

なぜ従来型アンチウイルス製品のままではいけないのか？

環境の変化

- ・リモートワークの増加
- ・海外拠点数の増加
- ・暗号化通信の主流

攻撃者の変化

- ・標的型攻撃
- ・ビジネスメール詐欺
- ・ランサムウェア

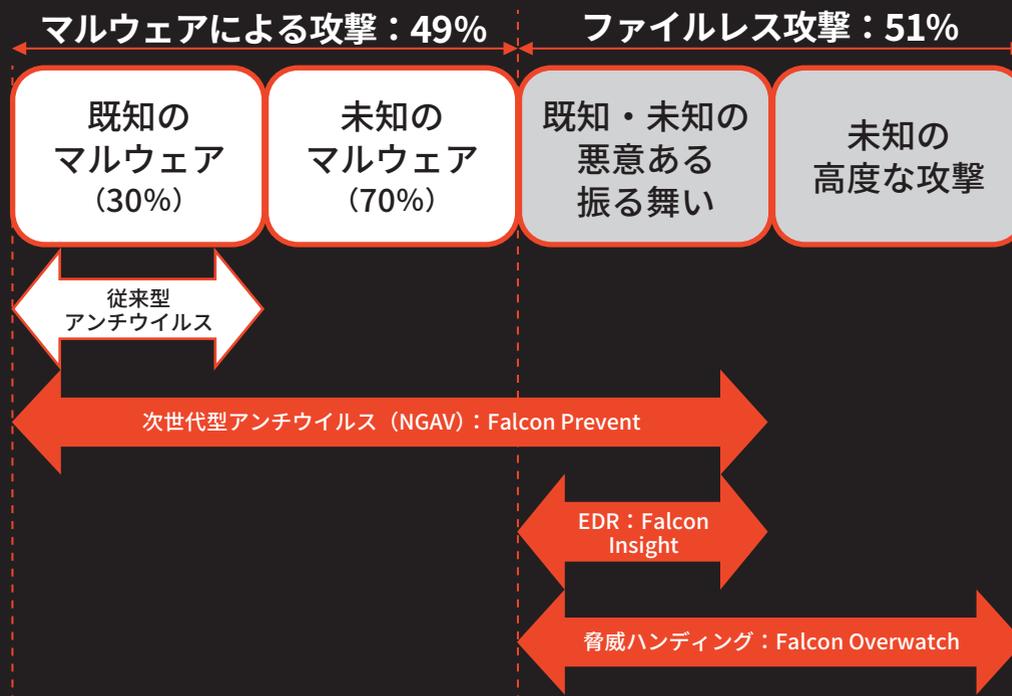
従来型アンチウイルスでは
阻止できない脅威が増えている！！

NGAV・EDR・脅威ハンディングで、従来型アンチウイルスでは、阻止できなかった脅威から守ることができます。

これまでのアンチウイルス製品は、ウイルスの特徴を登録したデータベースと検査対象のファイルを比較し、ウイルスを検出するという手法です。

この方法は、パターン化されていないものや、新種のウイルスなど、登録されていないウイルスを検出するのは難しいという点や、新たなウイルスの特徴をデータベースに登録する前にウイルスに感染してしまうこともあるという問題があります。

NGAV×EDR×脅威ハンディングで 3つの壁で脅威から守る！



※割合は、2020 CrowdStrike グローバル脅威レポートより抜粋。Crowdstrike.jp/gtr よりダウンロード可能。

NGAV Falcon Prevent

シグネチャを利用しない
機械学習により
既知・未知のマルウェアを検知。

- ◆オフラインでも検知・ブロック
- ◆ファイルレス攻撃を防御
- ◆軽量エージェント

EDR Falcon Insight

EDR が振る舞いを見て、
自動的に怪しいと
判断したものを検知。

- ◆リモートから端末の隔離可能
- ◆完全なリアルタイムの可視性
- ◆攻撃者が痕跡を消した場合も
行動を全て把握可能

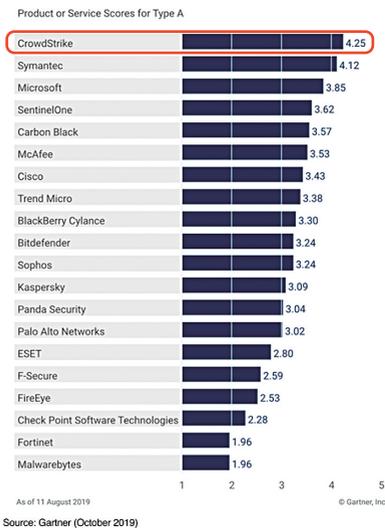
脅威ハンディング Falcon Overwatch

プロフェッショナルが、
24 時間 365 日振る舞いを監視し、
NGAV/EDR で機械的に
検出できない、
高度な攻撃を検知。

CrowdStrike製品は 高く評価されています！

CrowdStrikeおよびATPについて
Gartner社の第三評価においても
高い評価を得た実績のある製品と
なっています。

Figure 1. Vendors' Product Scores for Type A Use Case



As of 11 August 2019
Source: Gartner (October 2019)
出典: <https://www.crowdstrike.com/blog/crowdstrike-scores-highest-overall-gartner-critical-capabilities-epp-2019/>

セレマアシストなら全てサポートできる

ライセンス販売

- ・公式販売パートナーとしてのライセンス販売可能

導入支援

- ・お客様の環境に合わせた設計、構築、展開が可能

運用支援サービス

- ・弊社の運用センターの中でサポート
- ・専門的なセキュリティ知識を持つ技術者の提供
- ・標準的な運用資料の提供

製品の優位性

- ・ 予防・事前対策
- ・ 自動ブロックと検知・対処
- ・ ソフトウェアが軽量
- ・ 物理、仮想、クラウドを全てに対応
- ・ 自動化とプロアクティブな棒業

導入事例

	A社	B社	C社
ライセンス販売	×	○	×
導入支援	○	○	○
運用支援	○	○	×
導入台数	8,000台	100台	5,000台
期間	150日	90日	120日

株式会社セレマアシスト

本社 〒553-0003 大阪府大阪市福島区福島 1-4-40 JBSL 梅田ビル 9F
TEL.06-4797-6464 FAX.06-4797-6465

東京事業所 〒101-0041 東京都千代田区神田須田町 2-25-16
日宝秋葉原ビル 11F

TEL.03-6285-2930

06-4797-6464 受付(平日 9:00 ~ 18:00)

URL: <https://thelemaassist.com/>



お問い合わせはこちら

<https://thelemaassist.com/contact/>

