鈴木淳也の「Windowsフロントライン」:

「他のセキュリティ対策ソフトはもういらない」とアピールするWindows Defenderの現状

http://www.itmedia.co.jp/pcuser/articles/1804/10/news027.html

Windows標準のセキュリティ対策機能は“オマケ程度”という認識はもう過去のもの。Windows 10の世代では、Microsoftがセキュリティ対策を大幅に強化しており、最新のセキュリティ動向を考慮したアップデートも続けているのだ。

2018年04月10日 06時00分 更新

[鈴木淳也(Junya Suzuki), ITmedia]

先日Twitterのタイムラインを眺めていると、こんな趣旨のツイートが流れてきた。

客「Windows PCを買いたいのですが」

店員「セキュリティソフトの購入もお勧めします。そのままでは危険ですよ」

客「そんなに危ないのですか?」

店員「標準のセキュリティ機能は“ないよりはマシ”程度の機能しかありません。専用ソフトウェアの導入をお勧めします」

この話が真実かはさておき、かつてWindows搭載PCを購入する際には、定石のように語られ続けてきたセールストークだ。実際に店頭で同じような会話をしたことがある方もいるのではないだろうか。

だが2015年7月のWindows 10登場以降、Windows標準のセキュリティ機能「Windows Defender」は大幅に強化されている。もはや特定の“意図した”機能でも利用するつもりがない限り、専用のソフトウェアなしでもWindows Defenderを使うことでセキュリティ対策はほぼ十分、という水準になったといっても過言ではない。

Windows 10の世代では、Microsoftが提供するセキュリティ対策機能のシリーズ総称となった「Windows Defender」

次のデータは、AV-Comparativesというセキュリティ製品の第三者評価を続けている団体が提供している各ウイルス対策製品における防御率などを比較したものだ。ここでは名だたる大手セキュリティ対策ソフトウェアと同格で、Microsoftのセキュリティ製品（Windows Defender）が堂々の100%という防御率をたたき出している。

少なくともこのデータを見る限り、かつて聞かれた「Microsoftが提供するWindows標準のセキュリティ対策は紙程度の防御力」というのが過去の話になっていることが分かるだろう。

AV-Comparativesにおける各社セキュリティ対策製品の防御実績を比較したデータ

セキュリティ対策の世界も重視するポイントが変わりつつある。一昔前の「シグネチャベースのウイルス検出で感染前に確実に防衛する」というスタイルは過去のものとなりつつあり、むしろ「検出しにくいものをいかに見つけ出し、多重の防御壁を敷くかとともに、もし感染した場合には被害拡散を最小限に食い止める」という、いわゆる「Post-Breach（突破後）」対策に重きが置かれつつあるのだ。

検出されるウイルスなども単純な広域拡散型ではなく、企業など特定のターゲットを狙い撃ちし、意図的に拡散を広げていくものが多くなりつつある。ゼロデイ攻撃と呼ばれる対策前の脆弱（ぜいじゃく）性を狙う攻撃の他、シグネチャ検出を困難にするバリアントと呼ばれる亜種が短期で再生産される仕組みなど、従来の感覚では理解を超えた世界がそこにはある。

今回はWindows 10標準のWindows Defenderにスポットを当て、最新のセキュリティ対策の世界をみていく。

セキュリティ戦略とともに役割が変化したWindows Defender

Windows Defenderが最初にリリースされたのは2006年10月のこと。意外に歴史が長く、

その時々のMicrosoftのセキュリティ戦略を反映する形で遍歴をたどってきている。

もともとはMicrosoftがスパイウェアの対策フトウェアを開発するGIANT Company Softwareを2004年に買収したのがスタートで、Windows Defenderはこの技術を基にしたスパイウェア対策機能としてリリースされた。

比較的“おいしい”市場といわれていたウイルス対策ソフト市場へのファーストパーティであるMicrosoftの参入は、当時はまだサードパーティー側の反発が強かったが、セキュリティ強化の側面から考えて「まずはスパイウェア対策から……」という背景があったのだと筆者は考えている。

当初はWindows XPをターゲットにリリースされたWindows Defenderだが、後のWindows VistaとWindows 7では標準コンポーネントの扱いとなり、2009年以降に総合セキュリティ対策製品として「Microsoft Security Essentials（MSE）」がリリースされると、その役割は徐々に後継製品へと引き継がれていくことになった。

当時のMSEは一定以上の防御力が期待できるものの、サードパーティーが出す製品群と比べて若干劣るという印象があった。そのため「ファーストパーティによるサードパーティー市場の強奪」という声こそ一部にあったものの、まだこの時点ではユーザーもMSEにそこまで信頼を置いていない状態であり、競合他社が表立って市場参入を批判するほどの状況ではなかったといえる。

Windows Defenderに転機が訪れたのは2012年にリリースされたWindows 8だ。Windows 8では独自の防御機構を有しており、MSEが動作しなかった。Microsoftはアンチウイルス機能としてWindows Defenderの名称を復活させ、同OSならびに以降のWindowsバージョンにおけるMSEの代替製品として位置付けた。

MSEは2014年4月のWindows XP、続く2017年4月のWindows Vistaにおける延長サポートの終了を経て、対応OSが実質的にWindows 7のみとなり、その座をほぼ完全にWindows Defenderへと明け渡す形となった。

Windows 8以降のOSでは標準コンポーネントとして動作するWindows Defenderは、対応のサードパーティー製品が導入された場合にのみ切り替えが可能な方式となっており、Microsoft以外のセキュリティ対策ソフトを特に入れていない全てのユーザーが利用する標準製品となった。

その歴史的経緯からウイルスやスパイウェアまで、いわゆる「マルウェア」全般を防ぐ対策機能という印象のあるWindows Defenderだが、現在のWindows 10においてはMicrosoftのセキュリティ対策技術や機能を総称したシリーズ名として「Windows Defender」が冠され、それに続く名称で機能が説明されるというブランディングになっている。

