Cyber Security First Mover

AKDAN®

独自のハイパー分析検知

軽量ハイパーバイザー基盤

知能型セキュリティ威嚇対応ソリューション提供企業

About AKDAN INC.

サイバーセキュリティの未来をリードする企業です。

リアルタイムで発生する複雑且つ、精巧なセキュリティリスクを、迅速且つ、正確に検知し、
遮断できる**独自のハイパーバイザ基盤セキュリティソリューション**をご提供します。

History

2025
- **09 | 2025 初期創業パッケージ（Deep Tech）選定**
- **06 | 2025 優秀情報保護技術として指定（KISA）**
- 04 | AKDANHALL PED v1.0 国家機関（調達庁）加入
- 02 | AKDANHALL PED v1.0 国際化（英語）

2024
- 12 | ベンチャー企業認証獲得（R&D）
- **11 | 情報保護クラスター Closed-IR優先投資協議対象として指定**
- **11 | AKDANHALL PED v1.0 正式発売**
- 10 | TRIPITAKA SDK v1.0 正式発売
- **08 | シンボStartup NEST 16期**
- 01 | AKDANHALL PED v1.0 GS認証 1等級獲得

2023
- 12 | プログラムの著作権登録(AKDANHALL PED, TRIPITAKA)
- 11 | AKDANHALL PED v1.0 オープンベータサービス開始
- **10 | 城南創業競演大会 準々決勝**
- **08 | 京畿道民 新技術として指定**
- 07 | 企業付設研究所設立
- **06 | 創業成長技術開発政府課題 R&D 実施**
- **03 | 法人設立**

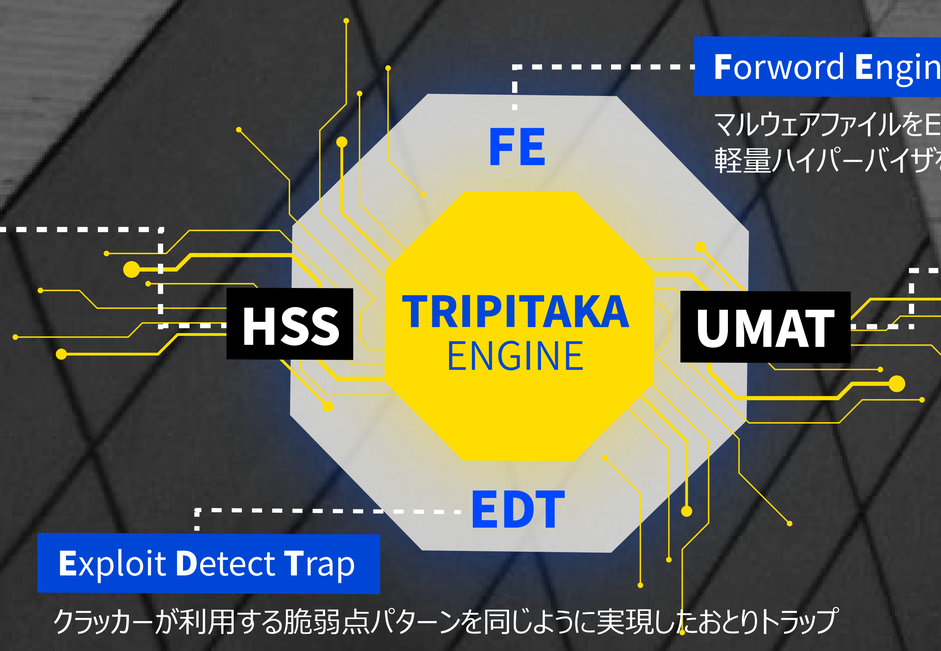
Technical Patent

特許出願 14 (登録 6件)



