

アプリが被害にあう前に



CrackProof®

アプリケーションをクラッキングやチートから
保護するセキュリティソリューション

無防備なアプリケーションは クラッカー(攻撃者)にとって格好の標的です。

近年、さまざまな分野においてアプリケーションのクラッキング(不正な解析、改ざん)被害が数多く報告されています。これは、クラッキングに関する情報や、初心者にも簡単に使えるクラッキングツールが、インターネット上で容易に入手可能となり、10年前と比較しても潜在的なクラッカー(攻撃者)の数が激増したためです。

クラッキング被害としては以下のような例が挙げられます。

代表的なクラッキング被害

自動車

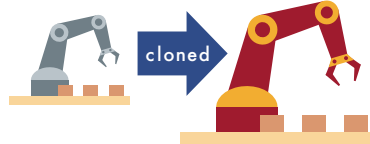
コネクテッドカーの
不正制御



自動車と連携するアプリが改ざんされ、自動車とスマートフォン間の認証が回避されると、車が遠隔から不正に制御される危険性があります。

産業機器

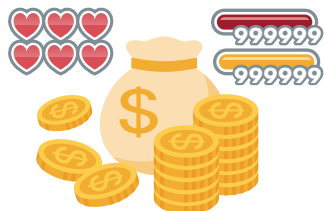
アルゴリズム
不正解析



組み込みアプリのアルゴリズムが解析されると、模倣製品が出回る原因に。入手したアルゴリズムを、競合他社に売却されるという被害も報告されています。

ゲーム

チートの横行



クラッキングにより不正ツールが作られることで、チート(課金回避や不正操作)が横行。ゲーム環境が荒れ、プレイヤー離れが起こる可能性があります。

エンタメ

コンテンツの
不正使用



電子書籍アプリを課金せずに閲覧されたり、VR関連アプリで内部コンテンツデータが不正に抽出されるなど、アプリ改ざんによる被害が多発しています。

認証システム

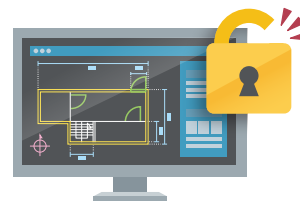
本人認証の
不正回避



電子決済の普及にともない、重要性が高まる認証システム。アプリが改ざんされると、本人認証の不正回避・なりすましが発生する原因となります。

業務用 ソフトウェア

海賊版の流通

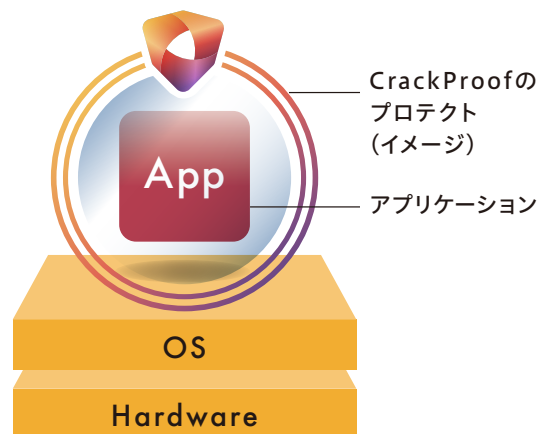


ソフトウェアの解析によって、ライセンス管理の仕組みが不正に解除されると、海賊版ソフトウェアが市場に流通してしまう可能性があります。



アプリケーションをクラッキングから 強力に保護するセキュリティ

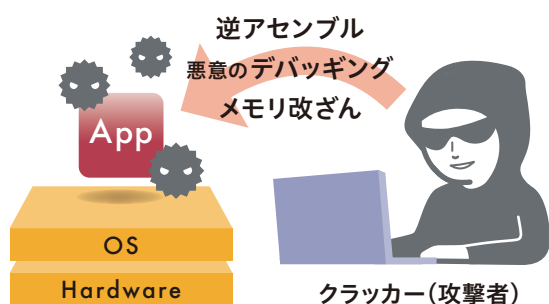
CrackProofは様々なクラッキング攻撃からアプリケーションを強力に保護する耐タンパセキュリティソリューションです。アプリケーションを包み込むようにプロテクトし、お客様の大切な知的財産を守ります。



セキュリティのイメージ

無防備なアプリケーション

アプリケーションはクラッカーの格好の標的となり攻撃を防ぐことができません。



CrackProofセキュリティ

CrackProofがアプリケーション全体をしっかりとプロテクトしてクラッキングを防ぎます。



クラッキング対策機能(一部)

