難読化でのアプリ保護をお考えの方に

セキュリティ対策ガイド

- アプリ保護について基礎知識を学びたい方
- 難読化の保護範囲（難読化で守れるもの・守れないもの）を知りたい方
- アプリへのセキュリティ対策をお考えの方

株式会社DNPハイパーテック

Copyright 2025 DNP HyperTech Co., Ltd.

難読化でのアプリ保護をお考えの方に
セキュリティ対策ガイド

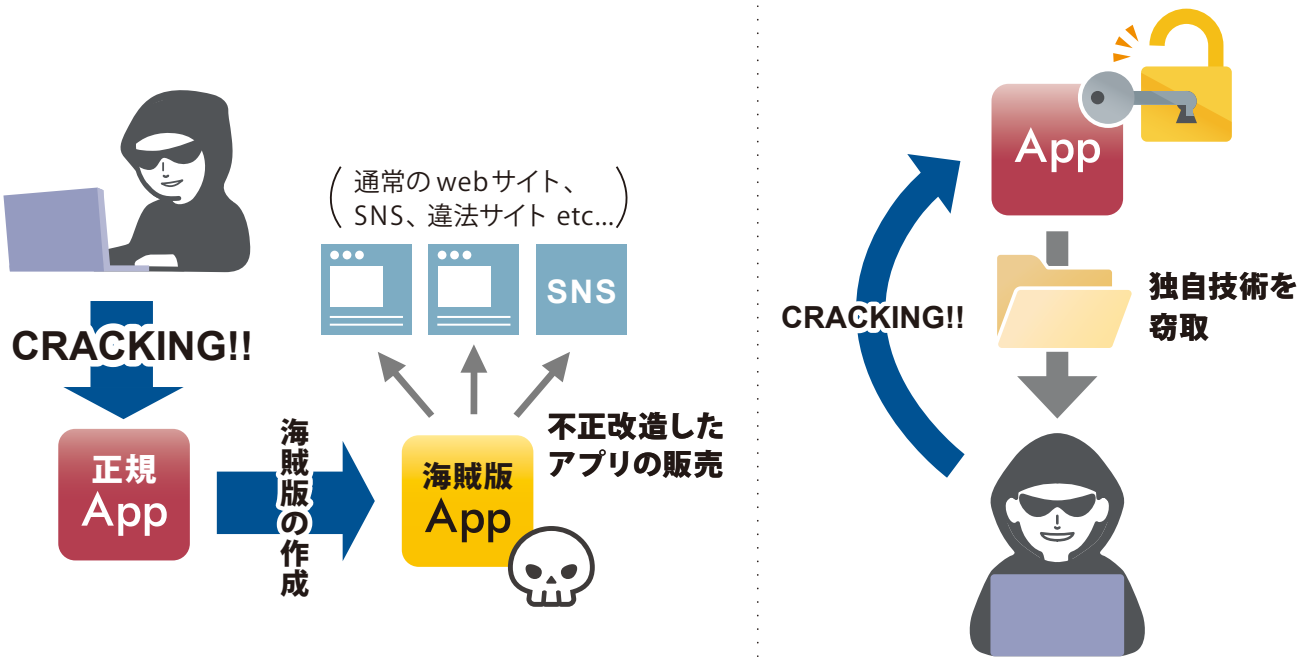
Copyright 2025 DNP HyperTech Co., Ltd.

1. アプリ保護手段としての難読化

セキュリティ対策をしないアプリ・ソフトウェアの危険性

近年では、事業サービスの一形態としてアプリの配信はスタンダードな手段となってきています。配信されるアプリには、攻撃者に狙われるポイントが多く含まれているため、アプリの開発･配信にはセキュリティ対策は重要な課題です。また、機器などに組み込まれているソフトウェアも同じように攻撃者に狙われる可能性があります。

攻撃者は、ソースコードを解析しアプリやソフトウェアの構造を把握することで、さまざまな不正行為を行います。たとえば、**不正コピーアプリを作成し売買されたり、製品に組み込まれたソフトウェア内の独自技術や機密情報を窃取し類似製品を販売される**おそれがあります。そのことにより、**本来得られるはずの収益が失われたり、製品の信頼性が下がってしまいます。**



企業に不利益をもたらす行為を受けるリスクが非常に高くなってしまうため、アプリ・ソフトウェア保護のためのセキュリティ対策は非常に重要です。

※以下、本文ではアプリ・ソフトウェアを総称して「アプリ」と表現します

Copyright 2025 DNP HyperTech Co., Ltd.

