製品開発・生産過程のセキュリティ対策はなぜ重要？独自技術・機密情報を守るためのアプリケーション・ソフトウェア保護とは

製造業の情報漏洩対策というと、データの持ち出しが可能な USB 機器などの管理や従業員へのリテラシー教育などが検討されることが多い。しかし、その他にも防いでおかないといけない危険性が普段の業務の中に隠れていることはあまり周知されていない。今回は、製品開発・生産に関わる独自技術・機密情報がソフトから盗まれる危険性について説明する。

株式会社DNPハイパーテック

製品開発・生産過程に潜む
独自技術・機密情報流出の危険性とは

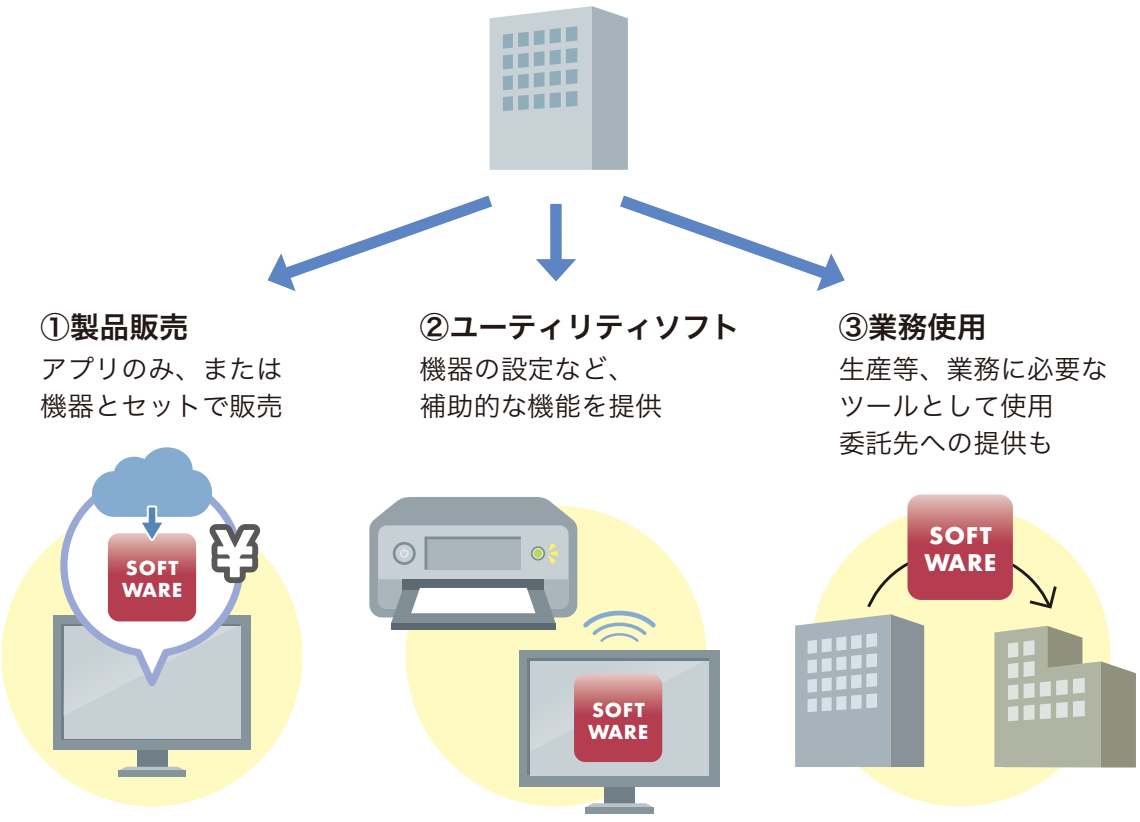
企業の保持する技術情報が入ったソフトが社外に出るパターンはさまざまで、事業の一環としてアプリの開発・販売を行っている場合や、業務で使用する内製ソフトを合弁会社や委託先などに渡す場合などがある。（図１）　どのパターンであっても、ソフトを不正に解析・改ざんする行為「クラッキング」の被害に遭う危険があるが、今回は後者の、業務で使用する内製ソフトがクラッキングされ、独自技術・機密情報が流出する危険性について解説する。