静的解析対策

暗号化

実行ファイルを複数回暗号化し、逆アセンブルを阻止

コード改ざん対策

実行ファイルの改ざんチェックをすることでコード改ざんを阻止

コード難読化

コードの難読化により、逆アセンブルからの解析を阻止

動的解析対策

デバッガ対策

デバッガによる解析の阻止

エミュレータ対策

エミュレータ上でのアプリ実行を阻止

メモリアクセス対策

他プロセスからメモリアクセスを阻止

上記以外にもさまざまなクラッキング対策機能を搭載しています。

ご注意: 上記はCrackProof 各製品がもつ機能を列挙したものです。製品によって実装されていない機能もあります。

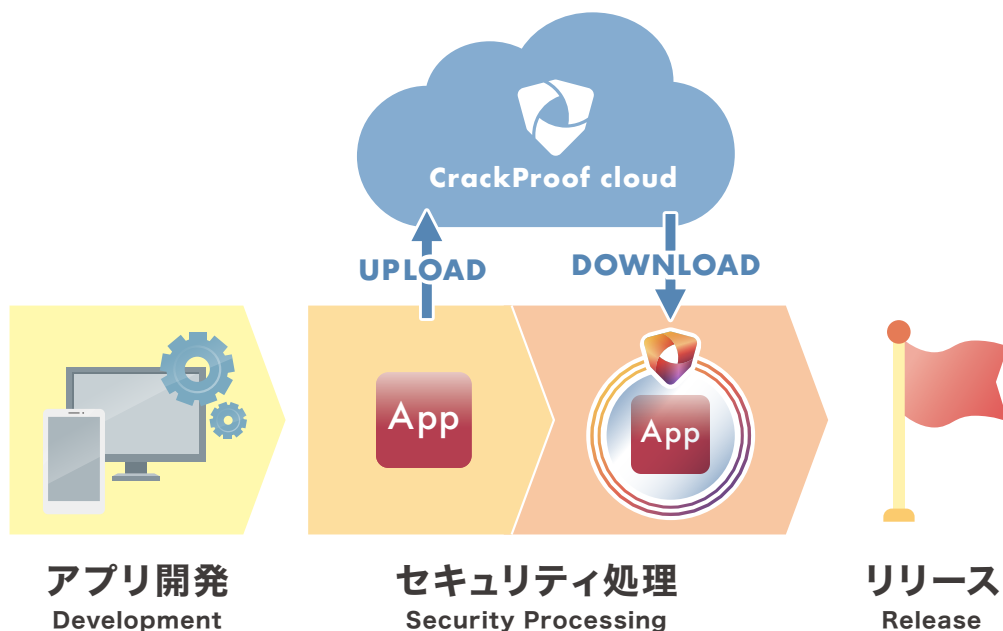
強力なセキュリティ(静的解析/動的解析対策)を 簡単操作で短時間かつ自動的に適用できます。

セキュリティ処理方法 4ステップの簡単操作で処理完了

アプリケーションをクラウドにUPするだけの抜群の使い勝手

操作はCrackProofクラウドに表示される画面にアプリをドラッグ&ドロップするだけです。
自動的にCrackProofクラウドにアップロードされたアプリは、クラウド上でセキュリティ処理され、
ダウンロードすれば動作確認後すぐにリリースできます。

- ・ 下記はCrackProofの基本的な操作イメージです。製品ごとに使用方法は異なります。
- ・ WebAPIご提供により、CIツールにも連携可能。 ※Android、Windowsのみ



CrackProofの特長 セキュリティ導入時にありがちな課題を解消

1/ セキュリティ処理が 簡単

プログラミングは不要※

アプリケーションのクラッキング対策をするためには、通常セキュリティの組み作業が必要ですが、CrackProofはビルド後の実行ファイル(バイナリ)に直接セキュリティ処理が可能です。

※ 製品によっては一部プログラミングが必要です。

2/ 静的解析・ 動的解析を阻止

さまざまな解析から
アプリを保護

ファイルレベルでの解析(静的解析)も、デバッガ等を使用したプログラム実行中の解析(動的解析)も共に阻止します。簡単な操作で高レベルの解析対策を実現します。

3/ パフォーマンス 低下ほぼ無し

低スペックな環境にも対応

CrackProofはアプリケーションのパフォーマンス(動作速度)にほとんど影響を与えないので、精密な動作が求められる組み込みアプリケーションにもご利用いただくことが可能です。

様々なプラットフォームに対応。
お客様のアプリケーションの実行環境に適した
CrackProofをお選びいただけます。

製品ラインナップ



CrackProof for Android dex 版

Kotlin / Javaで開発した
Androidアプリ(dex)向け



CrackProof for Android so 版

C / C++ / Unityソフトウェアの
C#(IL2CPP適用)で開発した
Androidアプリ(so)向け



CrackProof for iOS

iOSアプリを守るセキュリティライブラリ



CrackProof for Windows

Windows アプリケーション向け

※その他のOSについてはお問い合わせください



開発・販売 **株式会社DNPハイパーテック**

〒600-8813 京都市下京区中堂寺南町134番地
京都リサーチパーク（公財）京都高度技術研究所内

<https://www.hypertech.co.jp/>

TEL 075-322-1228

E-mail ht-sales@hypertech.co.jp



■IOSの商標は、Ciscoの米国およびその他の国のライセンスに基づき使用されています。 ■「Android」は、Google LLCの商標または登録商標です。 ■Linuxは、米国およびその他の国におけるLinus Torvalds氏の登録商標または商標です。 ■Microsoft、Windowsは米国Microsoft Corporationの米国およびその他の国における登録商標です。 ■Windowsの正式名称は、Microsoft Windows Operating Systemです。 ■ARMは、ARM Limited（またはその子会社）のEUまたはその他の国における登録商標です。 ■Intelは、アメリカ合衆国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。 ■これらの資料は、ユニティテクノロジーズまたはその関連会社がスポンサーとなったり、ユニティテクノロジーズまたはその関連会社と提携しているものではありません。[Unity]はユニティテクノロジーズまたはその米国や他の国々に所在する関連会社の登録商標または商標です。 ■各商標の記載時には®マーク、TMマークを省略している場合があります。