家庭向けのWindows 10 Homeにおいても全ての基本機能が備えられており、ウイルス対策を含む少なくとも10種類程度の機能が包含されているが、これがビジネス向けのWindows 10 ProになるとBitLockerやグループ管理の機能が付与され始め、さらに有料サブスクリプシ

ョンであるWindows 10 Enterprise E3やE5になると、より高度な管理機能が利用可能になっていく。

各エディションにおける対応セキュリティ機能の違い

進化するマルウェアとその対策

冒頭でも説明したが、最近のマルウェアは一昔前に主流だったセキュリティ対策ソフトの単純なシグネチャベースの検出エンジンでは検出が難しくなっている。シグネチャで検出されるような同種のマルウェアの存在確率はわずかで、実際にはバリアントと呼ばれるその亜種の方が圧倒的多数だからだ。

Microsoftの集計データによれば、（世界中の）クラウドを通じた毎日450万ファイルの分析において1000回以上検出されるマルウェアの数は全体のわずか0.01％で、96％のマルウェアは一度のみ検出され、以後は二度と出現しないという。

理由としては、マルウェア制作のハードルが比較的容易になる中でバリエーションの開発サイクルが非常に短く、かつ特定のターゲットを狙った攻撃が増加するなど、単純な広域拡散を想定していないケースが多いからだと予想される。つまり、マルウェアが発見されてから逐一対策する手法では、こうしたトレンドに対応できない。

ここで重要になるのは、いかに未知のマルウェアへの対策を行い、もし万が一感染したマシンが発見されても、そこを踏み台に拡散しないよう素早く対策を行うかという点だ。特に後者については、クラウドを通じて素早く感染情報を把握し、リアルタイムでマシンの防御力を維持する仕組みが重要になる。

Windows 10に搭載された「Windows Defenderウイルス対策」では、「Creators Update（1703）」以降に全てのPCで「クラウド保護」の機能が有効になってお

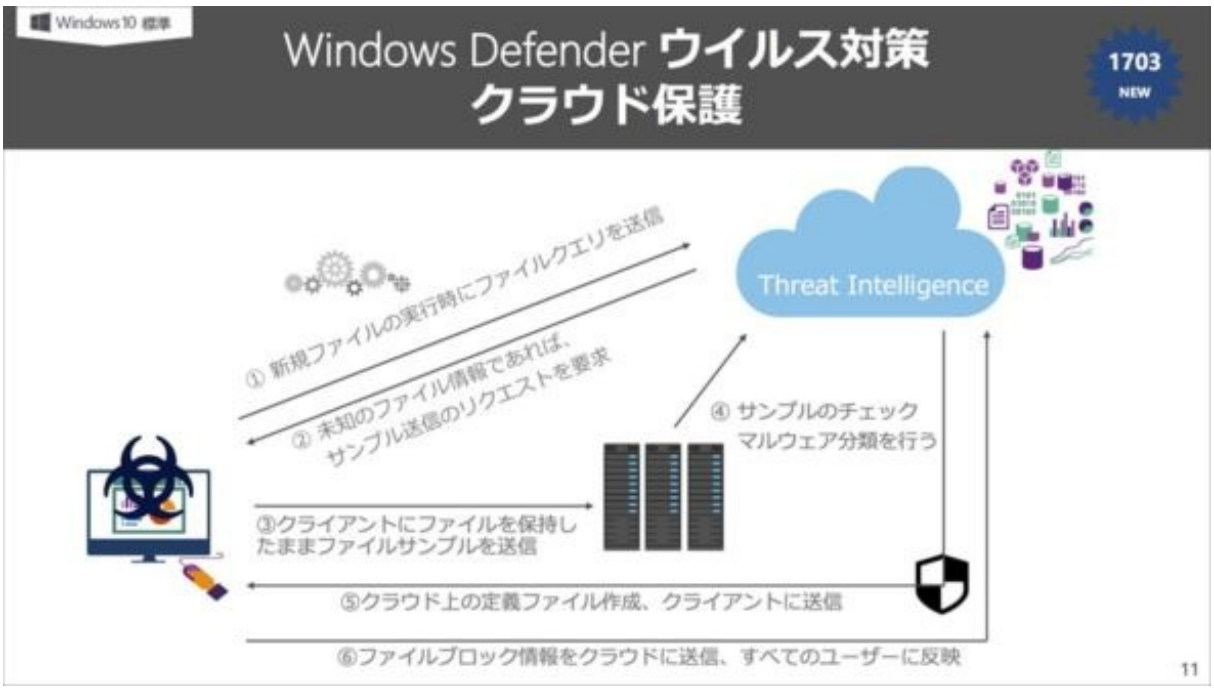
り(「Anniversary Update(1607)」ではオプションにて有効可能)、クラウドを通じてリアルタイムでほぼ最新の対策データが共有され、大規模拡散タイプの脅威を未然に防ぐことが可能だ。

進化するWindows Defenderでのマルウェア対策。「Fall Creators Update(1709)」ではクラウド保護に加えて、機械学習型エンジンが搭載されている

クラウド保護とはどのような仕組みなのだろうか。Windowsでは「テレメトリー(Telemetry)」と呼ばれる手法により、全てのマシン上で動作状況を定期的にモニタリングする仕組みが導入されているが、クラウド保護ではこの仕組みをウイルス対策に利用する。

新規ファイル実行時にクラウド保護が呼び出され、これが未知のファイルだと判断された場合、クラウド側にある「Threat Intelligence」の仕組みがファイルを実行しようとしたマシンに対してサンプルの送信を要求し、分析後に対策結果を返答するのだ。

この対策状況はクラウド保護に対応する全てのマシンですぐに共有されるため、特定マシンでの危険なファイル実行を未然に防ぐだけでなく、すぐに全てのマシンでその結果が共有される。一連の動作に必要な仕組みはテレメントリーを利用する関係上、通信回線にほとんど影響を与えないレベルのデータ送受信しか行われないため、当該マシンがインターネットに接続されている限りは、ほぼ自然な形で保護が継続中であると考えていい。

