Microsoft 365

教育機関向け

Windows のウイルス対策

日本マイクロソフト株式会社

2020 年 8 月版

本資料についての注意点

- タイミングによっては、最新の情報が反映されていない場合がございます。必要に応じて最新情報をご確認ください。
- 内容を精査しておりますが、一部に「一般企業向け」の情報が含まれている可能性がございます。
- ライセンス部分に関して「教育機関向け」と異なる可能性がございますので、購入検討の際は改めてご確認ください。

Microsoft Defender ウイルス対策

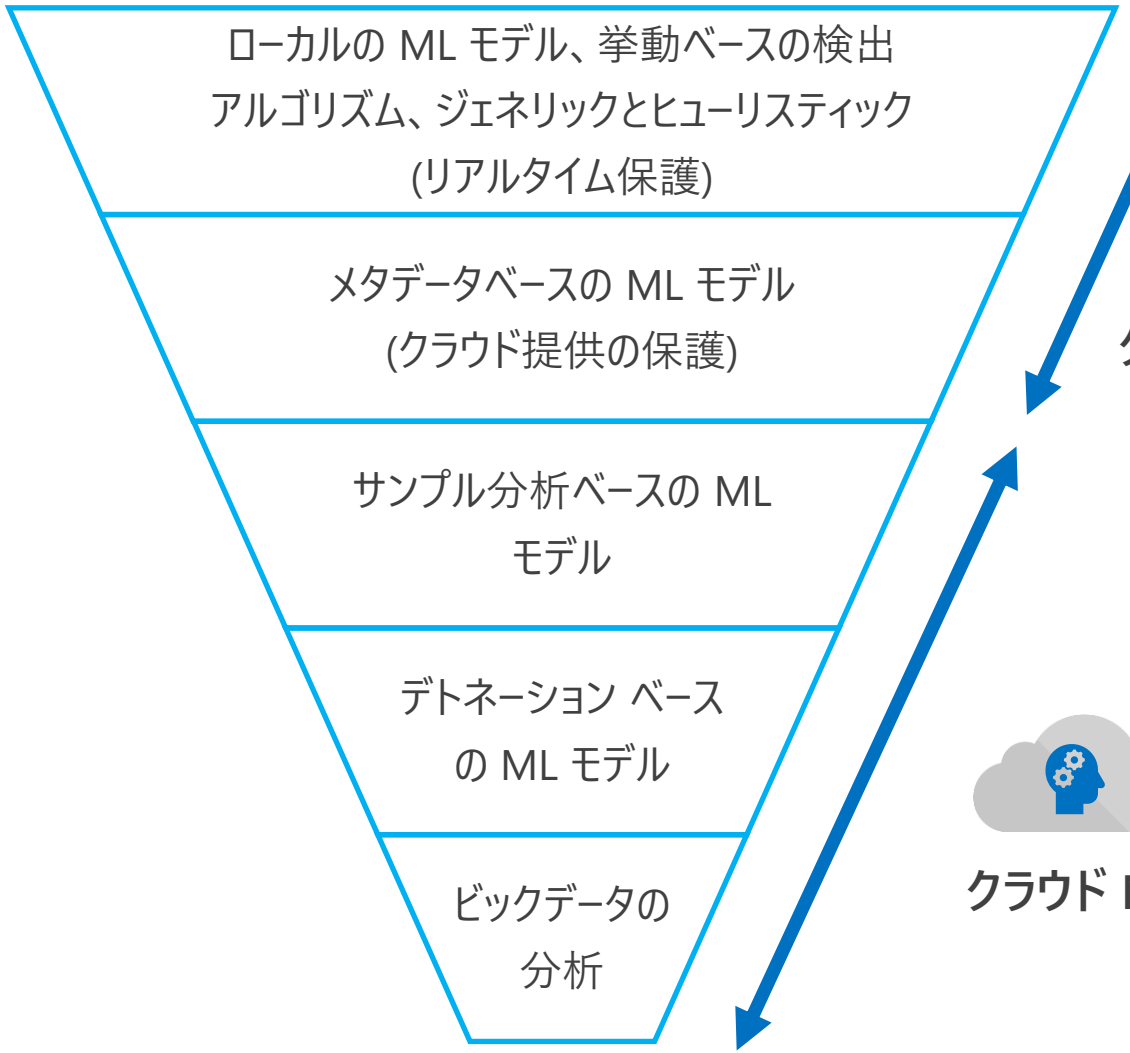
メール、アプリ、クラウド、Web 上のウイルス、マルウェア、スパイウェアなどのソフトウェア脅威に対して、
包括的・継続的に、かつリアルタイムでデバイスを保護