知能型威嚇対応 分析エンジン

AKDAN HYPER VISION
TECHNOLOGY



Forword Engineering
マルウェアファイルをEDT環境上で強制的に実行させる。
軽量ハイパーバイザを駆動する技術

High Speed Sandbox
マルウェア分析に最適化された
軽量ハイパーバイザで、
EDTとUMATを同時に作動させ、
検知を精巧且つ、迅速に実施

Unauthorized Memory Access Trap
メモリ上の異常動作と**脆弱点攻撃**をリアル
監視／検知

Exploit Detect Trap
クラッカーが利用する脆弱点パターンを同じように実現したおとりトラップ

1st Gen
ワクチン
シグニチャー比較
Unknown検知不可能

2nd Gen
侵入検知ソリューション
ネットワークパケット分析
知能型威嚇に対する対応不可

3rd Gen
APTソリューション
サンドボックス動的分析
容量が大きく、判断が遅い

4th Generation
AKDAN HYPER VISION
知能型威嚇ソリューション | ハイパー分析
超高速･高精度検知

Technical Features

当社は、他社製ソリューションが抱いているバージョン破片化、分析遅延、クラウドサービス未支援
ファイル解析用の追加ライセンス(OS/Office/App など) **追加購入費用などの問題が解決できる,**
知能型セキュリティ脅威を分析・遮断する、超高速・高精度検知ソリューションを提供します。

診断速度

1 Sec

他社平均 60秒以上

処理量

300 K+
One Day

他社平均 46K件

CPU 使用率

2.6%

平均 CPU 使用率

ライセンスフィー

0 $

Windows、MS Officeなど
別途のライセンス導入費用はありません。

区分	詳細区分	AKDAN®	A社	B社
分析プラットフォーム	OS	汎用（Windows／Linux）	Windows	Windows
	アプリケーション	軽量ハイパーバイザ おとりプログラム	Windows MS Officeなど	Windows MS Officeなど
	分析手法	ハイパー分析	サンドボックス 動的分析	サンドボックス 動的分析
分析性能	時間／件	1秒未満	~60秒	~300秒
	CPU／件	1core	1core	1core
	RAM／件	100MB	1GB	2GB
	同時分析件数	16	64	128
	分析件数／日	300,000	46,080	36,864
検査対象	文書	○	○	○
	マクロ	○	X（不可）	X（不可）
	実行ファイル	○（予定）	X（不可）	○
ライセンス 追加購入要否	分析環境	なし	OS Office	OS Office

ENDPOINT SOLUTION

AKDAN HALL PED



クラウド登録型サービス（年次更新）

使用方法
ユーザコンピュータにエンドポイントエージェントインストール

対象ユーザ
国内外の企業および個人ユーザー

Features

添付ファイルを開く同時に発生する知能型サイバー攻撃からエンドポイントを安全に守ります。
メールやメッセンジャー、USBなどの外部から入るコンテンツ基盤マルウェアを迅速に検知し、遮断ます。

- 実物サーバを構築する必要がなく、クラウド上の分析サービスを利用
- ファイル閲覧のタイミングでスキャンを行い、実行を事前に遮断
- 確認されたリスク要因や行為を分析し、レポートでご提供
- 注意ファイル／検査例外／検疫所／監査ログなどの機能ご提供