製品開発・生産の過程で社内で独自開発したソフトを使用することは珍しくないが、その内製ソフトが独自技術情報の窃取を目的としたクラッキング被害に遭う危険性があることはあまり認識されていない。

例えば、あるメーカーが海外の合弁会社と共同で製品開発のプロジェクトを進める際に、業務上必要となる社外秘の技術情報が含まれた内製ソフトを提供する必要があるとする。しかし、もしその合弁会社の製品開発の関係者に悪意を持った人物が紛れ込んでいた場合、内製ソフトがクラッキングされ、独自技術情報を盗まれる危険がある。（図2）

製品開発・生産に関わる業務ならば、合弁会社に対し情報流出を防ぐための最低限のルールが取り決められており、当該プロジェクト以外への情報使用を禁止する契約が結ばれていることが一般的である。**しかし、実際に上記のような事態が発生した場合、**

図１　企業の技術情報が入ったアプリケーションやソフトウェアが社外へ出るパターン



窃取された独自技術・機密情報が拡散されたり、契約外で技術を不正使用されるなど、被害が発覚した際にはもう事態を収拾する手立てがないという状況に陥ることも考えられる。もちろん、合弁会社に限らず、製品開発・生産に関わる業務をOEMなどで社外に委託する場合も同様である。また、社外とのやり取りがなくとも、悪意を持った人物が内部に紛れ込む可能性がある以上、企業内使用に限定していても、全くの安全とは言えないのが現状だ。

このように、ごく一般的な製品開発・生産の過程の中にも、技術情報流出の危険性は潜んでいるのである。

クラッキングを阻止する上で注目すべき要素は大きく３つ

では、そういったソフトへのクラッキングは具体的にどのように行われるのか。手口はさまざまだが、防ぐべきポイントは大きく分けて**「動的解析」と「静的解析」「不正環境での実行」**の３つである。