- Windows 10 標準搭載
- 無償利用可能
- 高度な機械学習モデル、および汎用的でヒューリスティックなテクノロジ、クラウド型保護を利用して、未知のウイルスもリアルタイムに検出
- Microsoft 製品のインフラを活用して管理が可能
  ※ 管理製品の使用のためのライセンスは別途必要

Windows 10、Windows Server 2016、Windows Server 2019 での次世代の保護
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-antivirus-in-windows-10

Windows 10 : [Windows セキュリティ] – [ウイルスと脅威の防止]

階層型の機械学習モデルによる防御



クライアント ML

クラウド ML

ミリ秒単位の保護
一般的なマルウェアは高精度の検出機能
リアルタイム保護によってブロック

ミリ秒単位の保護
世界中のクライアントから送信されたメタデータに基づき、
ML を活用したクラウド ルールによって疑わしいファイルをブロック

秒単位の保護
疑わしいファイルのサンプルをアップロード後、
マルチクラス ML分類器によって検査

分の保護
疑わしいファイルをサンドボックス内で実行し、
マルチクラス ML 分類器によって動的に解析

時間単位の保護
ML モデルとエキスパートが作成したルールに基づき、
大規模なセンサーのネットワークシグナルの関連性を発見し、
脅威を自動で分類

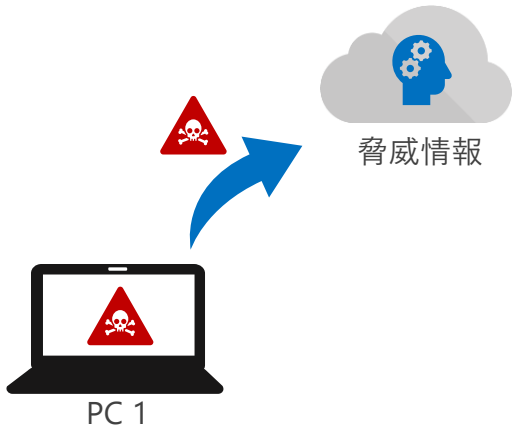
『クラウド配信の保護』機能の動作イメージ

定義ファイルの更新を待たなくてもブロックが可能、感染拡大を防ぐ仕組み

1

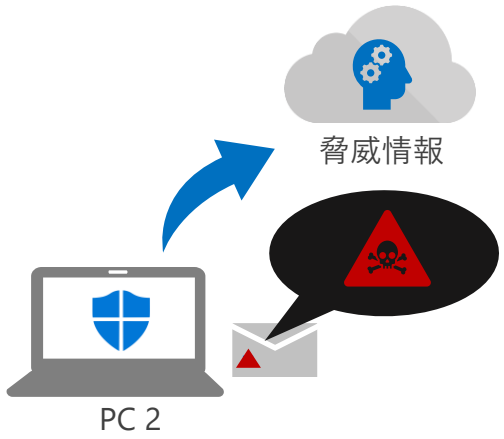
とある PC (PC 1) が
未知のウイルスに感染

2



感染した PC 1 は、自動的に
