Defense Platform

割込み型迎撃方式（Intercept）ディフェンスプラットフォームのご紹介

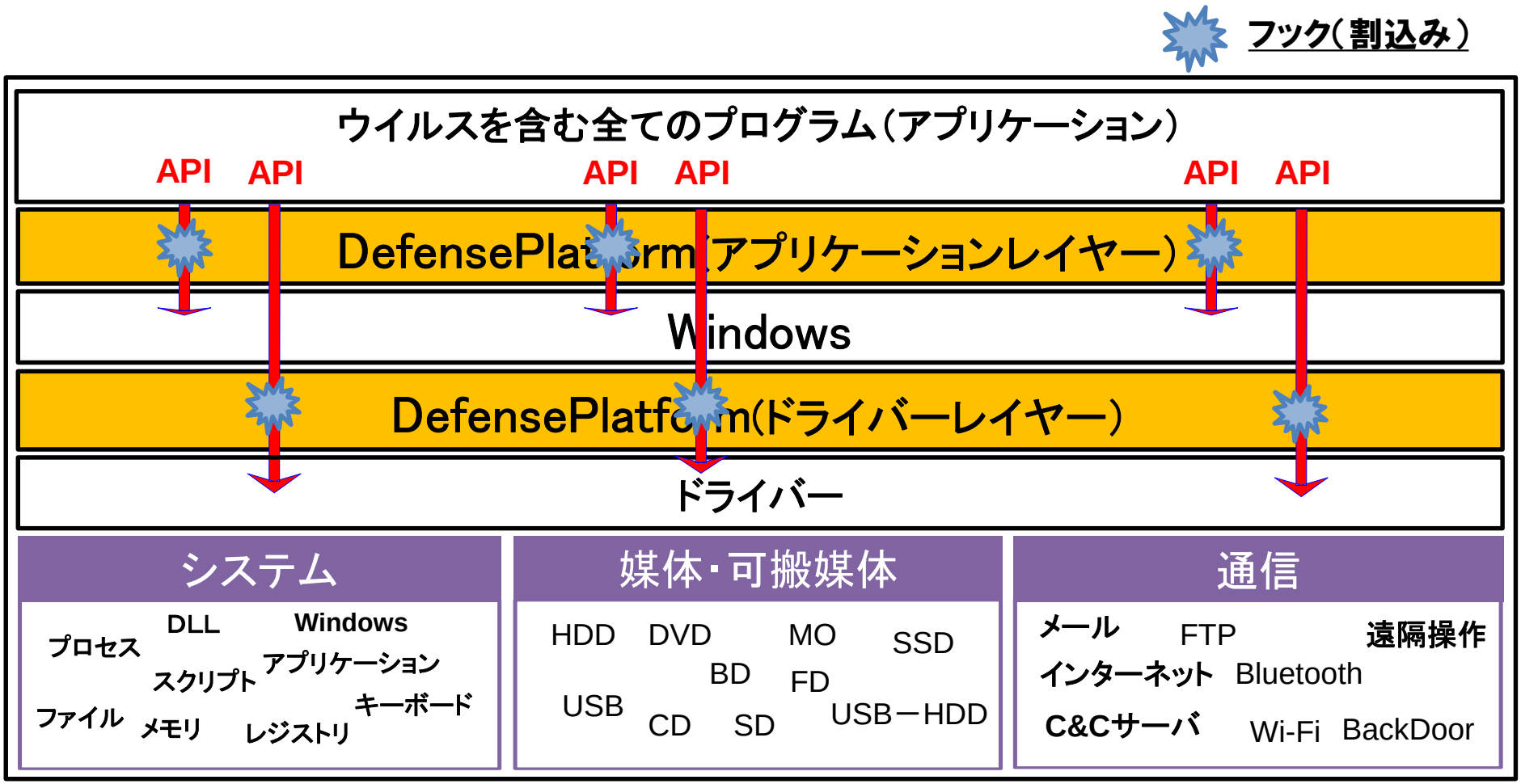
この資料は説明員からの説明が必要な資料です

第17版

Humming HEADS®

割込み型迎撃方式(インターセプト)API監視とは

割込み型迎撃方式(インターセプト)しくみ



DePの概略

① サイバー攻撃対策ソフトウェアです。

② エンドポイントで防ぐ単一のトータルセキュリティソリューションです。

③ APIを監視する「割り込み型迎撃方式」であり高級で詳細な履歴を収集記録します。

④ パターンファイルはありません。

⑤ 業務を阻害しない軽快なソフトウェアです。

⑥ 他社製品と共存が可能です。

当社が確認したDePと共存可能なアンチウイルスソフト

メーカー名	製品名
トレンドマイクロ	ウイルスバスター クラウド
シマンテック	ノートン インターネットセキュリティ
マカフィー	マカフィー インターネットセキュリティ
カスペルスキー	カスペルスキー インターネットセキュリティ
ESET	ESET SMARTSECURITY 7
ソースネクスト	スーパーセキュリティZERO
Ahnlab	AhnLab V3 Lite ver.1.3.0.582
AVAST	avast! Free Antivirus ver.8.0.1483.72
Avira	Avira Internet Security
Bitdefender	Bitdefender Internet Security
