CROWDSTRIKE

今こそ企業に必要なのは、検知・防御にとどまらない最先端の「NGAV」

2019年 12月

株式会社マクニカ

目　次

始めに

サイバー攻撃から自社を守るというミッションは全ての企業が持っています。そのような世の中で、企業を取り巻く環境や攻撃者は日々変化するため、攻撃者の手法や、それから企業を守るセキュリティ製品は 5 年あればほとんど変わってしまうとも言われています。
本資料はそのような変化に伴い、今企業にとってどのような対策が必要であるか知っていただくために、企業がエンドポイントセキュリティ対策において陥る課題やそれを解決するソリューションを解説します。「エンドポイントは従来型のアンチウィルスのみを利用しているお客様」・「社内セキュリティに課題を感じているお客様」・「エンドポイント対策の強化を考えているお客様」に是非読んでいただきたい資料となっています。

第1章：従来型アンチウィルス製品での課題

なぜ企業は今、エンドポイントでの対策の強化が必要であるのか

現在多くの企業が、エンドポイント対策の強化を検討しておりますが、改めてなぜエンドポイントでの対策が必要となっているのか整理してみましょう。

■ 攻撃者の変化

組織における 10 大脅威

順位	組織における脅威
1 位	標的型攻撃による被害
2 位	ビジネスメール詐欺による被害
3 位	ランサムウェアによる被害

出典：独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2019」

URL：https://www.ipa.go.jp/security/vuln/10threats2019.html

攻撃者の手法も年々多様化しており、上記は IPA が発表している組織に対する 10 大脅威の上位 3 種類の攻撃です。これまで標的型攻撃は注目され続けていましたが、近年脅威を増しているのは金銭獲得を目的とした 3 位にランクインしているランサムウェアや仮想通貨のマイニングマルウェアです。この様な攻撃は金銭の回収効率を高めるため、不特定企業や個人をターゲットとする傾向があり、今やどの企業もサイバー攻撃を受けるリスクがあると言えます。

数年前

企業・個人を狙った愉快犯

- 世間を騒がせ、自分のスキルをアピールすることを目的とした攻撃

近　年

特定の企業を狙った標的型攻撃

- 機密情報や知的財産を狙ったなりすましメールによる攻撃　等
- サプライチェーンを利用した攻撃　等

全ての企業を狙った無差別型攻撃

- 金銭を狙ったランサムウェアやマイニングマルウェア
- 金銭や業務妨害を目的としたゼロデイ攻撃　等

■ 企業を取り巻く環境の変化

攻撃手法だけでなく、皆さまの企業を取り巻く環境自体も変化してきています。以前までは出入り口が 1 つであった企業のネットワーク環境は多様化しており、それに合わせた対策が必要となってきています。そのため、出入り口対策が意味をなさなくなるケースが増え、企業ではサイバーセキュリティの見直しが必要とされています。

環境の変化	変化に伴う課題
働き方改革による 持ち出し端末の増加	社内 LAN を通らないため ゲートウェイ対策が困難
国内・海外拠点数の増加	拠点毎にゲートウェイ製品の 導入が必要となる
クラウドサービス利用の普及により 暗号化通信（HTTPS）が主流に	内容が見えないため ゲートウェイ対策が困難

サイバー攻撃で狙われるデータは PC 端末やサーバなどのエンドポイントに保存されていますが、上記の既存製品の課題によりサイバー攻撃がエンドポイントまで到達してしまうケースが増えています。このような環境の変化に対して、エンドポイントを強化することが最新の脅威への対策として一番有効であると言えます。そのエンドポイント対策としてシグネチャーでパターンマッチングを行うアンチウィルス製品が主流であり、マルウェアを防いできました。しかし、攻撃手法の変化や企業を取り巻く環境の変化により、従来のエンドポイント対策では不十分となってきているのです。

なぜ既存アンチウィルス対策では不十分であるのか

① 検知・防御が困難な攻撃の台頭

攻撃者も日々セキュリティ製品の抜け道を研究し、新しい攻撃手法を生み出しています。近年では従来型アンチウィルス製品を簡単にすり抜けてしまう様々な攻撃手法が主流となってきています。