当該ファイル情報 (ハッシュ値) を
ウイルスとして Microsoft の脅威
情報に報告。

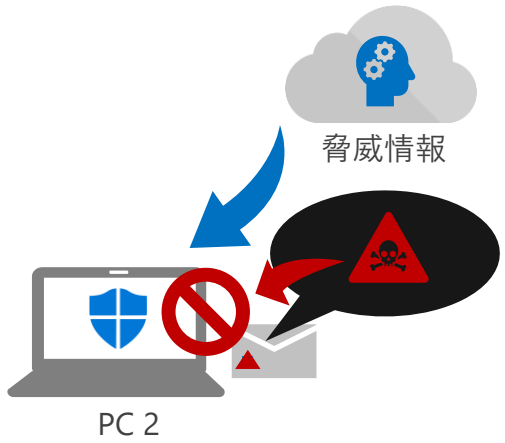
3



その後、別の PC (PC 2) が
同じファイルを受信。

ファイルを開くタイミングで、
最新の脅威情報を確認

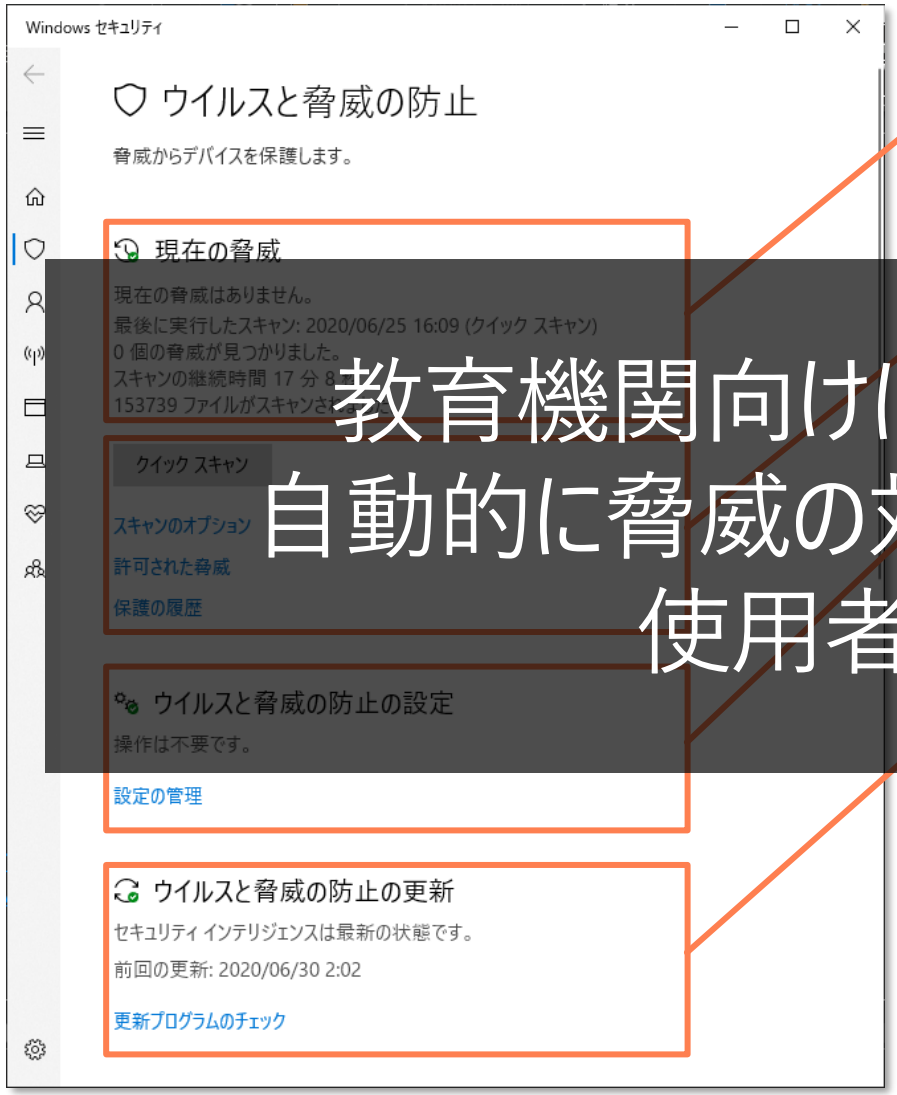
4



PC 1 が報告した情報を基に、
PC 2 は定義の更新をしてなくても
ブロックが可能に。

Microsoft Defender ウイルス対策でクラウド配信の保護を利用して、次世代テクノロジを使用する
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/utilize-microsoft-cloud-protection-microsoft-defender-antivirus

Microsoft Defender ウイルス対策 - ユーザーインタフェース



現在の脅威
検出された脅威の状況や、最後に実行したスキャン状況など

クイックスキャン
ユーザーによる手動実行でのスキャン
オプションによりクイックスキャンやフルスキャンなど選択可能

ウイルスと脅威の防止の設定
リアルタイム保護、クラウド提供の保護、機能の有効
サンプルの自動送信のオン / オフの設定など

ウイルスと脅威の防止の更新
セキュリティ インテリジェンス (定義の更新) の更新状況
最新の更新プログラムのチェック

教育機関向けに関しては、既定で UI は非表示
自動的に脅威の対処・駆除、自動的に更新を実施
使用者は特に操作の必要なし

Windows セキュリティアプリの Microsoft Defender ウイルス対策
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-security-center-antivirus