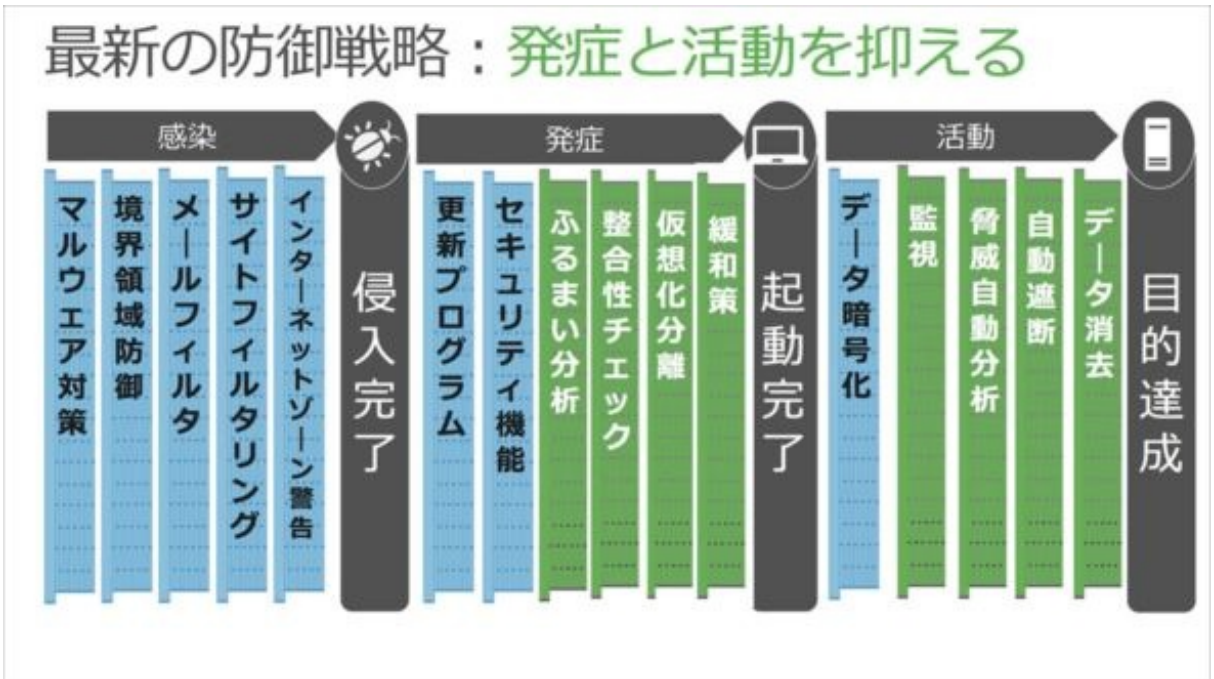


Windows Defenderクラウド保護の仕組み

「事前に検知して被害を未然に防ぐ」というのはマルウェア対策の基本で、これまでの対策はこの手順をほぼ踏襲しており、今後も変わりはない。実際、Windows Defenderウイルス対策に施された最新機能の数々は、この事前検知と予防に焦点を当てている。

一方で、現状の特定ターゲットを狙った攻撃の場合、いったん踏み台となるマシンの乗っ取りを完了させる、あるいは次の攻撃に必要なデータを入手した後、そこを踏み台として本来のターゲットへの侵入を試みるという多段階攻撃が行われることになる。つまり、会社組織のネットワークを狙う攻撃においては、感染後の対策の重要度が増すわけだ。

次の項ではこの辺りを少し詳しく見ていく。

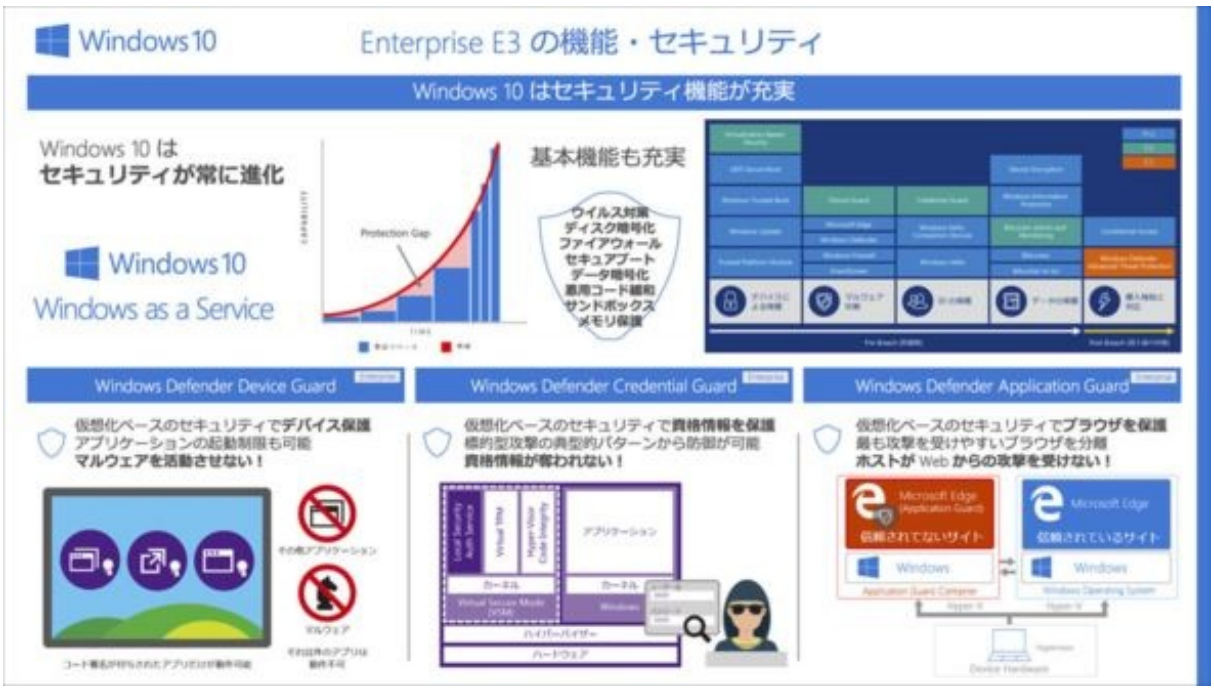


Enterprise E3／E5とAdvanced Threat Protection（ATP）

個々のマシンの拠点防御に必要な機能は、Windows Defenderのシリーズ製品として提供されている。また、企業向けサブスクリプションであるWindows 10 Enterprise E3／E5では、複数マシンを保持する企業組織において重要な管理機能の他、各種データ保護のための特殊機構を提供するWindows Defenderの機能が幾つか用意されている。