Service



SMB SOLUTION

AKDANHALL Mini

HWサーバに当社プラットフォームを搭載してご提供



使用方法

小規模インフラ向け分析サービスを実物サーバで運用

対象ユーザ

50~100名規模の中小企業

Features

顧客のインフラ環境で直接分析サービスを運用しています。

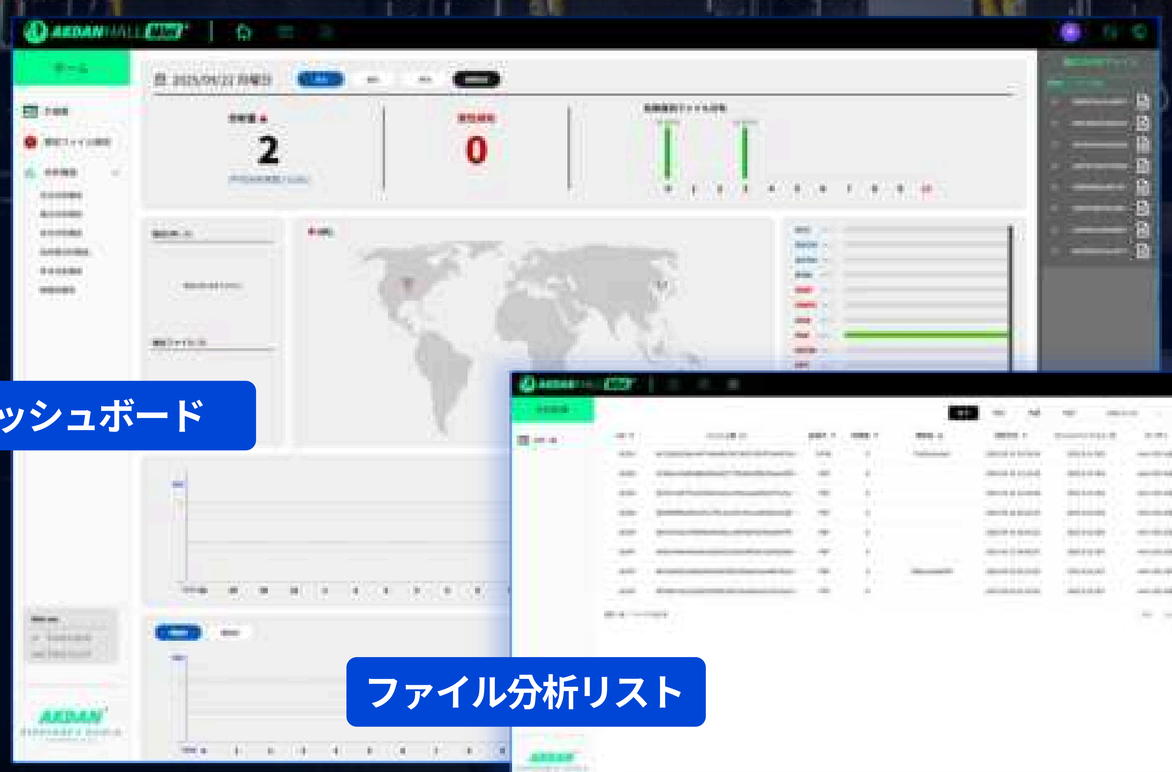
内部リソースを外部に持ち出せずにリスク分析が可能となります。

- 使用統計に基づいた日次／月次分析レポート作成及び、発送
- ピンポイント検査機能
- ユーザ別統計照会

Service



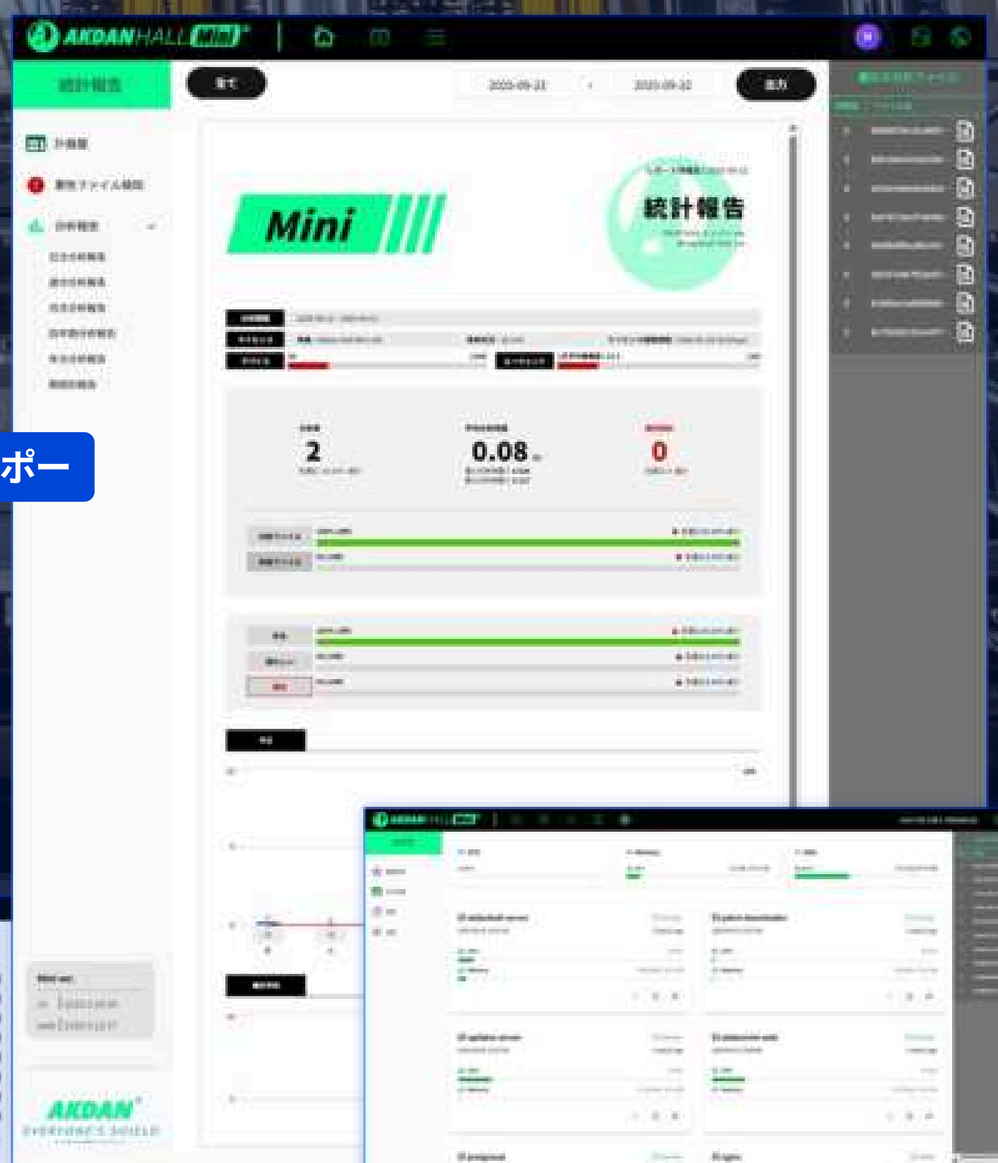
小型ミニサーバ



ダッシュボード

ファイル分析リスト

期間別レポー



管理者ページ

HYPER ANALYSIS TRIPITAKA ENGINE



分析エンジンSDK

使用方法

顧客社セキュリティ製品に当社SDKを組み込み、サービスをご提供

対象ユーザ

セキュリティ専門企業など

Features

文書やスクリプトファイルに隠されたマルウェアを1秒以内で検知·分析できる軽量ハイパーバイザ基盤エンジンです。

日々高度化しつつあるセキュリティリスクも迅速且つ精巧に取り出し、正確に分析します。

- 軽量ハイパーバイザ技術を利用することで、リソース使用が少なく、迅速な分析を実現
- 文書及びスクリプトなどの多様なタイプのファイル形式サポート
- WINDOWS及び、LINUXにて実行できるCLIパッケージご提供

「ハイパーバイザー基盤分析」とは？

OSより下位の層（仮想化レイヤー）で悪意ある挙動を監視・解析する技術です。