F-Secure	F-Secure インターネット セキュリティ 2014
G Data	G Data インターネットセキュリティ 2014
KINGSOFT	KINGSOFT Antivirus 2013
PANDA SECURITY	Panda Cloud Antivirus

弊社QEC環境にて実際の環境を用意し、DePインストール後の競合の可能性について検査した結果共存が確認できたソフト

デモンストレーション動画

登録するホワイトリスト情報を作成する検知モード

〈検知モード〉

〈ディフェンスモード〉

DePはホワイトリスト

パターンマッチ式や脆弱性診断は**ブラックリスト系**の製品です。ビルの入出管理で例えると、それは「ビルに**入らせない人**のリスト」を作成します。

DePは**ホワイトリスト系**の製品です。つまり「ビルに**入れる人**のリスト」を作成します。

DePはブラックを探すのではなく、**されたくない事を止める（捕獲を含む）**、**全く新しい割込み型迎撃方式（インターセプト）**のソフトウェアなのです。

DePの特徴

重要な情報ほどパスワードや暗号によって守られ、人間にしか開くことができなくなっています。
機械的にパスワード解除や復号が短時間でできないため、これらのファイル等を無視するしかありません。そのためアンチウイルスのパターン比較ができない場合があります。

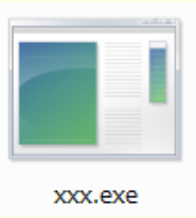
DePはパスワード入力、復号が行われブラックが通信、メモリ書き込み、ファイル書き込みなどを行うAPIの使用を止めます（寸止め、現行犯逮捕）。