まずはEnterprise E3／E5のみで提供される、企業向けの共通機能からみていこう。

一連のセキュリティ手順で利用されるWindows Defender（および関連セキュリティ製品）群と、Ennterprise E3／E5でのみ提供される機能群



Enterprise E3／E5で利用可能なWindows Defenderの機能群

Enterprise E3／E5では、マルウェアだけでなく、認められたアプリ以外の実行を防ぐ機能「Device Guard」、資格情報をOSの実行領域とは分けて保存することでマルウェアの攻撃を防ぐ機能「Credential Guard」が利用できる。

どちらも仮想化の仕組みを用いており、アプリ実行に必要な署名情報の保管の他、特定のサービスや領域へのアクセスに必要となる資格情報をマシン内の別領域で保存しておくことで安全性を高めている。

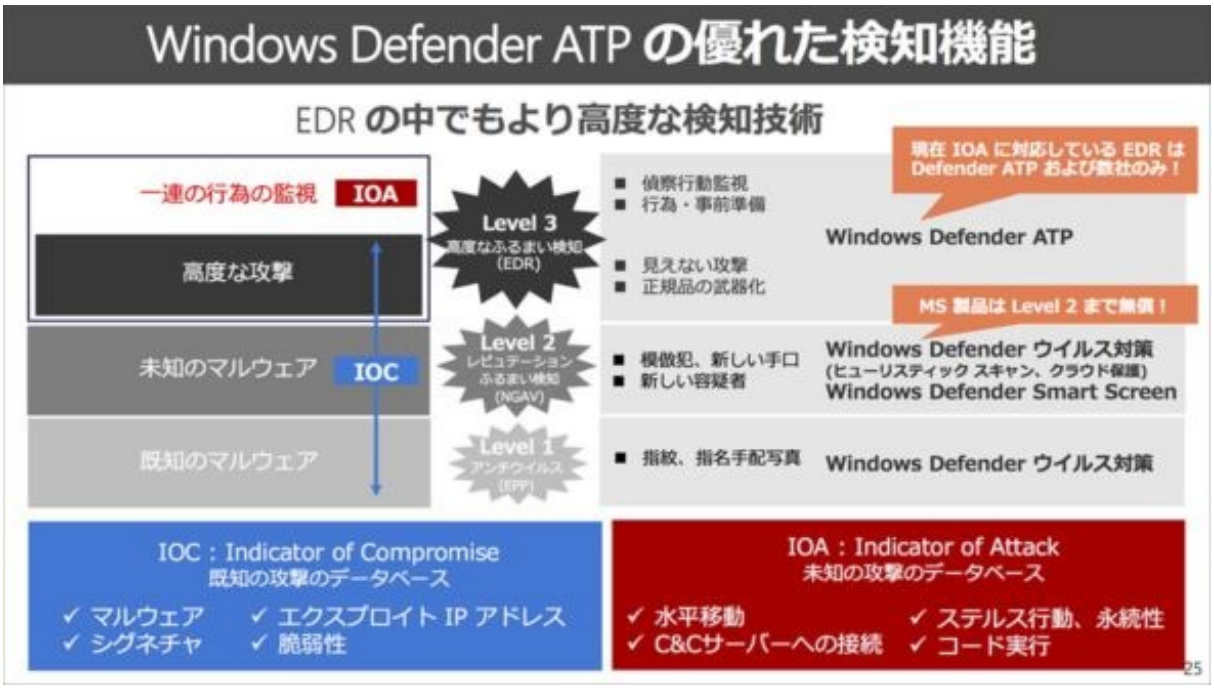
昨今のマルウェアではマシン上のメモリダンプを読んでこうした資格情報を入手するものが存在しているが、ここで入手した情報を基に本命である個人情報などを保管したサーバへのアクセスを試みるなど、踏み台的な使われ方をすることが多い。仮想化でOS領域そのものを論理的に区切ってしまえば、こうしたマルウェアが仮に侵入しても必要な情報にアクセスできず、安全性を高められるという考えによるものだ。

さらに「Application Guard」という機能も使える。これは、侵入の窓口として最も利用されやすいWebブラウザにおいて、仮想化を用いて信頼できるサイトとそうでないサイトの実行をそもそも分離して行うことで安全性を高める機能だ。

そして、エンタープライズにおけるセキュリティにおいて重要となるのがEDR（Endpoint Detection and Response）だ。企業ユーザーを対象にしたセキュリティ製品は多数あるが、EDRによる管理機構こそが選択におけるポイントだといえる。EDRでは組織内で活用するデバイスの挙動を監視し、必要であれば隔離や停止、対策などを行う仕組みだ。

MicrosoftのEDRは「Windows Defender Advanced Threat Protection」で、通称「ATP」と呼ばれている。ATPのメリットは幾つかあるが、その最大のものは「（管理機能を利用するための仕組みが）Windowsに標準コンポーネントとして組み込まれている」という点で、通常

のEDR製品で求められる「各デバイスへの“エージェント”のインストール」が不要となっている。この辺りはファーストパーティーの優位性といえる。



「Windows Defender ATP」の特徴

ATPはWindows 10のバージョンアップとともに進化しており、現在もなお新機能が追加され続けている。利用にはEnterprise E5のサブスクリプションが必要となるが、逆にいえばEnterprise E5のサブスクリプションさえあれば、Windows 10をバージョンアップし続けることで新機能が常に自動的に追加されるため、別途アプリケーションの追加ライセンスを購入したり、エージェントの更新を行ったりする必要はない（OSのバージョンアップ作業は必要だが……）。

