



# マルウェア対策 SDK

## クロスプラットフォーム

クロスプラットフォームのマルウェア対策SDKの統合は、マルウェア、ゼロデイ、および高度な APT 攻撃に対する業界最高の保護をお客様に提供します。

お使いのアプリケーション、エンドポイント、システムにマルウェア対策 SDK を実装することで、ファイルをローカルでスキャンしマルウェアを検知できるようになります。また、未知のファイルをリアルタイムに分類する Avira Protection Cloud にアクセスすることもできます。これは URL の脅威の分類を提供する Avira URL Cloud によって補完されます。マルウェア対策 SDK は、セキュリティ製品やサービスの開発者およびプロバイダーが迅速に市場に参入するためのシンプルな方法を提供します。さらに、受賞歴のある Avira のテクノロジーに関する経験や知識を活用することで、社内開発に伴うコストや遅延を抑えることもできます。マルウェア対策 SDK は、主要なセキュリティサービスのほか、高性能なオフラインスキャン、Avira Protection Cloud へのオンライン接続を提供し、マルウェアに対する完全な保護を提供します。

Avira のマルウェア対策 SDK は、アンチウイルス/アンチマルウェアソリューションの実装を検討しているハードウェアおよびソフトウェアベンダーによって幅広く利用されています。

またこれは、エンドポイントでの検知やマネージドセキュリティサービスのプロバイダー、次世代ファイアウォールベンダー、電子メールゲートウェイ、統合脅威管理、ソフトウェアユーティリティプロバイダーのほか、サービスプロバイダーなど、マルウェア分析を自社の製品やサービスに統合しようと考えている事業者によって幅広く利用されています。

## 統合

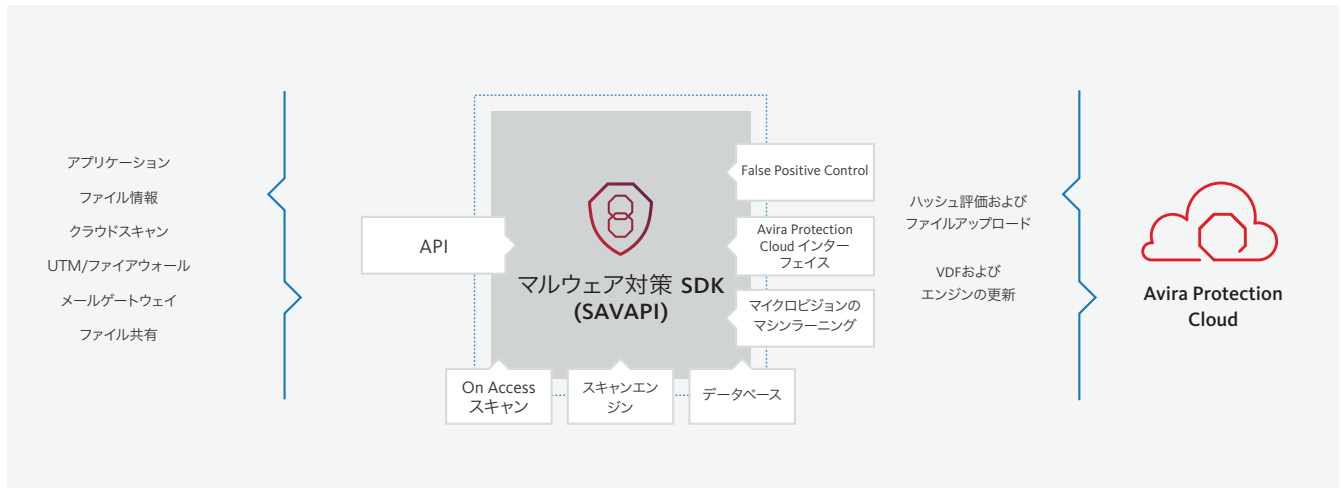
この SDK は C 言語で書かれており、一般的な C/C++ コンパイラで利用できます。いくつかの展開シナリオにより、最も単純なシナリオからより複雑なシナリオまで、幅広い統合オプションを提供します。内容: ライブラリモード: Windows (32ビットおよび 64ビット)、Linux、MacOS で利用可能な C ライブラリが、コールバックのサポートにより統合を完全にコントロールできるようにします。ファイル操作 (FOPS) コールバックを使用すると、SAVAPI はメモリを使用した仮想ファイルシステムおよび暗号化ファイルシステムと簡単に統合されます。デーモン/サービスモード: Unix およびネットワークソケット上のクライアント要求を待機するマルチスレッド サービスまたはデーモン。C#, Perl, Python, C, C++ などさまざまな統合方法を利用できます。

### 主な機能:

- 通常は数時間以内に完了する迅速な統合
- サービスを中断しないデーモンの更新
- あらゆるタイプのファイルのスキャンに対応
- シグネチャベース、ヒューリスティック、およびジェネリック分析を含むオフラインスキャン
- ローカルでのリスク評価を提供する統合マシン ラーニング
- Avira Protection Cloud との統合
- 強化された検出を提供するリアルタイムスキャナ 拡張
- False Positive Control



