マルウェアの検知・削除のための包括的なソリューション

# Kaspersky Scan Engine

kaspersky BRING ON THE FUTURE

# はじめに

Kaspersky Scan Engine（KSEn）は、どのようなアプリケーションにも統合可能な、クラス最高の脅威検知ソリューションです。

Kaspersky Scan Engine（KSEn）はウェブポータル、ウェブアプリケーション、プロキシサーバー、ネットワーク接続ストレージ（NAS）、メールゲートウェイを包括的に保護します。

保護機能はHTTP や ICAP で提供され、簡単に管理でき、スタンドアローンサービスあるいは拡張性が高いクラスター、Docker コンテナとして使用できます。KSEn はトロイの木馬やフィッシングの脅威、ワーム、ルートキット、スパイウェア、アドウェアなどのマルウェアの検知と削除に最新の検知手法を使います。

## 統合のシナリオ

ウェブポータルやクラウドサーバー

ファイルサーバー

NAS

メールサーバー

プロキシやゲートウェイ

アプリストアやソフトウェア販売サイト

## 主な機能

### 2 つのメインモード

REST ライクサービス：クライアントアプリケーションから HTTP リクエストを受信し、HTTP リクエストで渡されたオブジェクトをスキャンして、HTTP レスポンスでスキャン結果を返します。

ICAP サービス：プロキシサーバー、NAS、Web アプリケーションファイアウォール、NGFW などの ICAP プロトコルを使用するソリューションを通過する HTTP トラフィックをスキャンします。ユーザーによってリクエストされた URL をスキャンすることも可能です。悪意のあるウェブページ、フィッシングやアドウェアのコンテンツがフィルタリングされます。

