簡単DRM「プロテクトマネージャ」
プラットホーム

開発元 有限会社電机本舗

Java, VBSのファイルのDRMを実現

■フォルダ単位でDRMを実現

従来のDRMと異なり、フォルダ単位の保護を提供。

Javaなどのインタプリタ系の製品にDRMを提供します。

DRMの制御プログラムはOSにビルトインします。

フォルダは暗号化により保護します。

保護フォルダ
※フォルダ単位でDRMをかける

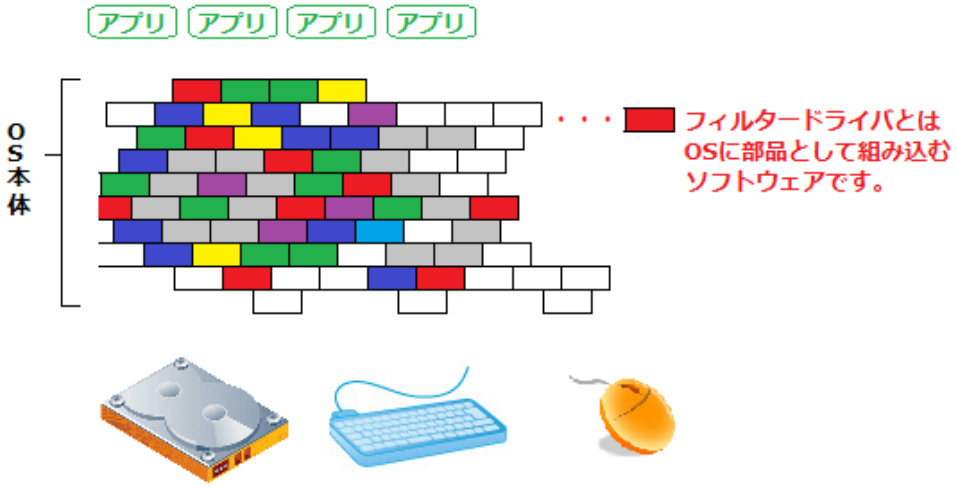
Java

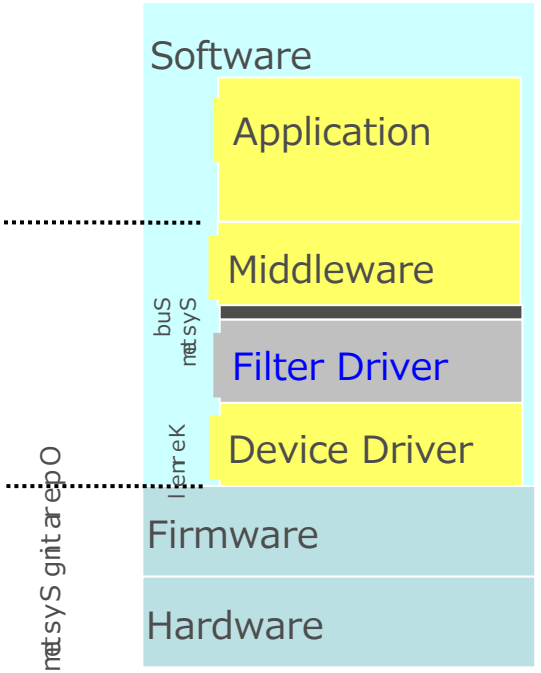
Microsoft .net

Sample.exe

電机本舗

フィルタードライバ概要





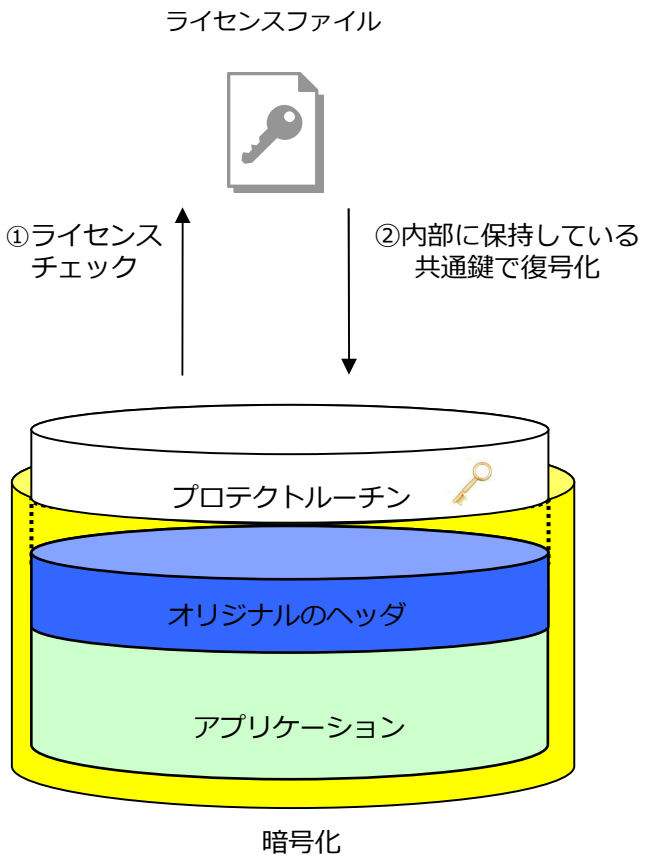
フィルタードライバは、OperatingSystemのコアに部品として組み込むプログラムと
思ってください。従い、オペレーティングシステムに柔軟に機能の拡張し追加します。

フィルタードライバは高度な技術を必要とするアンチ ウイルス製品の中核を構成す
るコアテクノロジーです。

従来ユーザ処理制約多くの製品が細かい拡張追加に不向きで実装困難があります。
■従来のシステムフックの問題点
フックと呼ぶ機能拡張性が高いがために機能しない。
・OSの深い機能を利用できない。

➡ フィルタードライバはこれらの制約を受けません。
オペレーティングシステムの深層部で、オペレーティングシステムの一部として動作します。このコアテクノロジーにより認証ロジックと暗号化を実装し、ファイル形式やアプリケーションに依存しないアクセス制御DRM（Digital Rights Management デジタル著作権管理）を実現しました。それが**簡単DRM**です。