ゼロデイ攻撃

ゼロデイ攻撃とは、ソフトウェアの脆弱性が発見されて修正プログラム（ パッチ ）がリリースされる日（One day）より前にその脆弱性を悪用する攻撃のことを指します。
ゼロデイ攻撃が行われた場合、それに対応するシグネチャーや URL レピュテーションの情報がない状況で攻撃が行われる為、シグネチャーを利用した従来型のアンチウィルスでは検出が不可能であると言っても過言ではないのです。

ファイルレス攻撃

攻撃手法には、主にマルウェアを使った「ファイルベースの攻撃」と、ファイルを伴わない Windows のコマンド実行ツールを悪用したり、悪質なプログラムをメモリ上に直接展開したりする「ファイルレス攻撃」に分類することが出来ます。

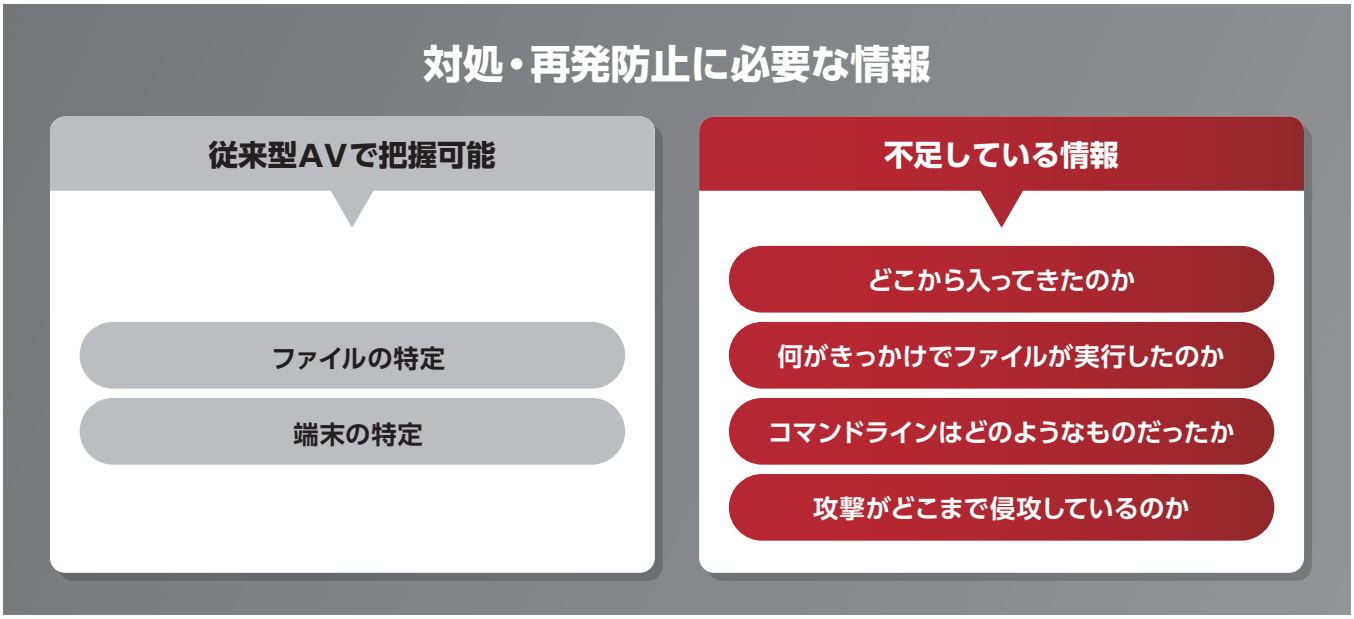
「ファイルベースの攻撃」… 従来型アンチウィルスのシグネチャーマッチング / 次世代型ファイルベースの機械学習・AI 検知にて検出可能
「ファイルレス攻撃」… 振る舞いベースの脅威検出製品にて検出可能

