アプリに必要な対策がわかる！

押さえておきたい
製造業のセキュリティ知識解説

今の
セキュリティ対策で
大丈夫？

アプリ配信前に
しておくべき
対策とは？

アプリは
どんな方法で
攻撃される？

株式会社DNPハイパーテック

Copyright 2023 DNP Hypertech Co.,Ltd.

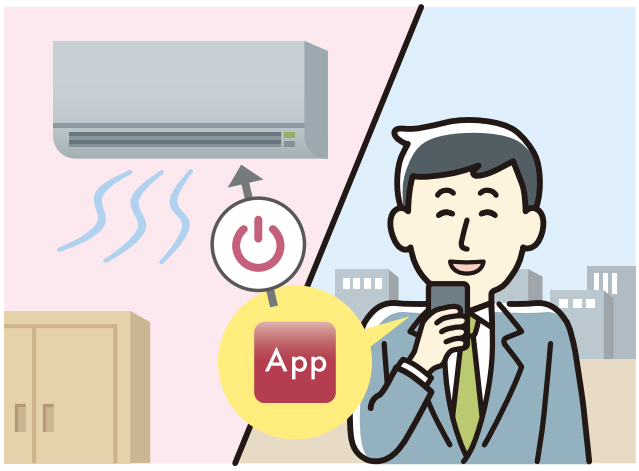
アプリに必要な対策がわかる！
押さえておきたい製造業のセキュリティ知識解説

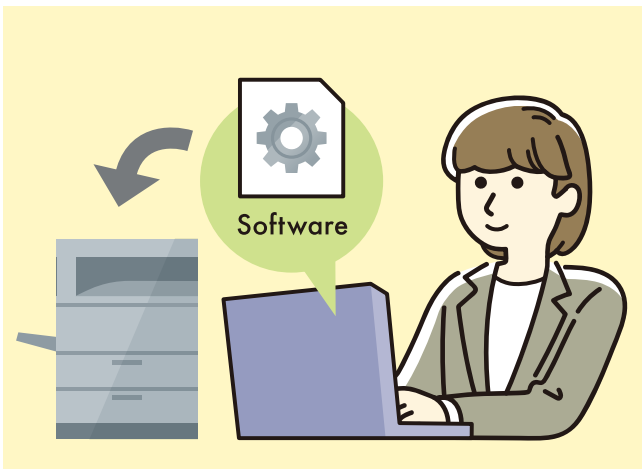
Copyright 2023 DNP Hypertech Co.,Ltd.

1. 製造業アプリのセキュリティの現状
～クラッキング被害とその背景～

製造業において、スマホアプリや PC ソフトを
事業に活用する手法が一般的になっているようです。
自社の製品とアプリを連携して
アプリから機器の操作を可能にしたり、
web サイトで提供していた自社サービスを
アプリで提供するなどのケースが最近では多くなっています。

また、製品ユーザーのためのユーティリティツールとして
ソフトを提供されている企業様や、
CAD/CAM/CAE など、独自技術をもって開発したソフトを
販売している企業様も多く見られます。