間もなく登場するWindows 10の大型アップデート「Spring Creators Update（1803）」においても新機能が追加されており、Microsoftが買収したセキュリティ企業であるHexaditeの自動化技術を組み込んだ、半自動化モードでの脅威への対応が可能となる。

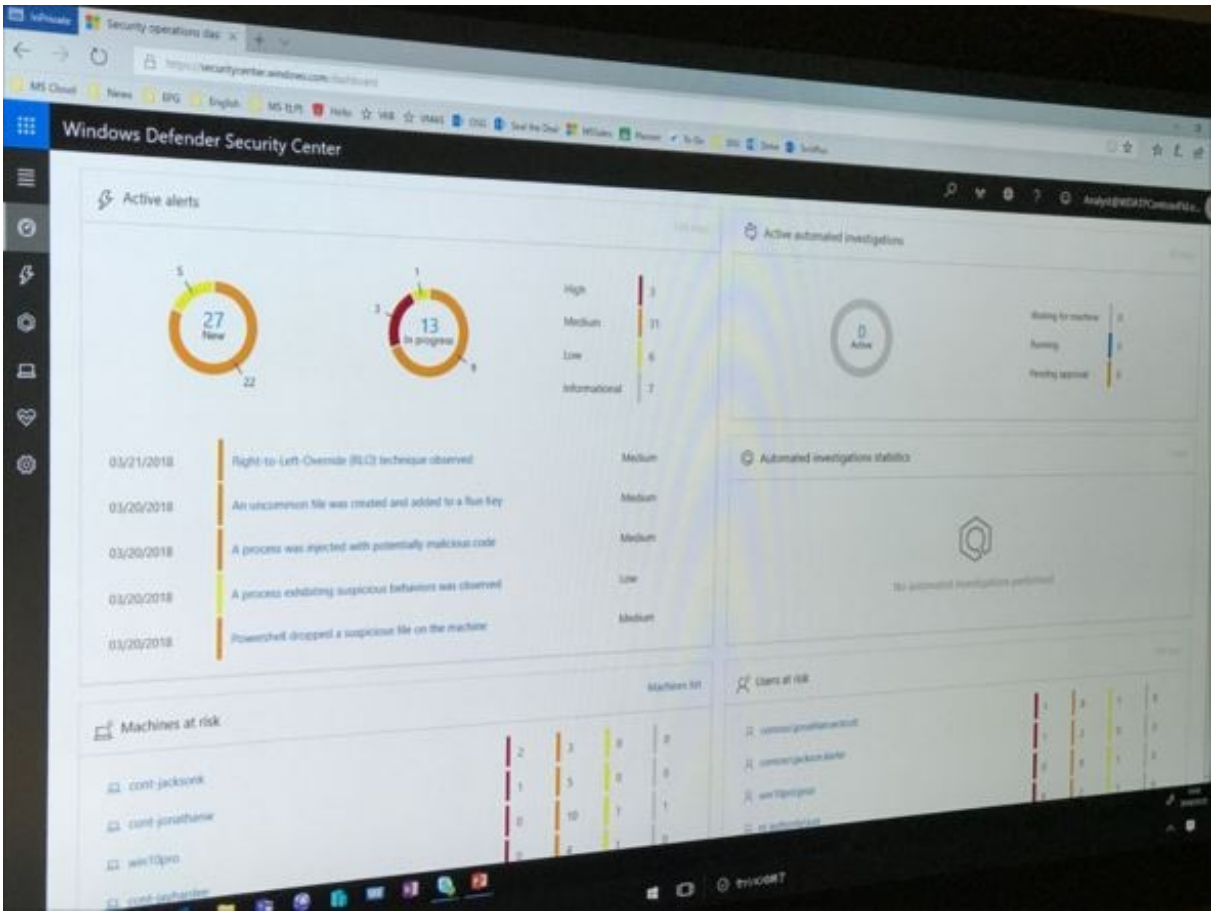
Windows 10のバージョンアップとともに進化するATP

「Spring Creators Update」ではHexaditeの半自動対処ツールを利用可能に

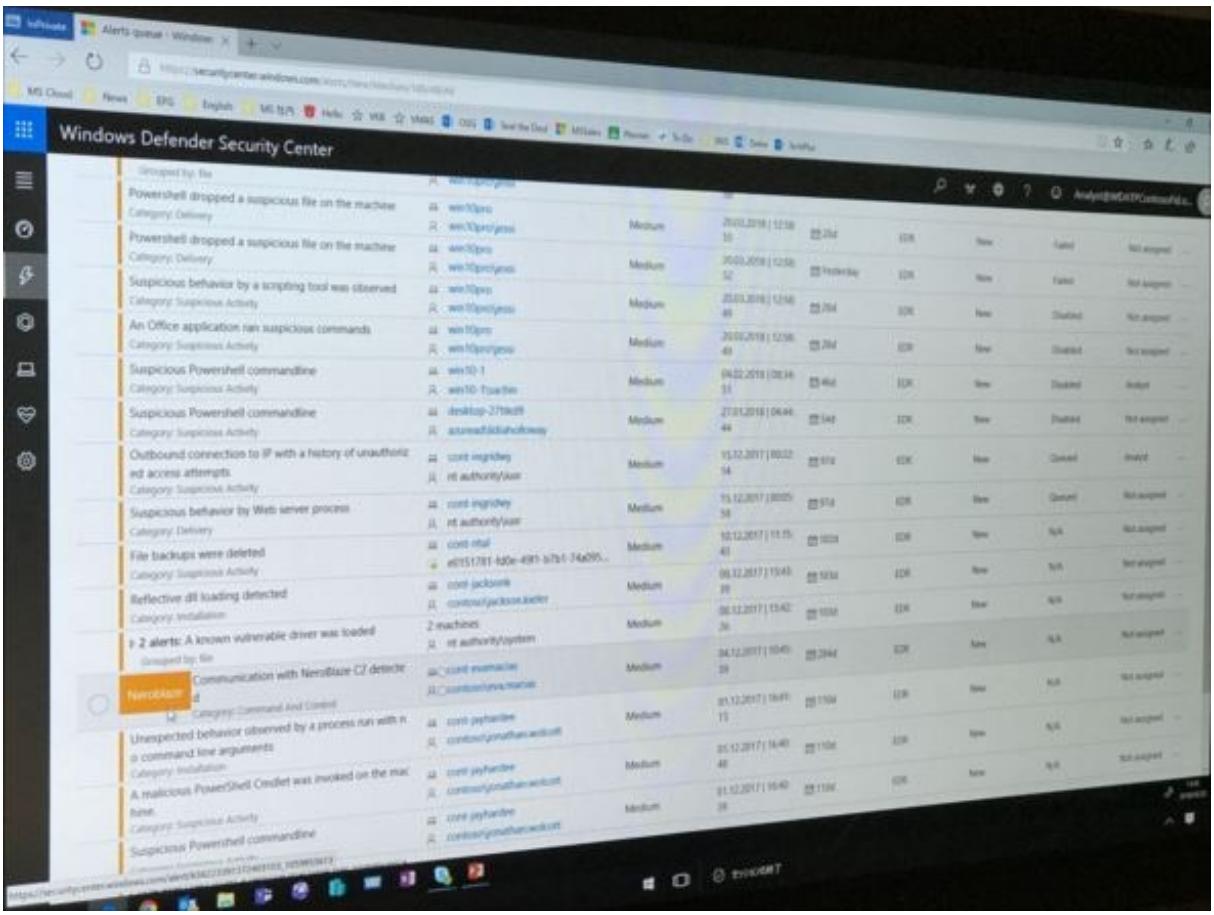
ATPは「Windows Defender Security Center」の管理コンソールから利用でき、通常はダッシュボードを起点に組織内のマシンを監視する形で運用される。