引用：CrowdStrike「2019Grobal Threat Report」
URL：https://crowdstrike.lookbookhq.com/web-global-threat-report-2019

現在 CrowdStrike 社によって観測した攻撃統計の約 4 割がファイルレス攻撃となっており、従来型のアンチウィルスでは検出できない攻撃が約半数近くになります。そのため、従来型のアンチウィルス製品での対策では不十分であると言えるのです。

② 不明瞭で特定困難な侵入経路

従来型のアンチウィルス製品で攻撃が検出された際、攻撃のもととなったマルウェアを特定することはできます。しかし、マルウェアの特定のみでは侵入経路やどのような挙動（外部通信等）を行ったのかが不明瞭なため、再発防止策を立てたり、上層部へ原因報告したりするには情報が不足しているケースが多々あります。



③ 運用者に立ちはだかる対処・復旧の壁

インシデントが発生した際、一般的にはネットワークの端末隔離や特定ファイルの削除が必要になるケースがあります。端末のネットワーク隔離を行うには、その端末を利用している従業員が実施する必要があり、リアルタイム性と確実性に欠けます。また、特定ファイルの削除など端末に対して操作を行う場合、端末を従業員から回収し詳細な調査を行う必要がありますが、回収までに数日要し修復すべき箇所を調べる技術が求められます。
このような対処は、従来型アンチウィルス製品では解決できず、セキュリティ運用のコスト増加に繋がります。

④ 業務に支障をきたす運用と端末負荷

従来型のアンチウィルス製品の運用をしていると、1 度はこのような声が従業員から出てくるのではないでしょうか。従来型のアンチウィルス製品のほとんどはシグネチャーを使い端末上でマッチングをさせているため、端末への負荷が大きくなります。また、定期スキャンが必要となるため、その時間帯はさらに業務効率が下がってしまう恐れがあります。

また、従業員だけでなく製品の運用部隊への負担もあります。オンプレミスの製品がほとんどであるため、サーバの管理が必須となり、サーバのメンテナンスや日々のシグネチャー管理による業務負担は多大なものとなります。

従来型アンチウィルス製品での対策の課題まとめ

従来型アンチウィルス製品の課題点

1. 検知・防御が不可能な攻撃の台頭
2. 不明瞭で特定困難な侵入経路
3. 運用者に立ちはだかる対処・復旧の壁
4. 業務に支障をきたす運用と端末負荷

企業はセキュリティの施策において、このような課題を抱えています。それでは具体的にどのような対策をすることが有効であるのか、第２章でご説明します。

第２章： 今までの常識を覆す最先端のNGAVソリューション

これまで述べたような、従来型のアンチウィルス製品の課題を解決するのが、CrowdStrike 社の提供する**機械学習・AI・振る舞いによる検知・ブロック、調査・対処**を行う NGAV 製品「**Falcon Prevent**」です。

課題を解決する次世代型エンドポイント対策製品

1. 多様な検出方法による検知・ブロック能力
2. インシデント状況とマルウェア挙動の可視化
3. 端末の確実なネットワーク隔離と遠隔操作の即時実行※
4. 軽量なエージェントとメンテナンス不要のクラウド環境

※こちらの機能はオプションとなります

① 多様な検出方法による検知・ブロック能力

Falcon Prevent は機械学習・AI・振る舞いにて攻撃を検知するため、マルウェア（ランサムウェアを含む）のみならずファイルレス攻撃の検出も可能です。検出だけでなく、検出したファイルの自動隔離や悪意のある挙動のプロセスの自動停止などのブロック機能を有しています。

また、第１章で言及した「ゼロデイ攻撃」に対しても機械学習・AI による検知が有効となります。機械学習はマルウェアの様々な特徴を日々学習しているため、新しい攻撃に対しても悪意のある動作と正常な動作を区別することができます。さらに、機械学習検知エンジンは端末上でも動作しているため、一時的なオフライン環境で検知・ブロックを行い、ブロックされたマルウェアは安全な形式で即座に隔離する事が可能です。