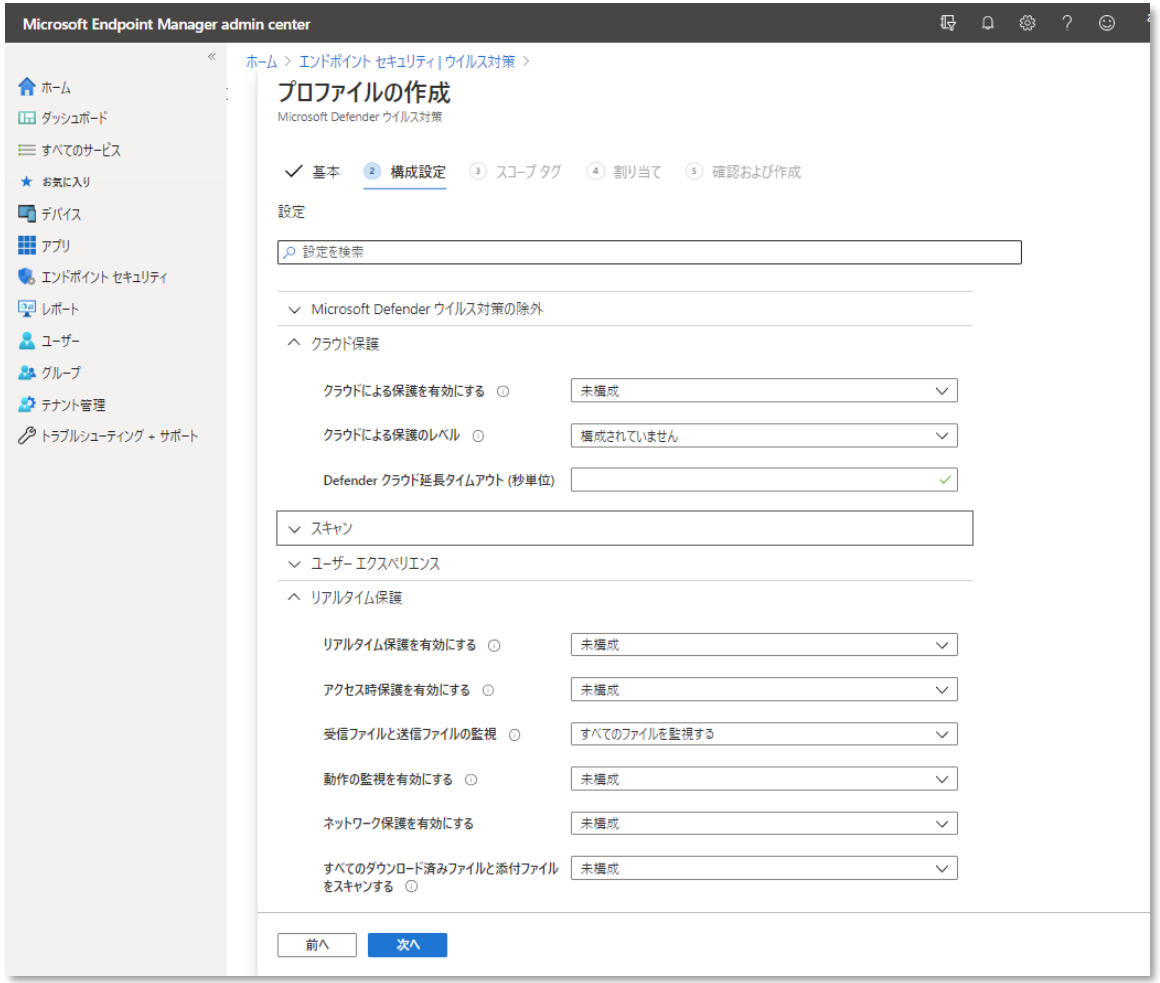
Microsoft Defender ウイルス対策の優位性

Windows 標準搭載
Windows OS に搭載されており、OS バージョンアップなどの互換性の問題が不要。パフォーマンスも最適化

最新のテクノロジーの活用
次世代型アンチウイルスとして、機械学習モデルや、定義ファイルの更新に頼らない「クラウド保護機能」などの最新技術を利用

膨大なセキュリティのビックデータの活用
Microsoft が保有する世界中のシグナルから得られるデータを活用したセキュリティ インテリジェンスによる最新の脅威からの保護