難読化とは？

それらの対策のうちの一つが**「難読化」**です。

「難読化」とは？

アプリの元となるソースコードを読みづらい形（人間には意味を理解できない文字列）にして、解析を困難にする技術です。攻撃者に解析コストを強いることによって、クラッキング（不正な解析・改ざん）を予防することができます。

実際に、アプリのセキュリティ対策として採用している企業も多いようです。しかし、**難読化だけでアプリのセキュリティ対策は十分だと言えるでしょうか？**　難読化はアプリ保護に一定の効果がありますが、あくまでソースコードを「読みづらくする技術」です。技術を持った人間が時間をかけて解析することで読み解かれてしまう可能性は否定できません。また、後述しますが、アプリの解析には様々な種類があり、難読化で全ての解析を防ぐことはできません。

結果として、**難読化「だけ」でアプリのセキュリティ対策が十分だと言えるものではありません。**

Copyright 2025 DNP HyperTech Co., Ltd.

難読化ツールの使用

アプリに難読化を施す場合、手作業で行うのは時間的コストと特殊な技術が必要となるので、あまり現実的ではありません。**難読化ツール**の使用が効率的です。

市販されている難読化ツールを使用するのが一般的ですが、欲しい機能を追加したい、機能を細かく調整したいなどの理由で自由度の高い難読化ツールを求める場合は、自作することも可能です。

弊社サイトに難読化ツールの自作方法について解説するコラムが掲載されていますので、ご参考いただけると幸いです。

DNP ハイパーテックサイト　開発者コラム
「Java ソースコード難読化ツール自作入門 – 第 1 回」

https://www.hypertech.co.jp/column/developer/2022/04/selfmade-obfuscation-tool-1/

Copyright 2025 DNP HyperTech Co., Ltd.

2. 難読化の保護範囲

アプリ保護のための対策ポイント

難読化がどのようにアプリを保護するのかを理解するため、ここでアプリを保護するために対策すべきポイントをご説明します。
アプリの対策ポイントには、大きく分けて三種類あります。

① 静的解析

② 動的解析

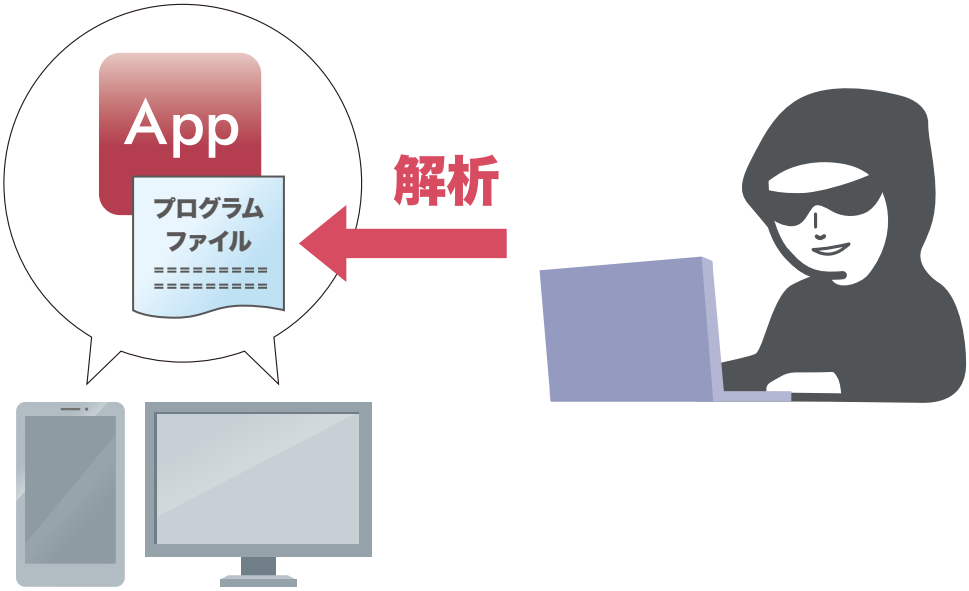
③ 不正環境での解析

それぞれの方法について説明していきます。

Copyright 2025 DNP HyperTech Co., Ltd.