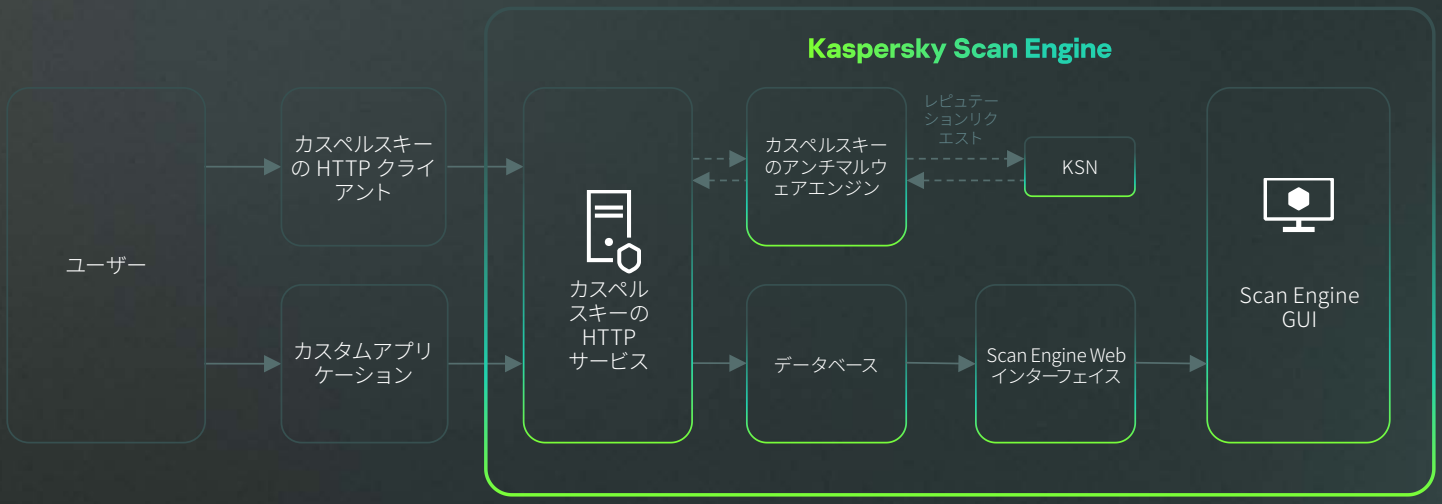
### KSEn for Linux

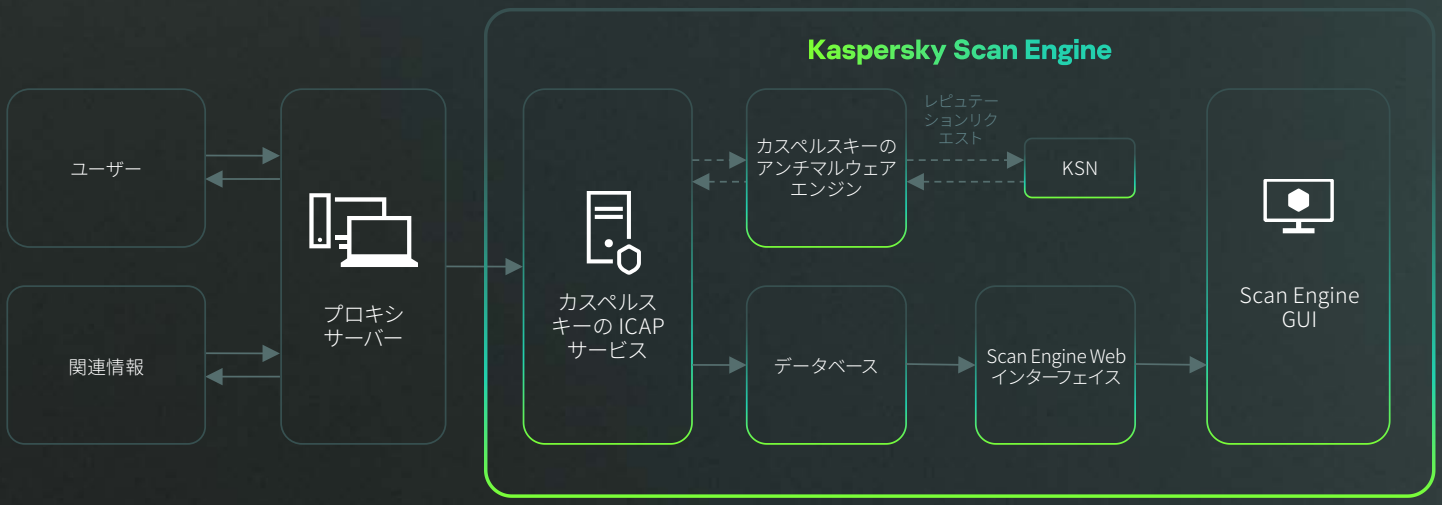
Linux Docker コンテナ（HTTP および ICAP モード内で）として使用することもできます。独立したコンテナとして Docker Swarm や Kubernetes、AWS EKS やその他の類似したクラウド環境にデプロイできます。

### GUI

Kaspersky Scan Engine にはウェブベースのグラフィカルユーザーインターフェイスがあり、製品の動作を簡単に設定でき、サービスイベントやスキャン結果を確認することができます。

# ユースケース




## どんなネットワークソリューションとも統合

多機能な REST ライク API とソースコード開示により、Kaspersky Scan Engine を自社ネットワーク上のほぼすべてのソリューションと簡単に統合できます。

Web ポータルをマルウェアのアップロードから保護

パブリッククラウドストレージ（AWS S3 バケットなど）とプライベートクラウドストレージ（Nextcloud、ownCloud、その他追加予定）を、悪意のあるコンテンツのアップロードから保護