■ アンチウィルスの代替ソリューションとしての第三者機関の認定

Falcon Prevent は従来型アンチウィルス製品と共存させて運用することも可能ですが、従来型のアンチウィルスの代替の製品として導入することも可能です。AV-Comparatives や SE Lab といった第三者評価機関が、**Falcon Prevent** のアンチウィルス機能を認定しています。

参考

https://www.av-comparatives.org/vendors/crowdstrike/
https://selabs.uk/download/enterprise/ar/2019-selabs-annual-report-1-0.pdf

② インシデント状況とマルウェア挙動の可視化

攻撃を検出・ブロックするだけでなくそのアラートに対する詳細調査が可能なことも、**Falcon Prevent** の大きな特徴です。従来型のアンチウィルス製品は侵入経路が分からず、対策が立てられないことも課題としてあげられますが、**Falcon Prevent** は検出した攻撃の前後のプロセスを可視化するため、侵入経路を簡単に把握することができるのです。また、詳細なプロセスアクティビティを表示するため、それらを利用したアラートの調査が可能です。

表示可能なプロセスアクティビティ

- プロセスの検知時間・実行ユーザー名
- 検知のサマリー（どのようなものをなぜ検知したのか）
- 利用された攻撃手法
- 実行されたコマンドラインの履歴
- ファイルパス
- ハッシュ値
- プロセスの開始時間と終了時間
- 隔離したファイルの詳細
- ユーザーの詳細（ログイン時間・ログインドメイン等）
- ホストの詳細（OS・ローカル IP・MAC アドレス等）
- ネットワーク通信の履歴
- レジストリの操作の履歴
- ファイル読み書きの履歴

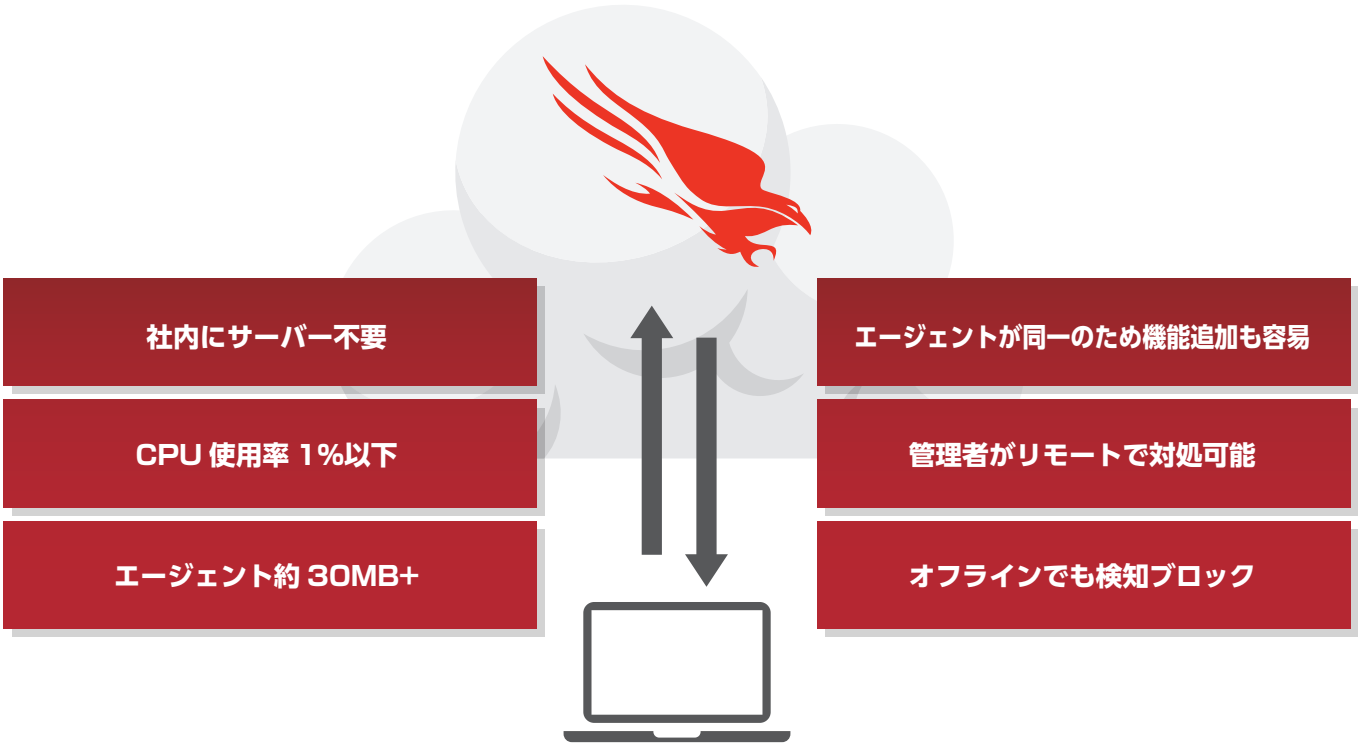
上記の様な 1 つの画面で、各プロセスに関する詳細なアクティビティを確認することが可能なため、アラート調査も容易です。