Microsoft 製品連携
既存の Microsoft 製品のインフラの活用が可能。AD のグループポリシーや、PC 管理製品 (Configuration Manager, intune) を介しての設定、Defender ATP を利用した監視も可能。



Intune の管理画面からの Microsoft Defender ウイルス対策の設定

Microsoft Defender ウイルスの最小要件

最小ハードウェア要件

- 各 OS の最小ハードウェア要件

サポート OS

- Windows 8.1, 10 各種エディション
- Windows Server 2016, 2019

※ Windows 7 に関しては、コンシューマー向けに “Microsoft Security Essentials” を提供。企業向けには “Configuration Manager Endpoint Protection” として提供 (要ライセンス)

※ Windows Server 2008 R2, 2012 R2に関しては、”Configuration Manager Endpoint Protection” として提供 (要ライセンス)

※ Linux, macOS は Defender ATP にて AV 機能も提供 (要 Defender ATP ライセンス)

※ Android, iOS は Defender ATP にて AV 機能も提供予定 (要 Defender ATP ライセンス)

Windows 10 では既定で Microsoft Defender ウイルス対策による保護が有効

Microsoft 365

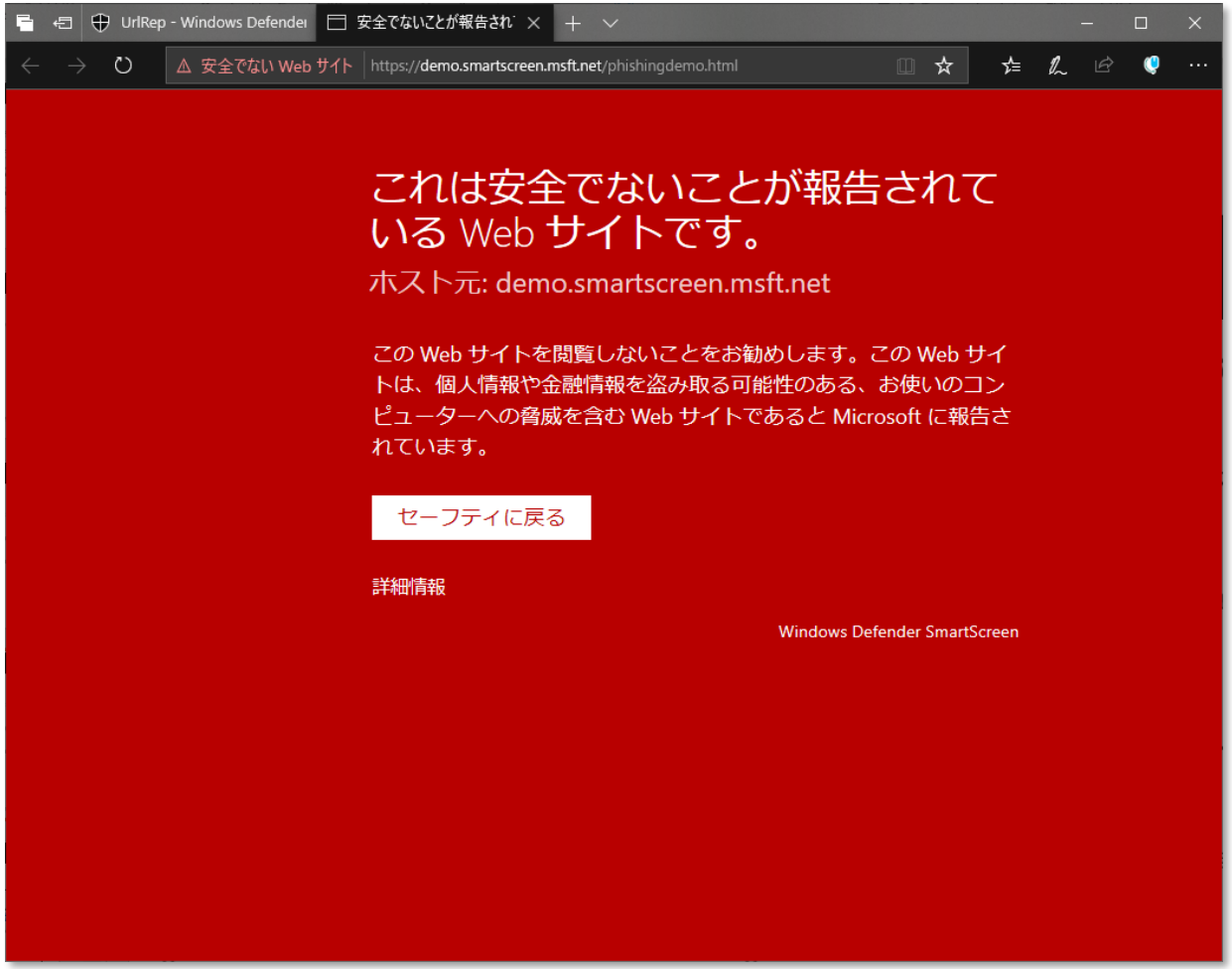
Microsoft Defender ウイルス対策以外の Windows セキュリティ製品