脅威はアラートを通じて発見する形となって、適時必要な対処を行っていくことになる。当該のマシンで怪しいプロセスが起動していれば機能を停止し、ブラックリスト化することで他のマシンでの実行を未然に防げる。

また、当該マシンのネットワークからの隔離の他、過去最大180日間までのタイムラインをさかのぼっての分析や対処など、必要に応じたアクションをとっていく。Fall Creators Updateではスコアリングの機能が追加され、現在の組織の脅威への対応状況をアップデートの適用率などを基準に判定してくれる。

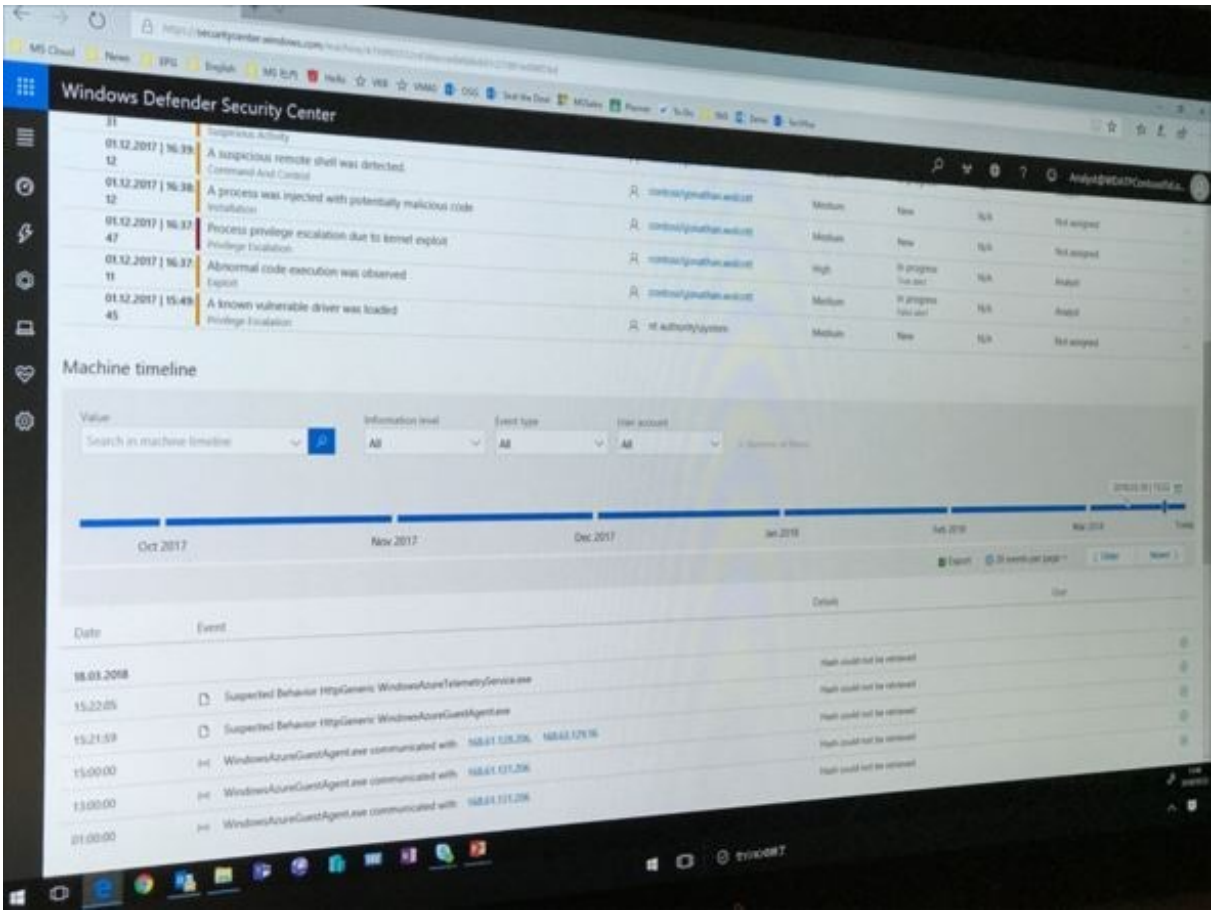
なお、管理コンソール自体はクラウド上で運用されているが、収集されたデータの管理などは各クライアントにATPの専用テナントが用意されるため、前述のThreat Intelligenceを除けば、他社を含むクラウド内でデータが横断的に利用される心配はない。



