検証可能です。

## 4. 汎用OS拡張予定注記:

- ※OSB-Edgeは、「FreeRTOS、QNX、VxWorks・・・等」の各種リアルタイムOS・汎用OSへの拡張提供も順次予定しています。

---

## 4. 実演デモUIへのアクセスURL

- OSB-Edge 実演デモコンソール: <https://cyber-armor-preview.vercel.app/>
- 株式会社オリビア 公式サイト: <https://orivia-hg.jp>