①静的解析

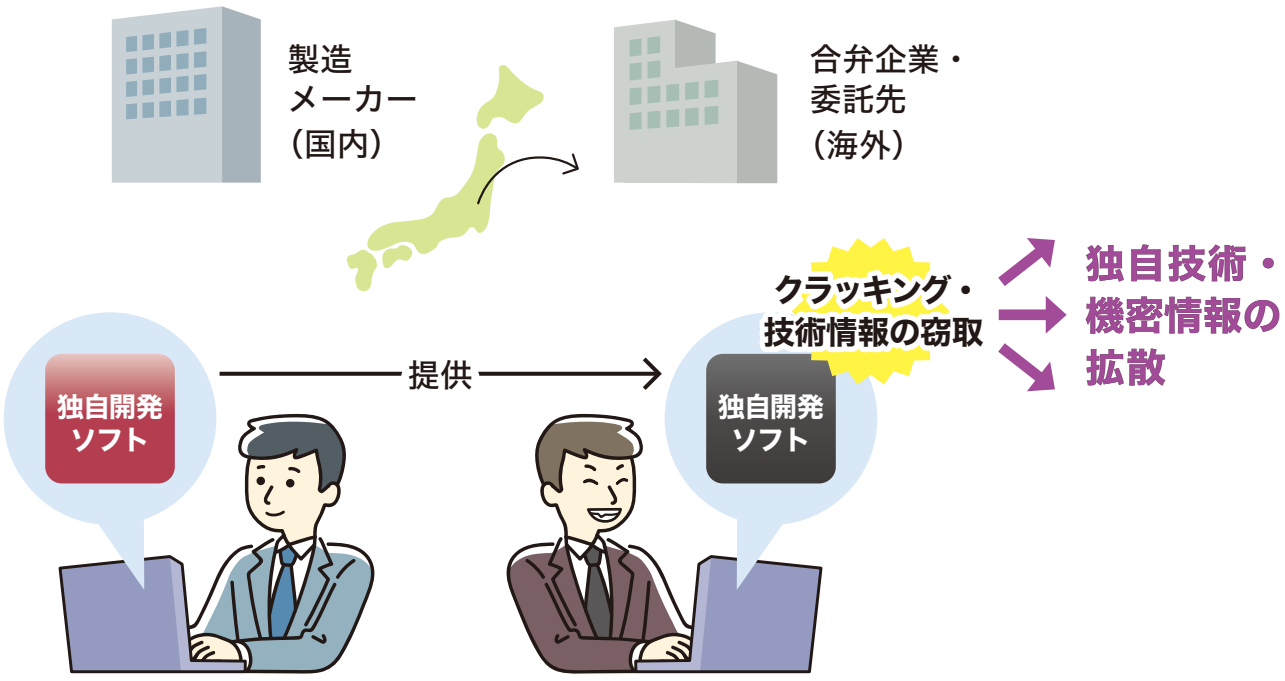
ソフトを実行せずに解析、プログラムファイルに記述された内容を読み取る。

②動的解析

ソフトを実行しながら解析、プログラムファイルそのものではなく、デバッガ（※）等を使用してソフトを実行している端末のメモリ情報等を読み取る。

※本来は、ソフトを動かしながらバグ（欠陥）を見つけて修正する作業に使用するツール

図２　合弁企業・委託先でのクラッキング被害イメージ



③不正環境での実行

上記のような解析を実行するため、エミュレーターなどを使用して攻撃者にとって有利な環境が使用される場合がある。

クラッキング対策としては、この３つのポイントに注意する必要がある。

ソフトへのクラッキングを防ぐには？

独自技術や機密情報が含まれているソフトを守るためには、事前にクラッキング対策を行っておく必要がある。セキュリティに関する専門知識を持った人材を雇い、自社内で対策するという方法も考えられるが、日々多様化・高度化する攻撃手法に対抗しうるスキルを持った人材を確保し、その技術を維持するのは簡単ではない。クラッキング対策の内製化には多大な時間的・金銭的コストが持続的に必要になる。

そのため、ここではセキュリティ対策技術を持つ専門会社が開発するツールを使用し、セキュリティに関するノウハウがなくても簡単にソフトを保護する方法を紹介する。**DNP ハイパーテックのクラッキング対策ツール「CrackProof」は、先に挙げた静的解析と動的解析を阻止し、さらにクラッキングをする際に使用される不正環境を検知することが可能だ。**

図３ CrackProof の保護イメージ

ソフトへの攻撃を阻止する クラッキング対策ツール 「CrackProof」の特長

CrackProofの主な特長を以下にまとめる。(図3)

1. クラッキングを多角的に防御

静的解析と動的解析、双方のクラッキング手法に対応。ソフトを何重にも暗号化し、攻撃者の解析ツールを無効化することで、不正な解析・読み取り・改変を多角的に防御する。

2. 開発済のソフトに簡単に適用可能

開発済のソフトに適用しセキュリティ機能を追加するため、開発段階でソースコードへの組み込み作業は不要。専用のクラウドにドラッグ＆ドロップするだけの簡単操作でセキュリティ処理ができるため、専門的な知識・技術がなくとも、ソフトへの適用が可能。

※OSにより一部例外あり。

3. 導入後も安心のフォローで お客様とともに対策を

導入後のサポートも充実。開発・サポート部署が国内で完結しているため、トラブル時のご相談に迅速な対応が可能。保護の対象となるソフトごとに異なる開発志向や配信方針に沿った対策のご提案をすることで、より強固なアプリ運用を実現できる。

おわりに

製品開発・生産に用いられる知識や情報は、これまでの研究開発に費やした時間やノウハウの積み重ねであり、企業の貴重な財産である。それらを盗まれ、悪意を持って流用されることで企業が被る損失はあまりに大きい。被害を未然に防ぐためにも、セキュリティ専門企業に相談し、自社のソフトに適した形で対策を施すことが重要である。

問合せ先 **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

DNPハイパーテック webサイト
https://www.hypertech.co.jp/

CrackProofの詳しい製品紹介や
セキュリティ知識が身につく
ダウンロード資料やコラムを
掲載しています

未来のあたりまえをつくる。
DNP