Microsoft Defender SmartScreen

報告されているフィッシング詐欺サイトおよび
悪意のあるサイトを動的な一覧と照合し、警告を表示
Intune で設定の管理が可能

- Windows 10 標準搭載
- 無償利用可能
- 不正な Web サイトからの保護
- 不正な Web サイトからダウンロードされたファイルをブロック

Windows Defender SmartScreen
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview



Microsoft Defender SmartScreen で Web サイトをブロックした様子

Microsoft Defender ファイアウォール

Windows に標準搭載されたパーソナルファイアウォール
Intune で設定の管理が可能

- Windows 10 標準搭載
- 無償利用可能
- 不正な通信からのブロック
  (送受信、プログラム、ポート、IP アドレス等)
- プロファイルごとに設定が可能
  (ドメイン、プライベート、パブリック)

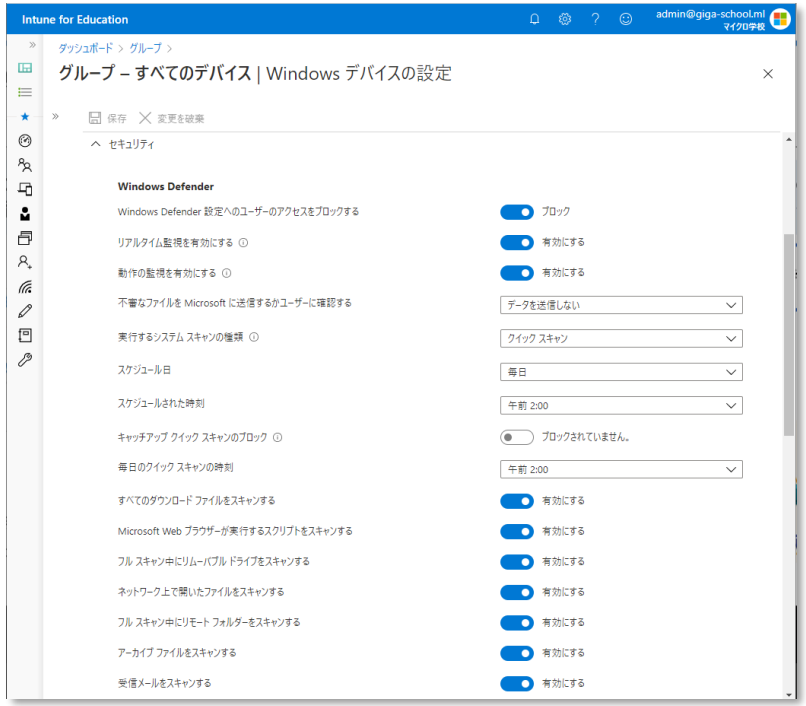
セキュリティが強化された Windows Defender ファイアウォール
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