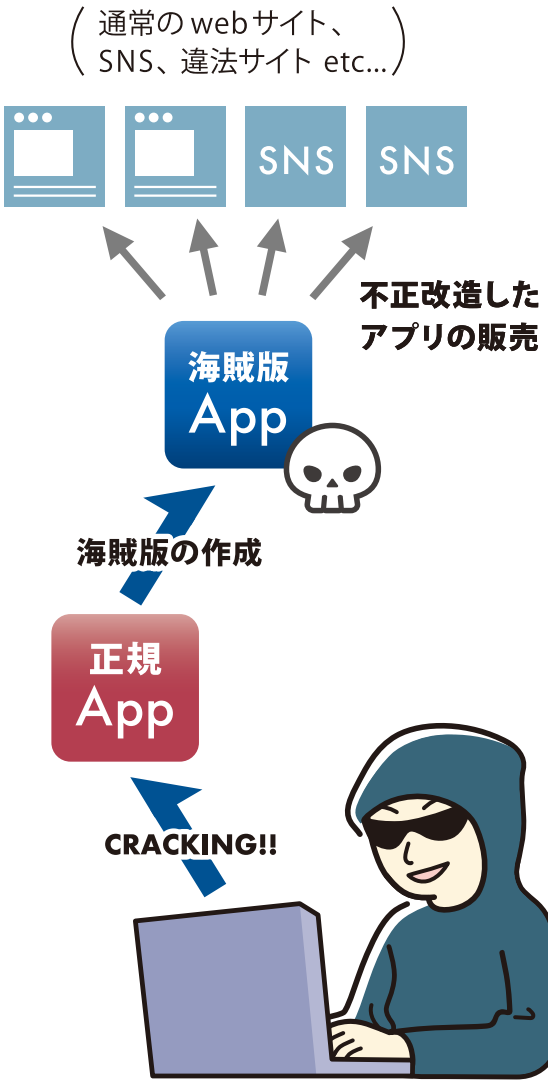
しかし、そのようなアプリ・ソフトが
クラッキング（不正な解析・改ざん）の対象となることは
ご存知でしょうか？

Copyright 2023 DNP Hypertech Co.,Ltd.

アプリへのクラッキング行為の例

主なクラッキング行為の例としては、以下のようなものが上げられます。

アプリが解析され、配信企業が
意図していない機能に改変された
海賊版アプリが不正に販売される。



アプリ内に埋め込まれている
アルゴリズムが解析され、
独自技術を窃取される。

このような事態が起きると、アプリ配信をしている
企業の技術ノウハウが流出してしまうだけでなく、想定しない事故にも繋がり
収益へ悪影響や信頼喪失となるおそれもあります。

Copyright 2023 DNP Hypertech Co.,Ltd.

アプリへのクラッキング行為の例

アプリのセキュリティ対策として、不正使用を防ぐドングルやライセンス認証などの方法を採用されている企業様も多いようです。

しかし、それらの対策を行っていても、**アプリ側をクラッキングすることによりその仕組みを解除される**というケースが考えられます。例えば下の図解のように、端末にインストールしたアプリに保護対策がなされていないと、攻撃者によりアプリの解析が行われてしまいます。そこでドングルやライセンス認証を解除するための情報入手が可能になってしまうのです。

既に対策をしていても、**アプリ自体へのクラッキング対策も行っていなければ、十分なセキュリティ保護体制を実現できず被害にあう可能性が残ってしまう**ということになります。