マルウェアがシステム内部で隠蔽や回避を試みた場合でも、より深いレベルで精密に検知することが可能です。
当社は、この分野で特許を取得した独自の技術力を基に、セキュリティソリューションを提供しています。

Service



tripitaka-sdk.zip

```
$ ./tripitaka
<Usage> tripitaka [In:File-path] [Out:Report-path] [In:License-code]
```

ENTERPRISE SOLUTION

AKDANHALL ES



高性能HWサーバーに当社プラットフォームを提供

使用方法
顧客インフラ向け分析サービスを実物サーバで運用

対象ユーザ
大手、公共機関、金融機関など500名以上の中・大規模企業

Features

大規模組織を持つ顧客向けのエンタープライズ実物サーバです。（今後発売予定）
メールやネットワーク分離などのネットワーク区間で利用可能なエンタープライズ向けソリューションです。

- AKDANHALL MINIの全ての機能を支援
- ネットワークインライン構成支援

Service

2026年発売予定

KISA
Korea Internet & Security Agency

2025年 優秀情報保護技術

AKDAN HYPER VISOR

FORWARD ENGINEERING



EXPLOIT HONEYPOT

Morphing SANDBOX

AKDAN INC.

京畿道 城南市 水正区 大旺パンギョ路 815 創業革新ゾーン東 4階 468号、13449
TEL | 031-698-4155　**FAX** | 031-698-4155
EMAIL | 031-698-4155

WWW.AKDAN.CO.KR