既存のDRM製品の課題



既存のDRM製品は保護対象ファイルに直接プロテクトルーチン（プログラムのこと）コードを追加する方式です。

プロテクトルーチンを最初に実行し、ライセンスチェックを行います。

オリジナルファイルをプロテクトルーチンであたかもラッピング（包み込む）するため、以下の問題点があります。

■脆弱性

復号化するための共通鍵は、プロテクトルーチン内部で保持あるいは管理します。つまりここにライセンスチェック、製品情報、マシン情報の照合、正規ユーザへの復号処理が集約しています。

従い、クラッカーには、プロテクトルーチンの正規ユーザの判定判断する箇所を解析し書き換えるだけでプロテクトを解除できます。
ドングルなどの物理的なハードウェアキーの接続チェックも同様で、攻撃対象は接続チェックの判定部分になります。

■豊富なクラックツール

作成の簡単なアプリケーションレベルで制御しているため、OllyDbgなどフリーで流通している
ソフトウェアICEで容易に解析できます。

■急速に普及しているJavaに代表されるインタプリタ使えない問題

最近普及しているJava/.NETアプリケーションに代表されるインタプリタ系プログラムでは動作しません。
インタプリタ系プログラムはソースコード（テキストファイル）あるいは中間コードと呼ぶ形式を取ります。これは直接実行できるコードではないので、通常はラッピングの結果、動かなくなります。

フィルタードライバを利用したDRMシステム

フィルタードライバベースの新たな手法により既存のDRM製品の様々な課題をクリアしました。

■SRG方式の高速無限乱数式(ワンタイムパッド）&AES暗号化エンジンの実装

理論上解読不可能と言われる、無限欄数式暗号を標準採用しました。DRMの保護対象はそれ
ぞれ異なる乱数で暗号化します。もちろんAES暗号も実装、二重に暗号化します。