様々な場面でブラックの動きを止める

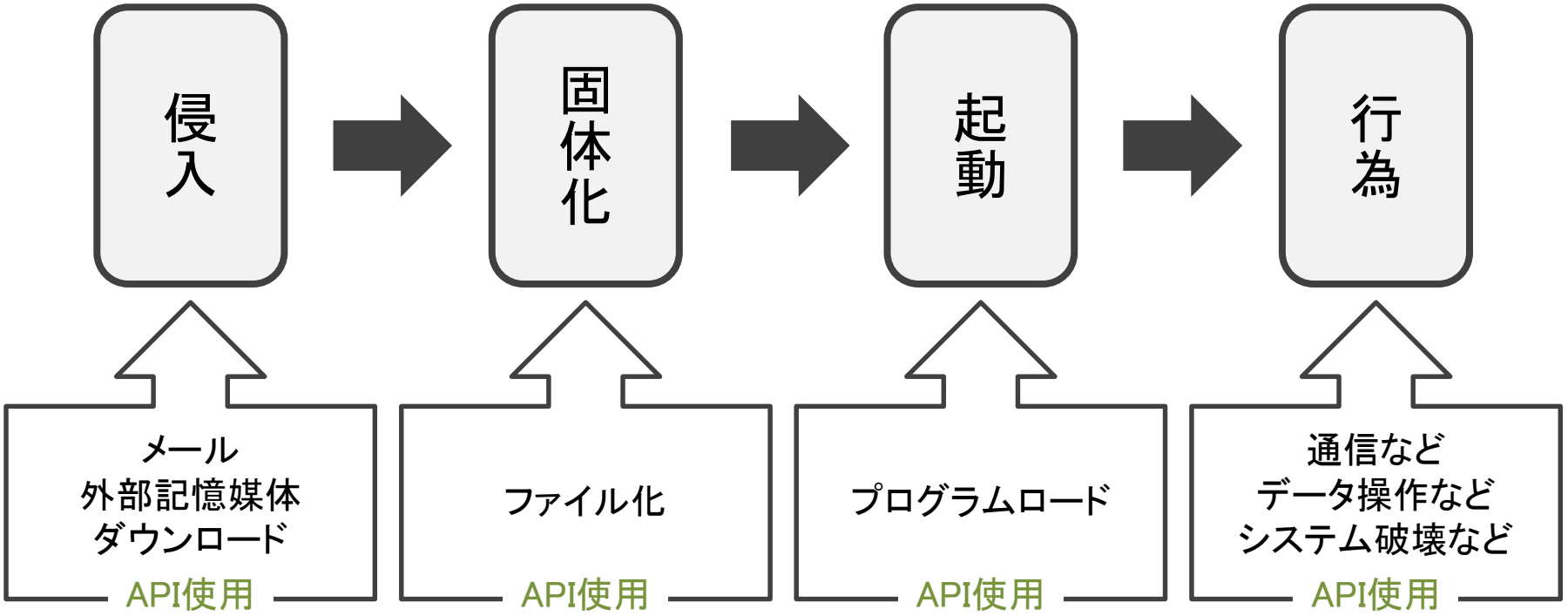
Defense Platform

ウイルス ＝ プログラム
プログラム＝APIを使用

- .exeファイル
- マクロ
- スクリプト



【PC内部でのプログラム（ブラック）の動作例】



WindowsXPサポート終了以降のDePによる脆弱性対策

2014/4/9にMicrosoftによるWindows XPのサポートが終了し、それ以降はセキュリティ更新パッチが提供されなくなります。又、2015年7月にはWindows Server 2003もサポートが終了します。そのため、それ以降で脆弱性が発見された場合、その脆弱性が埋まることがないため、悪意の第三者による攻撃が可能になってしまいます。

しかし、脆弱性を利用したサイバー攻撃も必ずWindowsAPIを使用しているため、DePによりシステムの改竄・破壊や、可搬媒体、通信を利用した情報窃取につながる全てのAPIを監視することで、脆弱性を利用されたとしても被害を発生させません。

また、新しいAPIの提供は、新しいOSやサービスパックのリリース等のタイミングでのみされるため、Windows XPはこれ以上APIが増えることはなく、つまり、Windows XPにはDeP未対応のAPIは存在しません。従いまして、今後、新たな脆弱性が見つかったとしても、その攻撃は全てDePに監視されたAPIを利用して行われるため、100%検知します。

また、脆弱性はOSだけでなくアプリケーションにも存在します。IE6やOffice2003のサポートもXPと同時期に終了します。自社開発のアプリケーションは一般に脆弱性に気付きにくいため未知の脆弱性として残り続けます。しかし、これらの脆弱性を利用した攻撃も、必ずWindowsAPIが利用されるため同様に対策することができます。

サイバー攻撃対策製品ラインナップ

ユーザ規模	構成	製品	特長	履歴の蓄積	ホワイトリストの作成・配信
中小規模・個人ユーザ	スタンドアロン	Defense Platform Home Edition	・サーバ不要	・各PCのローカルディスクに蓄積 ・一定サイズに達したら古い履歴から上書き	・各PC上で作成、即時反映
中小規模・個人ユーザ	クライアント・サーバ	Defense Platform Business Edition	・クラサバ環境の構築(インストール、設定)が簡単 ・各クライアントPCのハードウェア情報、ソフトウェア情報の自動収集が可能	・各クライアントPCのローカルディスク上に一時的に蓄積 ・指定のタイミングでクライアントからサーバに送信 ※OS起動時、OS終了時、ログオン時、指定時間間隔 ・サーバ上で全クライアントPCの履歴をまとめてCSV変換	・サーバ上で共通ホワイトリストを作成し、クライアントに即時配信 ※クライアントがオフライン時は次回サーバ接続時に取得 ・各クライアントPC上で個別ホワイトリスト作成が可能 ※サーバで作成した共通ポリシー優先 ※サーバから個別ホワイトリストの消去が可能
大規模ユーザ	クライアント・サーバ	SeP ＋Defenseオプション	・要件に応じた細かい設定が可能 ・過失による情報漏洩対策が可能		

品質評価センター「QEC（Quality Evaluation Center）」での動作検証

ハミングヘッズでは、弊社技術「InP」を使用した**自動**品質評価センター「QEC（Quality Evaluation Center）」で、日夜製品の品質評価を行っています。

4000台（物理PC2000台）800万項目の検査を18時間で行える技術により、常に高い品質を保っています。

	従来の手動による品質評価	QECによる品質評価
1回当たりの作業時間	約4ヶ月	18時間
テスト項目数	30万項目	800万項目
年間可能テスト回数	2回	300回以上

自動品質評価センター（QEC）