ドングル使用、ライセンス認証で対策されているが
アプリ自体には対策していない場合・・・

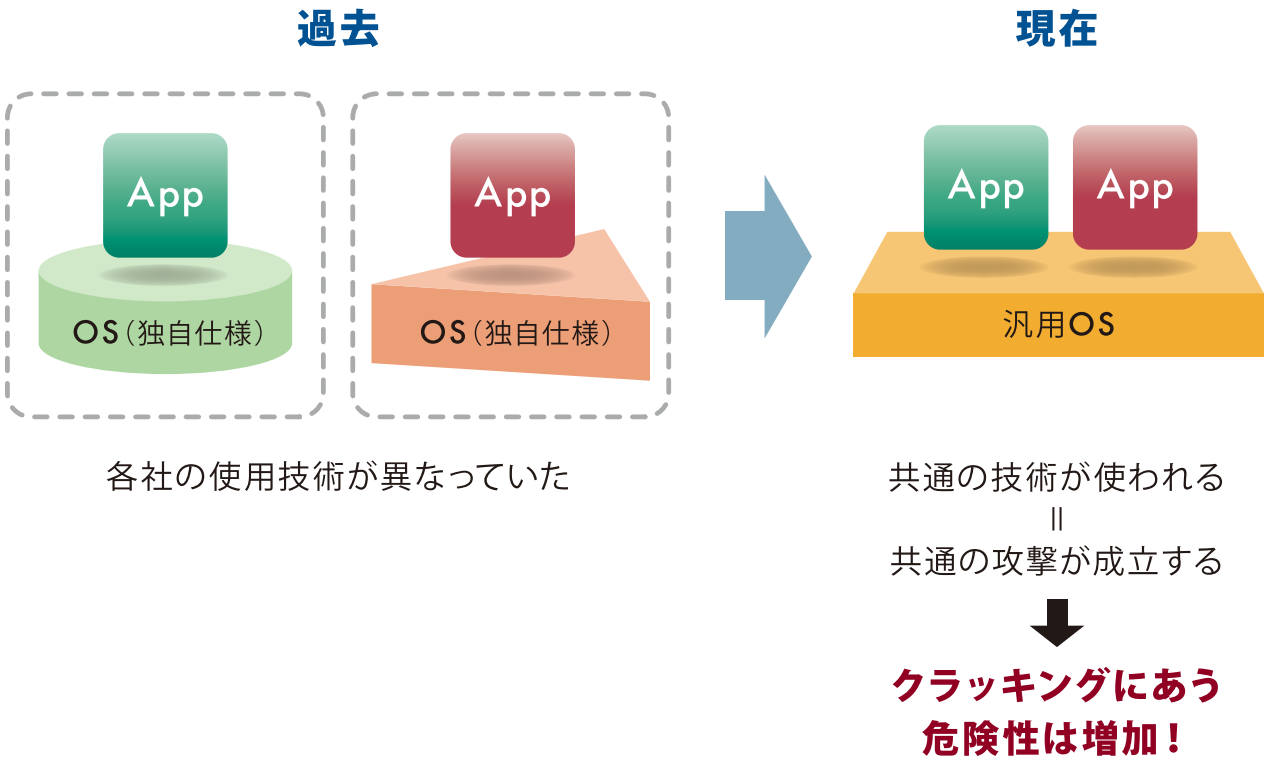
Copyright 2023 DNP Hypertech Co.,Ltd.

クラッキング被害がなくならない背景

従来、製造業を含むさまざまな分野では、専用端末と専用OSが使用されてきました。ハード、ソフト共に企業が独自仕様のものを使うため、それらのクラッキングには専門的で高度な知識が必要でした。

しかし、近年ではAndroidなどの汎用OSが使われることも増えてきました。自社開発に比べて開発スピードが上がるため、この流れはとどまることはないと考えられます。そして、そのことにより、汎用OSを対象とした攻撃が成立し、クラッキング難易度が下がる結果となりました。また、そういった知識やその成果物として開発された道具を広めることをインターネットの普及が後押しし、多くの人がそれらを共有できるようになりました。

それらの要因により、クラッキングの被害がなくならないような状況が常態化しているのです。

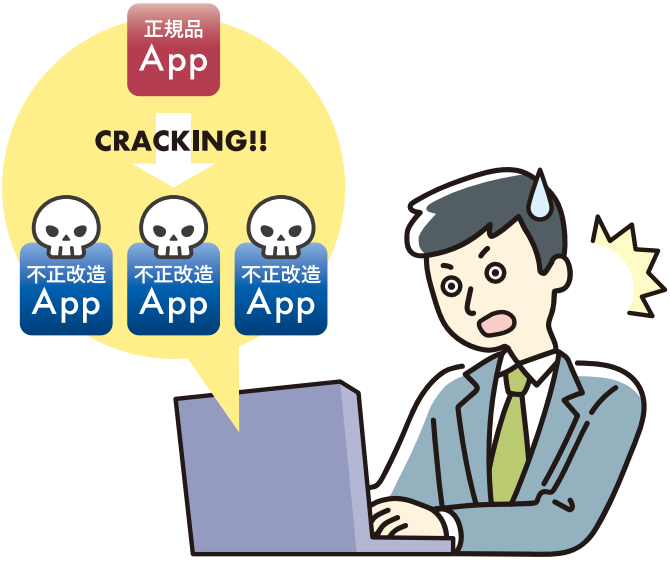


Copyright 2023 DNP Hypertech Co.,Ltd.