③ 端末の確実なネットワーク隔離と遠隔操作の即時実行 ※こちらの機能はオプションとなります

Falcon Prevent では調査したインシデントの対処と復旧まで行うことが可能です。対処が必要な場合には、アラートの調査画面から 2 クリックでその端末に対するネットワーク隔離が可能です。また、通常実際に端末を回収して作業を行うようなファイルの取得・削除、レジストリの確認・削除などのコマンドを利用した遠隔操作も実行できます。
この機能を利用することで、管理者がリモートでネットワークの隔離を行い端末所有者の対応が不要となるため、確実にネットワーク隔離することが可能となります。また、遠隔操作で対処を行うことで端末回収が不要となり、どこに端末があっても即時の対応が実現します。

④ 軽量なエージェントとメンテナンス不要のクラウド環境

端末負荷の観点として、シグネチャーに依存しない機械学習検知エンジンを採用しているため、ディスクに書き込むデータは数十 MB と軽量であり、また、稼動時の CPU 使用率は 1% 未満と端末への負荷も低い仕様になっています。システム管理の観点では、端末の日々のシグネチャアップデート作業は不要となり、クラウドのシステムは CrowdStrike 社が管理しているため、こちらも作業は不要となります。



クラウド型が実現する軽量な次世代型エンドポイント製品

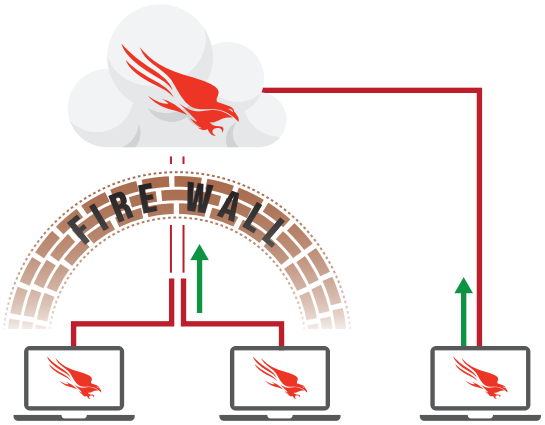
サイバー攻撃から自社を守るためには、様々な変化に対応する製品を選択していくことが非常に重要です。**Falcon Prevent** は振る舞い・機械学習・AI での検知・ブロック、調査・対処を行うクラウド型の製品であるため、現在のさまざまな課題をもつ企業の皆さまに有効なソリューションとなっています。

第３章：包括的なエンドポイント対策を提供するCrowdStrike Falcon

CrowdStrike 社は次世代型アンチウィルス製品 **Falcon Prevent** だけではなく、様々な機能を提供しています。それらは「Falcon シリーズ」であり、Falcon シリーズを通して提供が可能な CrowdStrike 社の強みを最後にご紹介します。