①静的解析

アプリを動かさず、アプリそのものを対象にしてプログラムファイルを解析します。



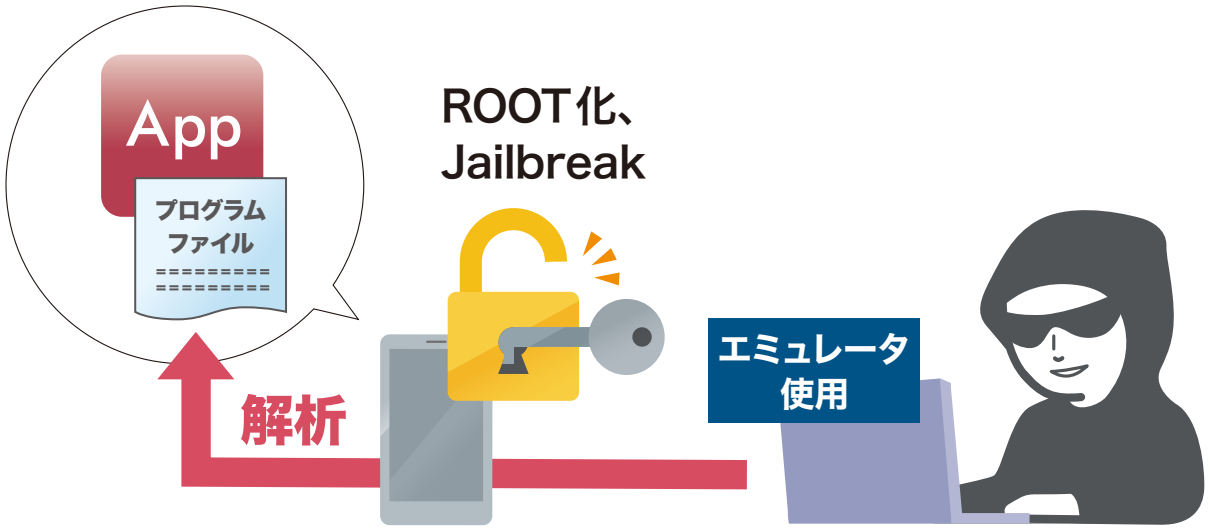
②動的解析

アプリを動かしながら、端末のメモリ情報などを解析します。

Copyright 2025 DNP HyperTech Co., Ltd.

③不正環境での解析

ROOT 化や Jailbreak などを行って通常は許可されない特権を取得したりエミュレータを使用するなど、攻撃者にとって有利な環境を用意した上で①、②のような解析を実行します。



難読化はアプリのプログラムファイルを読みづらくして解析を妨げるので、①の静的解析を防ぐための手段の一つとなります。

②の動的解析、③の不正環境での解析を防ぐ手段にはなりません。

これが、前章で「難読化だけでアプリのセキュリティ対策が十分だと言えるものではない」と述べた理由となります。アプリを強力に守るには、より多角的な保護が必要となるのです。

Copyright 2025 DNP HyperTech Co., Ltd.