## マルウェア対策SDK統合の例



### AVIRA PROTECTION CLOUD

Aviraのマルウェア対策SDKをAvira Protection Cloudと併用すると、99.99%を超える検出率を達成できるほか、ゼロデイおよび高度なAPT攻撃からお客様を守ることもできます。マルウェア対策 SDKは分類されていない未知の疑わしいファイルを検出すると、Avira Protection Cloudにハッシュ照会を送信します。ハッシュが「未知」であると報告された場合(ゼロデイ攻撃のマルウェアの可能性ある)、ファイルをAvira Protection Cloudに送信し分析されることができ、Avira Protection CloudはAviraの第3世代のAIプラットフォーム、NightVision™を含む革新的なシステムとアルゴリズムを利用してファイルをリアルタイムで分類し、マルウェア対策システムにフィードバックを供給します。軽量のスキャンエンジンとほぼ無限のクラウドコンピューティングの力を組み合わせることにより、最高性能のマルウェア対策ソリューションを実現し、非常に迅速な応答時間を可能とします。

### ON-ACCESS の拡張機能

On-Accessはリアルタイムのスキャン拡張機能です。これにより、Aviraのマルウェア対策SDKがOSレベルでアクセスされるファイル、あるいは実行されるファイルを自動的にスキャンできるようになります。On-Accessは他のプロセスの実行やOSの前にスキャンを決定できるため、新たなセキュリティレベルが追加されます。自在に設定変更ができるほか、複数のフィルタリング機能、およびファイルアクセスやファイル実行イベントの検査も提供されます。

### FALSE POSITIVE CONTROL

False Positive Controlはリアルタイムで例外的な偽陽性検出の識別を確実にし、マルウェアスキャンのパフォーマンスへの影響を防止するAviraのメカニズムです。Aviraのマルウェア対策SDK、SAVAPIでご利用いただける無料オプションです。



## 仕様

サイズ:  
100MB

プラットフォーム要件:  
1.6GHz 以上の CPU, 512MB RAM アンパック専用の, 1GB のディスク領域

対応OS:  
Windows (32 ビットおよび64ビット)  
Linux, MacOS, FreeBSD, OpenBSD

実装:  
ライブラリだけのモード、デーモン/サービスだけのモード、またはClient Libraryおよびデーモン/サービスモード

機能性:  
>99.99% の検出率、ジェネリックおよびヒューリスティックスキャン、高度なアーカイブスキャナー、Windows 用 On-Access 拡張機能、False Positive Control、Avira Protection Cloud の統合

機能性:  
>99.99% の検出率、ジェネリックおよびヒューリスティックスキャン、高度なアーカイブスキャナー、Windows 用 On-Access 拡張機能、False Positive Control、Avira Protection Cloud の統合  
スキャンと検出:  
悪意のあるWindows PE 実行ファイルおよびDLL、Linux、MacOSおよびAndroid のマルウェア、悪意のあるスクリプト: JavaScript、VBScript など。Officeドキュメントおよび埋め込みマクロ  
アーカイブ解凍:  
ZIP,ZOO,ARJ,ARC,RAR パスワードで保護されたアーカイブのフラグ立て  
デコード:  
MBOX、MIME の添付ファイル

アドウェアおよびスパイウェア(選択):  
ワーム、メーラー、Webベースのマルウェア (HTML,JavaScript,VBS)、スクリプトウイルス、DOSバッチ、MIRC/IRCスクリプト、シェルスクリプト(Bashなど)、PIF,INI,REG(ASCII)

ウイルス(選択):  
暗号化プログラム、ポリモーフィック、メタモルフィックウイルス、ステルスウイルス、ブート/ファイル/マルチパートウイルス、Javaアプレット、ファイル形式の悪用、SPR(セキュリティまたはプライバシーのリスク: jokeなど)、バックドアのトロイの木馬(リモートアクセスのトロイの木馬)、パスワード/キーロガー/DoS、ドロップパーなどのマクロウイルス(MS Office、埋め込みオブジェクト、Excel計算式、MSO/HTML、PDF)

## OUR AWARDS



## FIND OUT MORE

Website: [oem.avira.com](http://oem.avira.com)

Email: [oem@avira.com](mailto:oem@avira.com)

Blog: [insights.oem.avira.com](http://insights.oem.avira.com)

Social Media: [@AviraInsights](https://twitter.com/AviraInsights)

### Europe Middle East, Africa

Avira  
Kaplaneiweg 1  
88069 Tettngang, Germany  
Tel: +49 7542 5000

### Americas

Avira, inc  
c/o WeWork, 75 E Santa Clara Street  
Suite 600, 6th floor San José  
CA 95113 United States

### Asia/Pacific and China

Avira Pte Ltd  
50 Raffles Place  
32-01 Singapore Land Tower  
Singapore 048623

### Japan

Avira GK  
8F Shin-Kokusai Bldg  
3-4-1, Marunouchi Chiyoda-ku  
Tokyo 100-0005, Japan

### China

中国北京市朝阳区东方东路19号  
外交办公大楼D1座17层1727室  
邮编: 100016