2. 製造業アプリの被害事例

ある CADメーカー様の場合

自社のCAD製品の
海賊版が販売されていることが
判明した。



自社製品がクラッキングされ
ライセンス認証の仕組みが解除、
不正コピーされたものが、
無断で販売されていることがわかった。
本来あったはずの収益を失うだけでなく
企業としての信用が失墜することを
防ぐため、クラッキング対策をすることに。

社内にはセキュリティ担当部署はなく、
クラッキング対策は開発部署が
兼任で担当することに・・
本来の業務のクオリティは
下げられないため、
クラッキング対策に
割けるコストには限界がある。

Copyright 2023 DNP Hypertech Co.,Ltd.

3. アプリのセキュリティ対策

セキュリティ専門企業に対策を任せるメリット

ここまでで、アプリ自体にセキュリティ対策を施す必要があるということがおわかりいただけたかと思います。

セキュリティ診断などは既に外部専門企業に依頼するのが常識になっているようですが、クラッキング対策については、まだそのような意識が浸透しておらず、自社対応を検討される企業様もいらっしゃるかと思います。

しかし、**アプリへの攻撃は日々多様化・高度化しており、そこに対応するための日々の調査・対策技術の開発に多くの時間を消費することになります。**また、**セキュリティ知識を持ち、対策を実装できる人材を育成・雇用するためのコストも必要になってきます。**自社対応を採用される場合は、それらの負担を継続して維持できるかどうかを事前によく検討することが重要です。

そこでおすすめするのが、アプリ保護の技術を持つセキュリティ専門企業に対策を依頼する方法です。専門企業に対策を依頼するメリットとして、以下が上げられます。

■ 最新のセキュリティ対策技術を適切に適用できる

セキュリティ対策とは、何かトラブルが起きた際に対応するだけのものではありません。日頃から市場の様々な攻撃手法を常にリサーチし、対策技術を迅速に開発する体制が必要になります。専門企業に依頼することで、そのような体制の構築をまるごと任せることができます。

■ セキュリティ専門エンジニアが不要になり、自社のアプリ・ソフト開発業務に集中できる

専門エンジニアの育成にかかるコストを負担することなく、アプリ保護対策に関するノウハウが無くても技術サポートを通じて、安全、安心なアプリ開発を行うことができます。

Copyright 2023 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、アプリのセキュリティ対策に最適なソリューションとして、**「CrackProof」**をご紹介させていただきます。