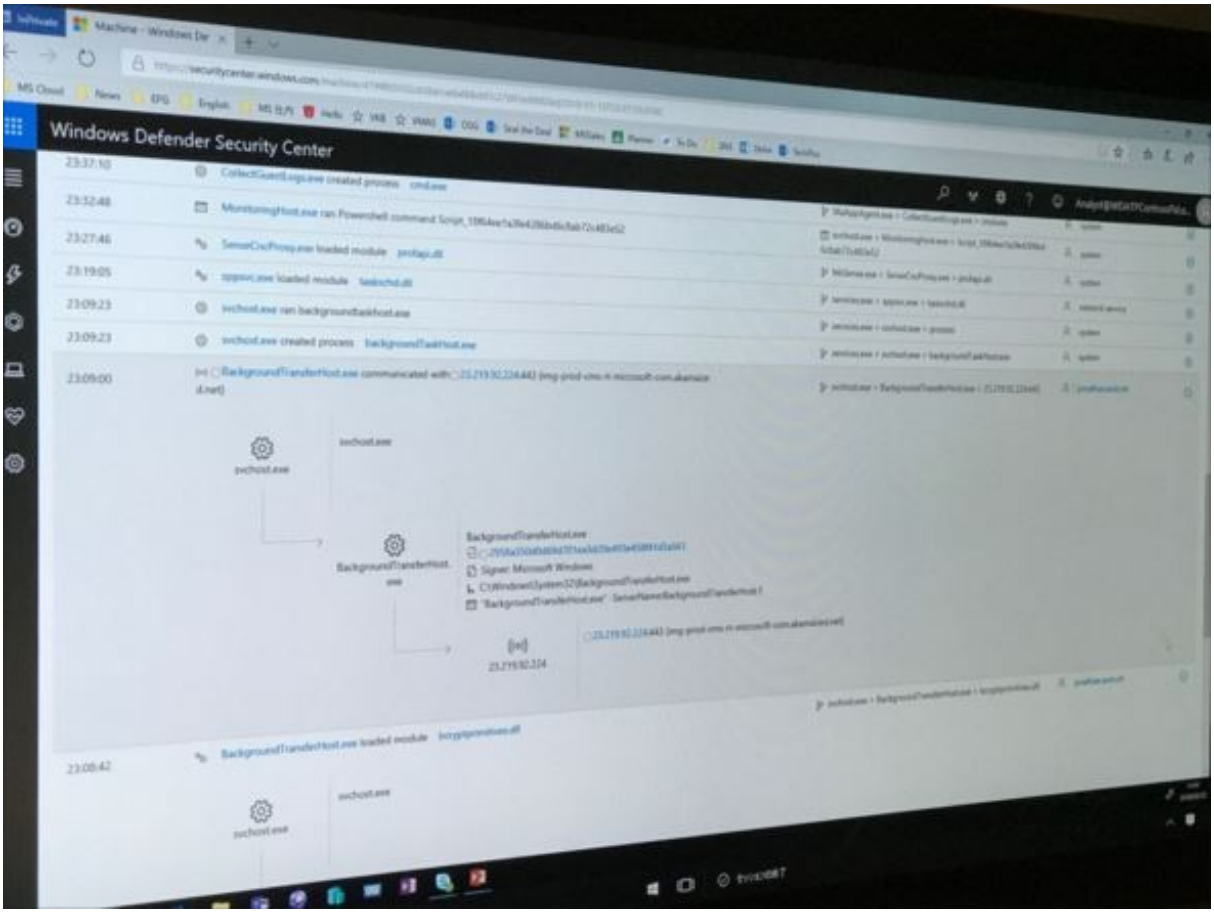
「Windows Defender Security Center」のダッシュボード。ATPの基本画面



アラートが一覧表示されるので、個々の状況を調べていく



個別のマシンの稼働状況を履歴をたどって調べることが可能



感染に至るプロセスの分析の他、怪しいプロセスの稼働状況を調べるのに利用できる

Windows 7／8.1に最新セキュリティ対策製品が提供されるワケ

なお、MicrosoftはWindows 7／8.1にもこのATPを提供すると予告している。一般提供開始の時期は「2018年夏」としており、4月以降にプレビュー版の提供を開始する予定だ。ただし、利用にはWindows 10 Enterprise E5のサブスクリプションが必要となる。つまり、Windows 7／8.1での利用は「ダウングレード権」を行使してのものであり、Windows 10のライセンスを購入しなければならない。