アプリストアやソフトウェアマーケットプレイスを、悪意のあるアプリのアップロードから保護。

Windows/Linux のファイルストレージをスキャンしてマルウェアの有無を確認。

サードパーティの Web / メールゲートウェイ用のアンチマルウェアプラグイン。統合実績のリストについてはお問い合わせください。随時更新しています。

企業の文書管理システムやソフトウェア開発管理システムなど、マルウェア混入のチェックが必要なシステムでのアンチマルウェアモジュール。

# 主要な機能

## 受賞歴を誇る アンチマルウェア

多くの受賞の実績のあるKasperskyのアンチマルウェアテクノロジーが、最高クラスのマルウェア検知率を実現し、新たに出現する脅威に瞬時に対応します。

## フィルタ

悪意のある URL、フィッシング URL、アドウェア URL をブロックします。

## 検知

多重圧縮されているオブジェクトの検知。多数のパッカーやアーカイブ形式に対応しています。

## プラットフォームコネクター

Amazon S3、Nextcloud、ownCloud、Kubernetes など、多数のサードパーティ製プラットフォームをネイティブに、またはコネクターを通してサポートしています。

## ファイルの駆除

感染したファイル、アーカイブ、暗号化されたオブジェクトを駆除します。検知された脅威は、完全に削除するか、可能であれば、悪意のあるペイロードだけを削除して、ファイルの残りの部分を安全な状態で残すことができます。

## 最新プログラム

アップデート可能なアンチウイルスエンジン：定義データベースの定期的なアップデートによって検知テクノロジーと処理ロジックをアップグレードまたは変更できます。

## 高度な機能

高度なヒューリスティック分析と機械学習に基づく検知テクノロジー。

## ビッグデータ

ビッグデータの活用：Kaspersky Security Network がファイルの評価やウェブリソースに関する情報を提供し、それによってより迅速でより正確な検知を確実に行います。

## 拡張性

Kaspersky Scan Engine は最高レベルのパフォーマンスを提供し、拡張も非常に簡単にできます。

## フォーマットレコグナイザ

フォーマットレコグナイザコンポーネントで、フィルタリング層を追加できます。このコンポーネントを使用することで、スキャン処理で特定のフォーマットのファイルを認識したり、あるいはスキップしたりすることができます。実行可能ファイル、Office ファイル、メディアファイル、アーカイブなどの多数のフォーマットをサポートしています。

## TLS サポート

REST ライクサービスモードでは TLS プロトコル経由の通信がサポートされます。

## クラスターモード

Kaspersky Scan Engine はクラスターモードで実行できます。Kaspersky Scan Engine の複数のインスタンスを同じネットワーク内にデプロイし、ウェブ UI で管理することができます。

# Kaspersky Scan Engine 2.1 の新機能

2022 年 6 月リリース

## 安全性とコンプライアンス

- マルチユーザーモード、ロールベースのアクセスコントロール
- 操作の監査
- API トークンによる HTTP クライアント認証のサポート
- Web-UI でのパスワード総当たり攻撃からの保護

## アーキテクチャの変更

Scan Engine を 2 つのモジュールに分離。これらのモジュールは、(1) AV エンジン (KAV SDK)、(2) 主な製品機能 (KAV SDK のラッパーとしての Scan Engine) として個別にリリースされます。

## ドキュメントの改善

SIEM (MicroFocus ArcSight、Splunk) との統合用マニュアル、Oracle Solaris VScan、F5 Application Security Manager、GoAnywhere MFT、Dell Isilon OneFS との統合用マニュアル

## 運用の改善

systemd の完全サポートで各サービス (開始 / 停止 / ステータス / 再起動) の操作に対応

## クラスターモードの改善

アイドル状態のノードをクラスターから自動的に削除、異種混合 (HTTP、ICAP) クラスターのサポート。

## Syslog 出力の変更

複数の送信先
送信するイベントのフィルタリング。

# アワード

独立テスト機関によるカスペルスキー製品の最近の受賞歴

詳しくはこちら

# Kaspersky Scan Engine

30日間無料の評価版をご利用いただけます。
KSEn の評価版をご希望の場合は、 以下のリンクをクリックしてください。

詳しくはこちら

www.kaspersky.co.jp



#kaspersky
#bringonthefuture