アプリのクラッキング対策ツール「CrackProof」のご紹介

ここで、難読化で守り切れない部分も包括的に保護するセキュリティ対策として、「CrackProof」をご紹介させていただきます。

CrackProofの保護機能

① 静的解析対策

- 暗号化
- コード改ざん阻止
- コード難読化

② 動的解析対策

- デバッガ検出
- エミュレータ検出
- メモリアクセス阻止

③その他動作環境チェック等

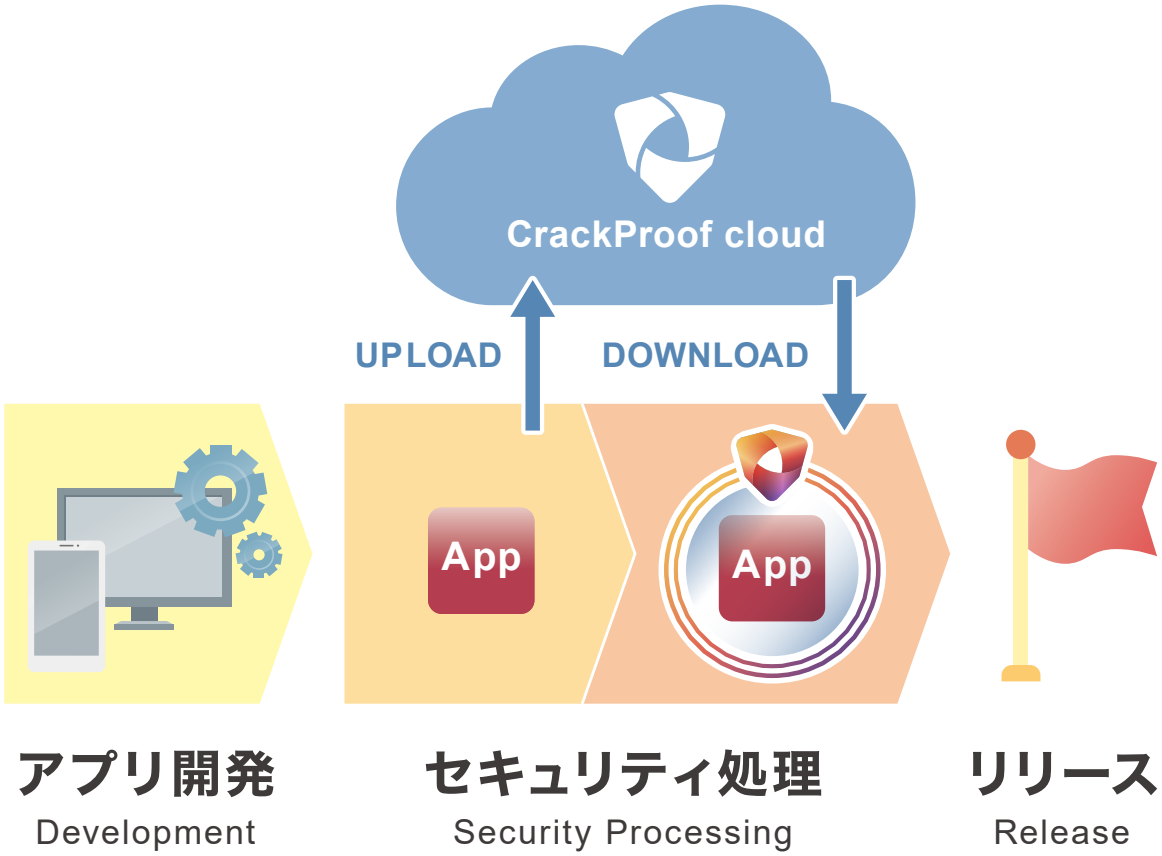
- ROOT化、Jailbreak環境での起動阻止
- 署名改ざん検知

※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。

CrackProofで堅牢化処理されたアプリは、静的・動的ともに悪質な解析を阻止し、不正な実行環境も検知します。難読化で保護しきれない部分に対しても、**CrackProofなら多角的な保護を施すことが可能です。**また、「可用性重視」や「セキュリティ強度重視」など、柔軟な機能セッティングも可能です。

Copyright 2025 DNP HyperTech Co., Ltd.

CrackProofの処理方法



・上記は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

アプリを直接セキュリティ処理するため、開発段階でソースコードに組み込む作業は不要です。（iOSのみ、仕様により一部開発段階での作業が必要となります）**CrackProofクラウド上にアプリをドラッグ＆ドロップするだけで、開発済みのアプリにも、自動的に強固なセキュリティ処理が施されます。**ダウンロードし、動作確認等を行った後、すぐにリリース可能です。

Copyright 2025 DNP HyperTech Co., Ltd.

Windowsソフトウェア向けのクラッキング対策ソフトとして開発されたCrackProofは、販売開始より約20年の実績がございます。現在ではAndroid/iOS/Windowsに対応を広げ、製造・エンタメ・ゲーム・銀行・電機・家電・情報通信・自動車等、様々な業界において、CrackProofの導入活用が進んでいます。

弊社DNPハイパーテックのホームページには、さらに詳しい製品紹介やセキュリティ知識が身につくダウンロード資料もございます。ご興味を持たれた方は、ぜひご覧ください。

DNPハイパーテックサイト TOPページ

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

また、弊社製品CrackProofや不正な攻撃への対策、その他アプリのセキュリティ対策について詳しく話を聞いてみたいと思われた方は、ぜひお気軽にお問い合わせください。

お問い合わせページ

https://www.hypertech.co.jp/contact/

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 ASTEM棟 5F
TEL：075-322-1228 / E-Mail：ht-sales@hypertech.co.jp
URL：https://www.hypertech.co.jp/

未来のあたりまえをつくる。
DNP

Copyright 2025 DNP HyperTech Co., Ltd.