# 専用サーバー不要・クラウド送信ゼロの次世代オンプレミス防衛

## SupplyChain Enterprise Suite (v1.0.1)

公式実機ベンチマーク＆製品ブリーフ

検証年月：2026年11月 ｜ 開発：Studio Melchie LLC

# 専任の情シスがいない中堅・中小企業の「3重苦」を1本で解決

1. **終わらない高額サブスクと管理サーバー構築費からの解放**

　既存の社内共有フォルダ（NAS等）を連絡網として活用する独自の「サーバーレス自律分散設計」により、数百万円かかる専用管理サーバーの構築が一切不要。

2. **機密データを外部クラウドへ「1バイトも出さない」完全ローカル主権**

　社内台帳・セキュリティ状況・業務ログを外部AIや他社クラウドへ一切送信しないため、製造業・防衛関連・医療・士業などの厳格な機密保持基準を100%クリア。

3. **「実機の防衛」と「経産省基準の監査書類作成」を一体化**

日々のサイバー防衛だけでなく、経済産業省・IPA『SCS-400 Ver.1.1（最高位★4基準）』および米国『NIST CSF 2.0』に準拠した評価シート・社内基本規程（全10条）までワンクリックで自動出力。

【対応OS】** Windows **10/11** (64bit) ／ macOS 11以降 (Apple Silicon) ／ Linux (Ubuntu・Debian) 混在環境対応

# 客観的実機ベンチマーク検証結果（業務を止めない超軽量証明）

**検証環境：** 実稼働オフィス環境（バックグラウンド 1,041プロセス稼働中・外部通信量 0バイト）

| 検証テスト項目 | 計測内容・条件 | 実測結果 | 法人運用目標値 | 判定 |
| --- | --- | --- | --- | --- |
| **1. 通常業務での誤検知耐性** | オフィスソフト稼働＋大容量Excel連続生成（計50回反復） | **誤検知 0件（0.0%）** | `0.5%未満` | **合格** |
| **2. 異常検知時の即時遮断速度** | トリガー発生からローカル通信遮断完了まで（30回平均） | **0.50 ミリ秒** | `50ミリ秒未満` | **合格** |
| **2b. 突発残業時の即時現場復帰** | 管理者暗証番号（PIN）による隔離解除＆残業承認 | **1.33 ミリ秒** | `1秒未満` | **合格** |
| **2c. 重要データ復元検証（RTO）** | 暗号化バックアップの改ざん検査・復元テスト（SHA-256） | **0.042 秒（42.1ms）** | `300秒未満` | **合格** |
| **3. パソコンへの負荷（軽量性）** | 常駐監視時の平均CPU使用率 ／ メモリ使用量 | **CPU 0.1%未満 ／ 104.2 MB** | `CPU 3%未満` | **合格** |
| **4. 経産省SCS-400監査判定** | 全43項目（★4基準）＋NIST CSF 2.0 オフライン一括評価 | **0.23 秒（234ms）** | `2秒未満` | **合格* |

※パソコンが重くなることは一切なく、古い事務用ノートPCでも快適に常駐稼働します。

# 技術解説：なぜ「誤検知 0.0%」と「メモリ104MBの軽さ」が両立できるのか？

## 疑問①：なぜ通常の仕事で誤作動（誤検知）が起きないのか？

一般的なAI型セキュリティソフトは、普段のExcelマクロや大容量ファイル処理まで「怪しいかもしれない」と確率で推測するため、誤検知アラートが多発し業務が止まります。本製品は曖昧な推測に頼らず、**「通常業務では原理的に触れ得ないセキュリティ境界センサー」と「会社の営業時間ルール・不審管理コマンド検知」を組み合わせた決定論的設計** を採用しています。そのため、通常の事務作業では誤検知 **0.0%** を実現しつつ、ランサムウェアや自律型AIボットが機密探索を行った瞬間には **0.50ミリ秒** で確実に遮断します。万が一、社員が申請忘れで夜間残業し保護ロックがかかっても、外部サポートを何時間も待つことなく **現場の管理者がPIN番号で0.001秒で即時解除** できます。

# 技術解説：なぜ「誤検知 0.0%」と「メモリ104MBの軽さ」が両立できるのか？

## 疑問②：なぜ専用サーバー無しで、メモリ104MBと超軽量なのか？

親機（管理者PC）から発行した設定パック（`.dat`）を各社員の子機PCへ読み込ませる **「自律分散エッジ監視方式」** を採用しているためです。

・各PCが自分の内部だけで完結してC++17機械語エンジンで高速処理するため、重たい常時通信が不要でメモリ消費はわずか約104MB。

・社内NASの共有フォルダ1つで稼働状況を自動集約するため、Windows・Mac混在の社内でも幅広く一元把握が可能（親機の電源がOFFの間も、各子機は自律して端末を守り続けます）。

# 多層防御としての安心共存 ＆ コンサル不要の監査内製化

**既存のウイルス対策ソフトを消さずに「そのまま併用」可能（多層防御設計）**

本製品はWindows DefenderやMac標準保護などの一般的なウイルス対策ソフトと競合・衝突を起こさない設計です。

・「玄関で既知のウイルスを止めるOS標準対策」はそのまま活かし、

・「万が一すり抜けて侵入したランサムウェアや内部不正・夜間異常を社内で食い止める『第2の館内警備システム』」として重ねて導入することで、中小企業でも大企業水準の多層防御（Defense-in-Depth）が即日完成します。

# 多層防御としての安心共存 ＆ コンサル不要の監査内製化

**外注すれば50万〜100万円超かかる「取引先提出書類・社内規程」も自動生成**

・**公式SCS-410 自己評価シート（Excel / PDF）**：実機の防衛状況と連動してワンクリック出力

・**社内情報セキュリティ基本規程（全10条 PDF / 編集用テキスト）**：自社名・施行日入りで即座に制定可能

・**IT資産・スマホ脆弱性（14日ルール）台帳 ＆ 重要取引先（VRM）管理台帳**：全9ヶ国語対応