CrackProofの保護機能

静的解析対策

- 暗号化
- コード改ざん阻止
- コード難読化

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

その他動作環境チェック等

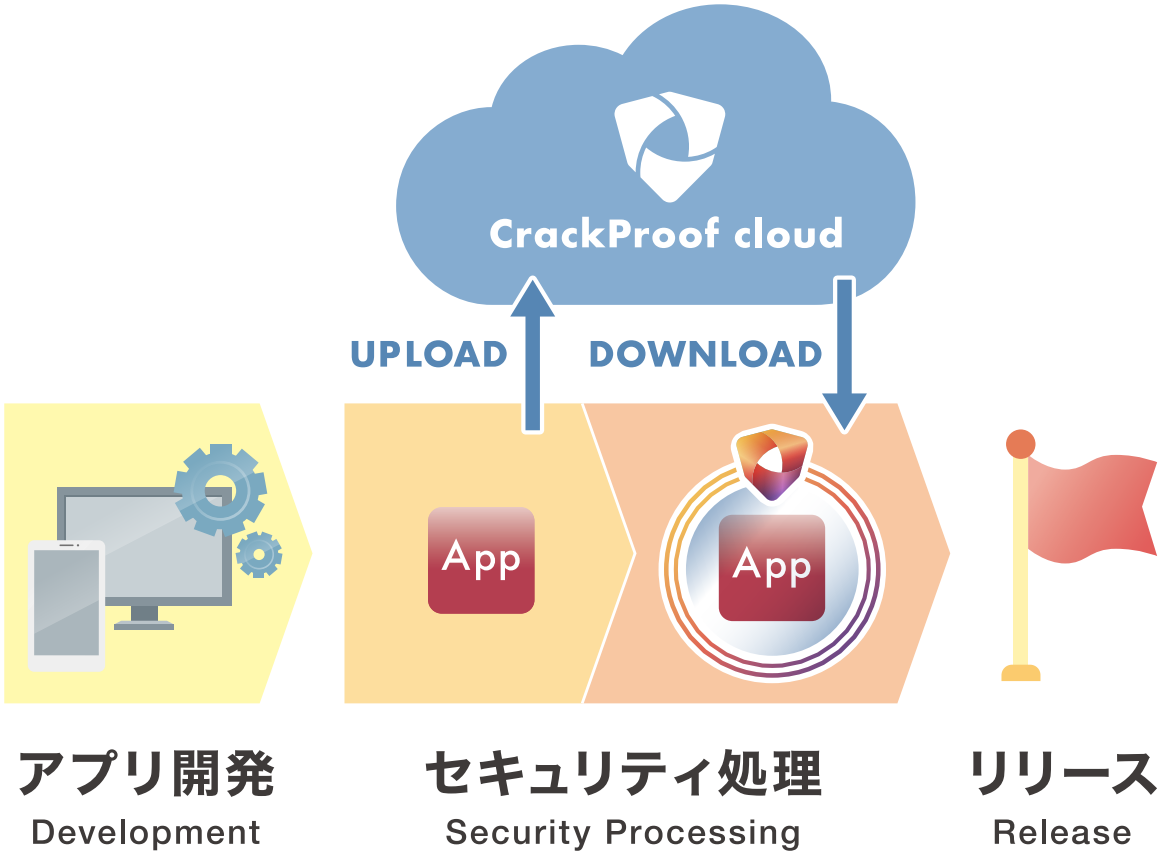
- ROOT化、Jailbreak環境での起動阻止
- 署名改ざん検知

クラッキング（不正な解析・改ざん行為）を防ぐためには、アプリ自体を直接解析する「静的解析」と、アプリ実行中の動作情報を解析する「動的解析」の両方を防御することが重要です。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、デバッガやエミュレータなど不正な実行環境も検知します。

アプリのセキュリティ対策として難読化を採用される企業様もいらっしゃいますが、こういった**多角的な保護を施すことが対策としては必要と言えます。**

Copyright 2023 DNP Hypertech Co.,Ltd.

CrackProofの処理方法



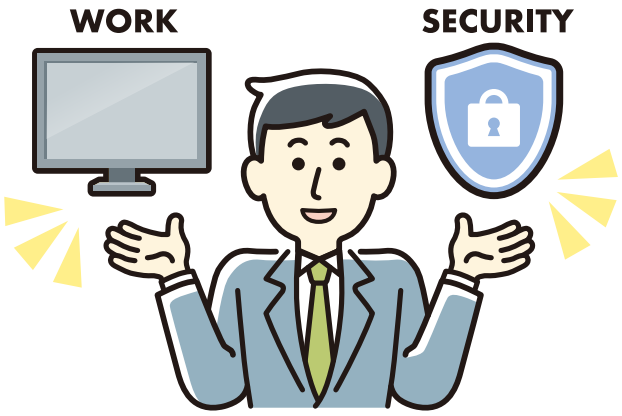
・上記はCrackProofの基本的な操作イメージです。製品ごとに使用方法は異なります。
・WebAPIご提供により、CIツールにも連携可能。 ※Android、Windowsのみ

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。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・動作確認後、すぐにリリース可能です。

Copyright 2023 DNP Hypertech Co.,Ltd.

「2. 製造業アプリの被害事例」で
ご紹介した CAD メーカー様は、
CrackProof を採用することで
クラッキング対策を達成されました。

CrackProof 導入について
懸念点として上がっていたのは
CAD ソフトのパフォーマンスが
低下してしまわないかという点でした。
しかし、実際に導入してみたところ
心配していたパフォーマンスの低下は
ほぼ見られませんでした。
（CrackProof 購入前には
トライアル期間も設けられているため、
導入前の疑問・不安などを
事前に確認することができます）



CrackProof 導入後は
被害の報告を受けることはなくなり、
本来の業務に負担をかけることなく
クラッキング対策を実現できています。

Copyright 2023 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 2023 DNP Hypertech Co.,Ltd.