■強固な認証ロジック

保護対象のデータにはチェックルーチンを付加していないため、条件分岐は存在しません。
ライセンスコード内に定義されている共通鍵は、固有のハードウェア情報を基に暗号化されており
その都度、ハードウェア情報をフィルタードライバ側で取得し、算出した鍵情報で保護したデータを
復号化します。
認証済みのハードウェア上で実行されているか否かは、毎回正しく鍵が算出されているかで判断
しています。ライセンスチェック通過後も、「共通鍵を算出して復号化する」処理が残るため
保護ファイルに条件分岐が存在せず、攻撃対象になりえない点が大きな特徴です。

■耐タンパ性

ハードウェア構成が一致して初めて正しい鍵を生成します。従いハードウェア構成が一致していな
い環境では鍵の生成は失敗します。従い、DRMの保護ファイルは復号化できません。
加えて、これらの処理はドライバレベルで行っているため、一般的なデバッガでは解析できません。
ドライバ間で行われている処理を解析する環境を起こした上で**簡単DRM**をマウント
する必要があるため、クラッキングに対するハードルが高くなります。
メモリ上に展開した認証済みのプロセスはAPIフックによって２次ブロックを行い各モジュール間での
改ざんチェック、難読化などあらゆる対策が施しています。

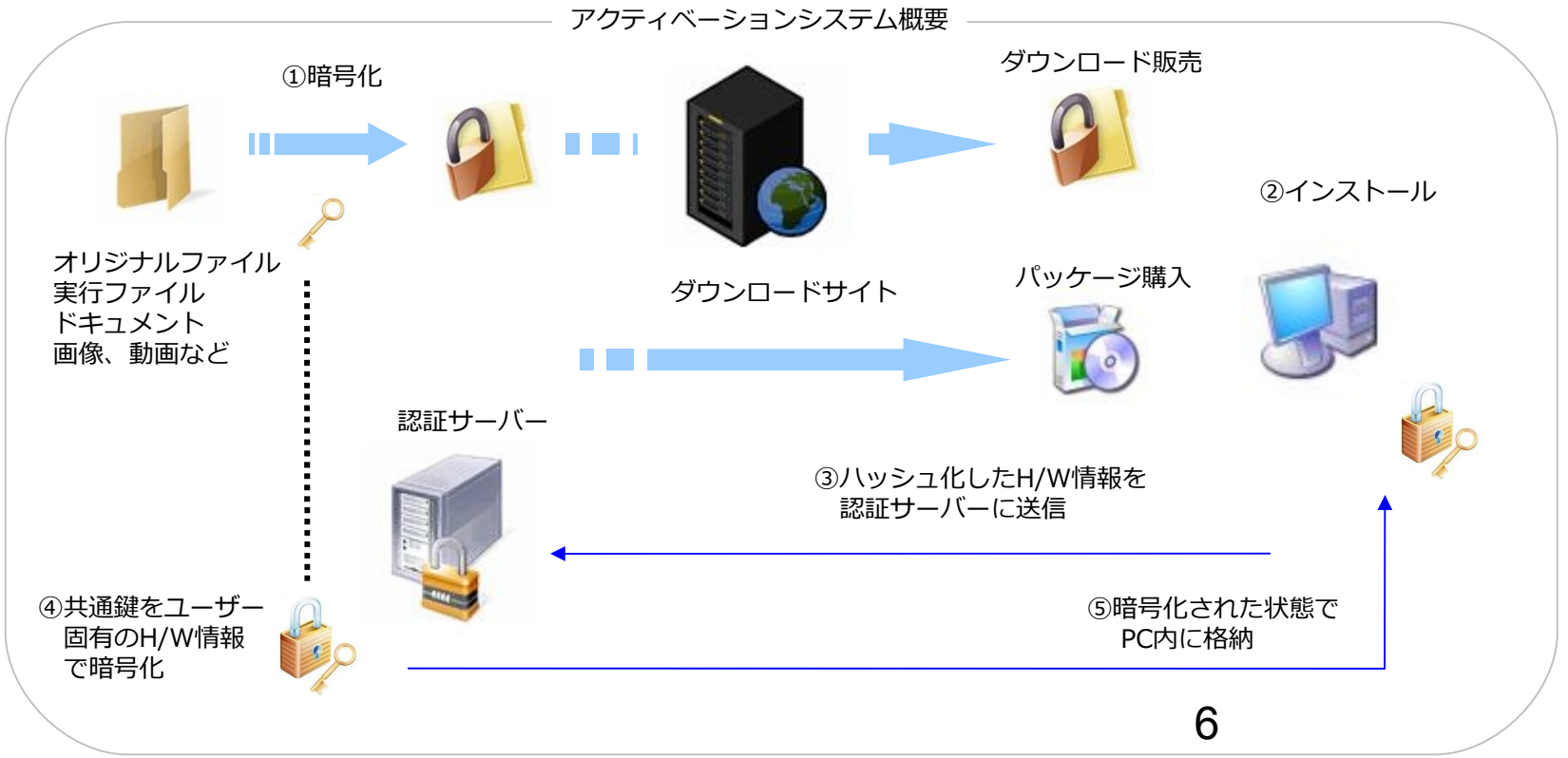
■安定性

既存のDRM製品でもメモリ上に展開された後も暗号化された状態を維持し、ロードされた
タイミングで都度復号化する機能はありますが、ソースコード内にマーキングする必要があり
モジュール全てを暗号化する事ができないなど制約も多いのが現状です。
簡単DRMは保護領域全体をオリジナルの状態を崩すことなく復元した上で
プロセスをブロックしておりますので、暗号化前と暗号化後で挙動の違いはありません。

オンラインアクティベーションシステム

簡単DRMのSDK（開発キット）にはオンラインライセンス認証を行うサーバーモジュール、クライアント、サーバー側の各種ツール類が収録されており、ライセンスの管理はもとより、販売・開発・サポートなど様々なビジネスシーンで活用できる情報の蓄積、分析が可能です。

■認証サーバーへ自動的に利用ログを送信。クライアントの利用状況、環境、バージョン、ホットフィックス適用状況などを把握する事でサポート面の負荷軽減。