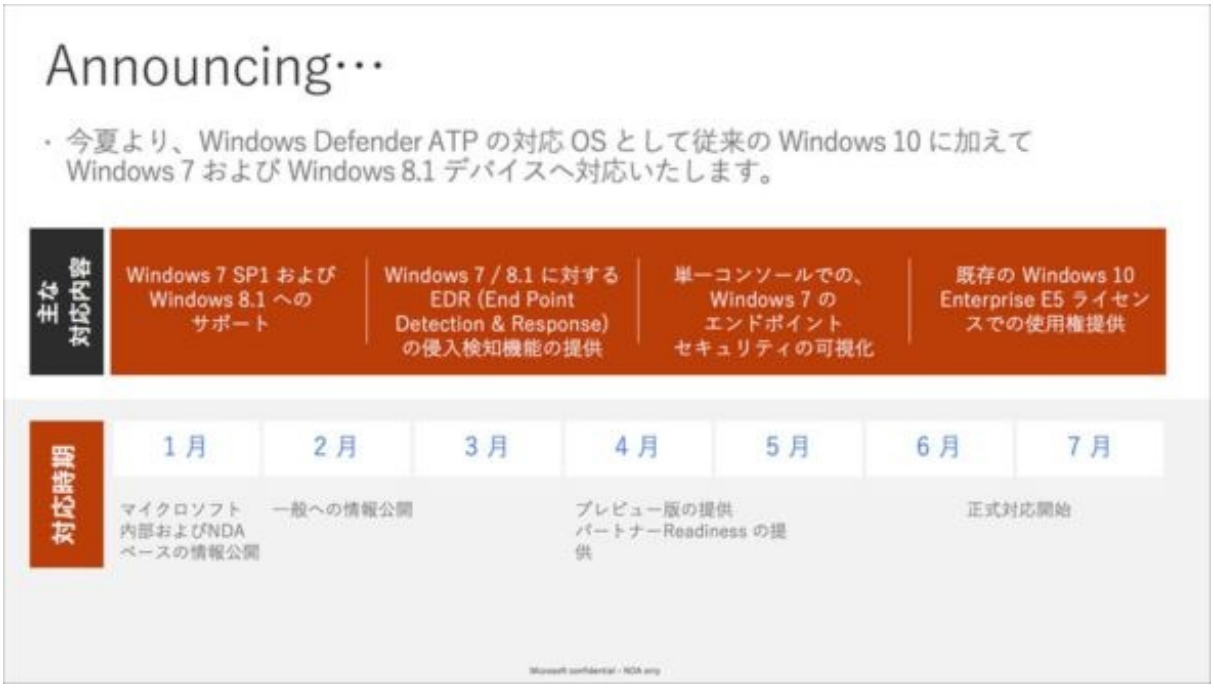
Microsoftとしては「Windows 10への移行までの中継ぎ支援」というスタンスで、機能的にも差別化を行っている。

具体的にはSecurity Center経由でリモートマシンに対して実行可能なコマンドが限定的であり（基本的には監視のみ）、侵入検知や他のマシンへの拡散防止を支援するものとなる。スコアリングのダッシュボードには「Windows 10へのアップグレード状況」が表示され、ATPを通してWindows 10へのアップグレードを促す役割も果たしている。

また、ATPでは標準のWindows Defenderウイルス対策以外にサードパーティー製品との併用が可能だが、Windows 7／8.1でWindows Defenderウイルス対策を利用した場合はクラウド保護などのWindows 10特有の機能が利用できないというデメリットがある。

いずれにせよ「混在環境での中継ぎソリューション」ということで、フル機能が利用できない点には注意したい。

ATPは2018年夏にWindows 7／8.1に対応する



ATPのWindows 7／8.1対応までのタイムライン

ATPのWindows 7／8.1利用における制限事項

Microsoftでは60万台のPCが稼働しており、同社によれば世界で2番目にサイバー攻撃を受けている組織だという（1番は米国防総省）。同社の製品は世界中の組織や個人で利用されており、収集される情報の幅も広い。故に膨大なノウハウが蓄積されており、少なくとも「Microsoftのセキュリティ対策は弱い」と一概にいえるものではないだろう。

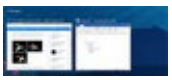
一方で既存の対策ではまだまだ不十分という認識もあり、Windows 10の「Windows as a Service（WaaS）」の仕組みを使ってOS自体のセキュリティ機能を半年ごとにグレードアップさせており、クラウド保護などの機能と合わせて日々強化が続いている。

OS自体の脆弱性も現在進行形で発見されており、最近ではGoogle Project Zeroの研究者であるトーマス・デュリエン氏がWindows Defenderに関する脆弱性を発見したことで、4月初旬にセキュリティ対策パッチが配布された。Microsoft Malware Protection Engineで利用されているRARファイルの解析プログラムに脆弱なオープンソースコード（UnRAR）があったことが原因で、今日もなおこうした問題の対処が続いているわけだ。

「Windows 7などの古いOSではセキュリティ対策が不十分」というのをWindows 10移行の理由に掲げているMicrosoftだが、技術的側面から見ればこれは正しい。「最新のセキュリティ対策は最新製品で」というのはある意味で当然だ。Windows 10への移行がまだならば、Windows Defenderのメリットも含めて検討してみてはいかがだろうか。

関連記事


主役はAIとクラウドへ　5月のMicrosoft開発者イベント「Build 2018」を占う
米Microsoftは5月7日（現地時間）に年次の開発者カンファレンス「Build 2018」を開催する。明らかにされた基調講演のテーマやセッションから、同社の注力ポイントがあらためて分かってきた。


2018年春のWindows 10大型アップデートが完成か　見え始めたRedstoneの終わり
2018年4月に配信が始まる予定のWindows 10次期大型アップデート。いよいよ完成のとき、一昔前

のWindows OSでいえば「RTM（Release To Manufacturing）」の時期が到来したようだ。

「Windows 10 S」を新しい動作モードとして広めようとするMicrosoft
Microsoftの「Windows 10 S」に対するスタンスが変化しつつある。一部には「Windows 10 Sは死んだ」といった論調の報道もあるが、実際は死んだどころか、むしろ特定用途ではメインストリーム製品としてプッシュする勢いで扱いが変わってきているのだ。

企業向けWindows 10のサポート期間がまた延長　大型アップデート配信から2年に
年に2回の大型アップデートを繰り返して機能やセキュリティを強化していくWindows 10。長期運用ではこのサイクルに対応することが求められるが、Microsoftは展開に時間を要する企業向けにサポートポリシーを変更した。

Windows 7から10への移行は進んでいるのか　2020年問題を起こさないために
2020年1月14日のWindows 7延長サポートまであと2年ちょっと。Windows 10への移行はどこまで進んでいるのか、これからどれだけ進むのか。現状と今後の見通しをまとめた。

日本マイクロソフトはOffice 365＋AIで働き方をどう改革したのか
働き方改革のリーディングカンパニーを目指す日本マイクロソフト。自社が提供するツール群を積極的に活用することで、業務の無駄を省き、効率アップを進めている。

Windows 10「Fall Creators Update」のビジネス向け新機能まとめ
「Fall Creators Update」という名称からはイメージしにくいが、この大型アップデートで法人向けのセキュリティ対策や管理機能が強化されている。直近のサポートポリシー変更とともに、まとめて紹介する。

関連リンク

Windows 10 大特集

日本マイクロソフト

ITmedia Inc.