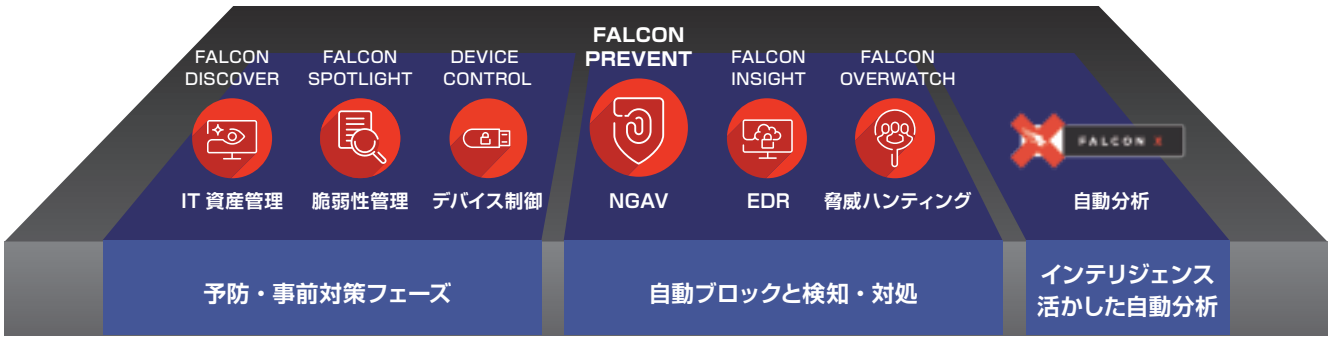
■ 攻撃者の行動を全て見透かす業界最高水準の EDR

深い情報を取得し、様々な情報検索機能や対処機能が備わった EDR（Falcon Insight）も多くのお客様にご利用頂いております。端末からリアルタイムで、操作ログをクラウドへアップロードしているため、攻撃者が痕跡を消してしまった場合も行動を全て把握することができます。



■ 多機能を実現するシングルエージェント

CrowdStrike Falcon はアンチウィルス機能だけでなく、EDR 機能や USB 制御など多数の機能を有しており、その全機能を Falcon Prevent と同一のエージェントで利用することができます。そのため、機能追加したい場合も環境構築は一切不要となっており、機能の追加を気軽に行うことができます。



■ インテリジェンスを活かした 24 時間 365 日の監視

また、CrowdStrike 社は独自のインテリジェンスを保有しており、インテリジェンスチームは世界中の 120 以上 の攻撃者グループを日々監視し、彼らの攻撃手法やモチベーションを調査しています。また世界 178 か国にある Falcon センサーからは週に 2 兆個のイベントログを収集しており、それを 1 か所に収集することでインテリジェンスをより強固なものとしています。そのインテリジェンスはFalconと連携しているので、常に最新の脅威へ対応した製品でお客様を守ることが可能となっています。さらに、「Falcon Overwatch」の機能を利用すると、そのインテリジェンスを活かした CrowdStrike 社のハンティングチームが皆さまの環境を 24 時間 365 日監視します。彼らは機械では見つけられないような、高度な攻撃まで見つけることが可能です。

おわりに…

サイバーセキュリティは企業にとって、必ずついてくる課題です。限られたリソースでどのような対策を行っていくか十分に検討し、最適な選択を行う必要があります。そのような検討に、是非この資料をお役立てていただければ幸いです。

「Falcon Prevent Free Trial」

お客様の環境で 15 日間無料でお使いいただけます。
Falcon Prevent を試したい方はこちらまで！

cs_sales@cs.macnica.net
件名：Falcon Prevent Free Trial に関して
本文：（下記をご記載ください）
ご氏名（ローマ字名）
勤務先社名
導入予定先企業名
E メールアドレス
電話番号

045-476-2010　cs_sales@macnica.co.jp　https://www.macnica.co.jp/

MACNICA

株式会社マクニカ

〒222-8563 横浜市港北区新横浜1-5-5
TEL.045-476-2010 FAX.045-476-2060

西日本オフィス
〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916　FAX.06-6227-6917