■利用環境のパフォーマンス、利用頻度の高い機能や時間帯などを把握してライセンス数、システム構成など、マーケティング販売促進に活用。
■利用時間による従量課金やサブスクリプションサービスの提供。



フィルタードライバを利用したDRMシステム（応用）

実行形式以外にも、ドキュメントファイル、画像、映像、音声データなどあらゆるファイル形式を保護できます。

■専用プレーヤー（ビューア）に依存しない制御

暗号化する際に再生を許可するプレーヤー、ビューアを事前登録する事で、ソフトウェア
ベンダー、コンテンツホルダー側で再生を許可するアプリケーションを選択できます。
暗号化されたコンテンツ専用のプレーヤー、ビューアのインストールは不要です。

■保護領域外への持ち出し禁止

プロセスブロックの設定次第で、特定のデバイス、サーバー上でのみデータにアクセス
許可をきめ細かく制御できます。
保護領域外への持ち出し禁止による情報漏えいを防止し、認証済みのクライアント
（ライセンスを取得したPC）でのみデータへのアクセス、コンテンツの再生を許可します。



フィルタードライバを利用したDRMシステム（応用）USBメモリ

実行形式以外にも、ドキュメントファイル、画像、映像、音声データなどあらゆるファイル形式を保護出来ます。

■専用プレーヤー（ビューア）に依存しない制御

暗号化する際に再生を許可するプレーヤー、ビューアを事前登録する事で、ソフトウェア
ベンダー、コンテンツホルダー側で再生を許可するアプリケーションを選択できます。
暗号化されたコンテンツ専用のプレーヤー、ビューアのインストールは不要です。

■保護領域外への持ち出し禁止

プロセスブロックの設定次第で、特定のデバイス、サーバー上でのみデータにアクセス
可能にする制御が可能です。
保護領域外への持ち出し禁止による情報漏えいを防止し、認証済みのクライアント
（ライセンスを取得したPC）でのみデータへのアクセス、コンテンツの再生を許可します。

ロードマップ

Mac OS向け、組込み機器向け（スマートフォン、カーナビ、ゲーム機など）フィルタードライバを予定。
プラットフォーム、データ形式やアプリケーションに依存しないコンテンツ保護が可能になります。