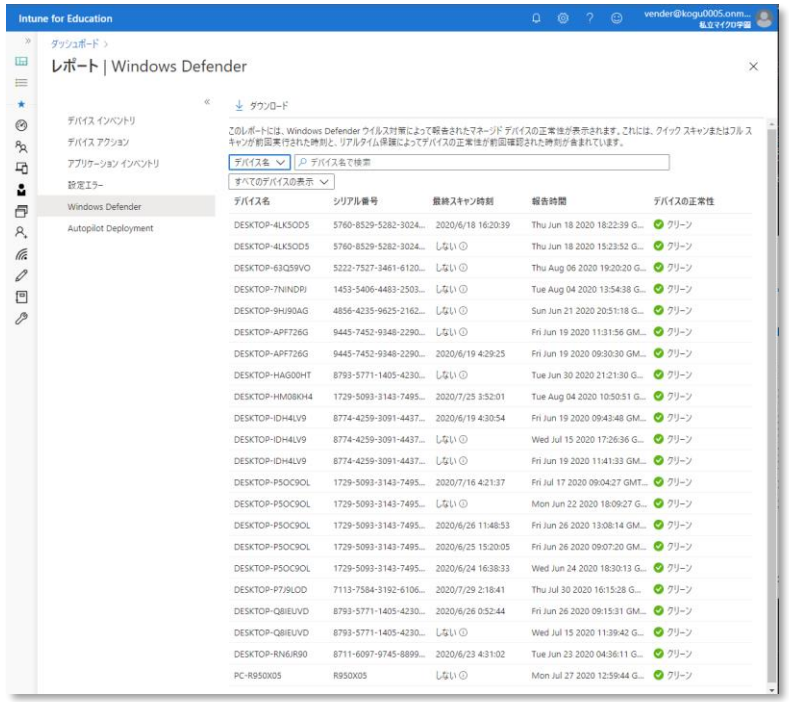
Windows 10 : [Windows セキュリティ] – [ファイアウォールとネットワーク保護]

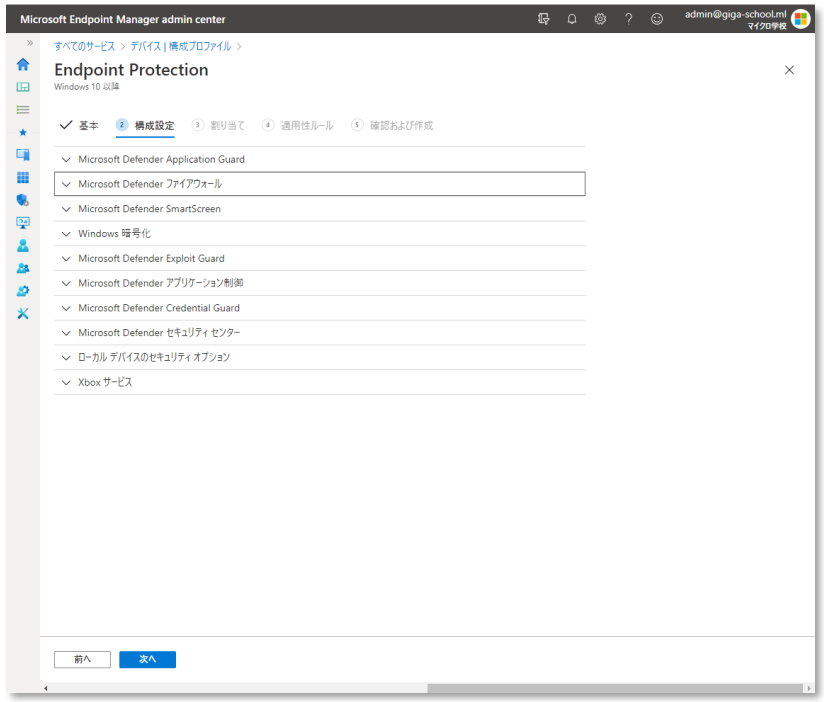
Microsoft 365

Intune for Education による Microsoft Defender ウイルス対策の管理

Intune for Education によるセキュリティ管理







Intune for Education でのセキュリティ設定

Microsoft Defender ウイルス対策や
Microsoft Defender SmartScreen の設定は
Intune の管理コンソールから設定が可能

Intune for Education のレポート

Microsoft Defender ウイルス対策の
現状の確認は Intune のレポートより確認可能

※ 過去のそれぞれの端末のウイルス感染状況の確認や、
ウイルス感染時のメール通知などが必要な場合には、
別途製品 (Microsoft Defender ATP 等) が必要となります。

Microsoft Endpoint Manager での設定

Microsoft Endpoint Manager Admin Center
から intune の設定を実施することにより、
Intune for Education のメニューには表示されない、
より詳細な設定を行うことが可能

Intune (Microsoft Endpoint Manager) による管理

Intune for Education より詳細な設定や確認が必要な場合は Intune のコンソールから設定が可能

脅威エージェントの状態
Defender ウイルス対策のリアルタイム保護の状況や AV エンジンや定義のバージョンなどの詳細ステータスを確認することが可能

⚠ 注意：アラートについて

Defender ウイルス対策により「ウイルスを検知した」という旨のアラートの情報の出力やそれをメール通知するといった機能は Intune にはありません。
Education においては、各端末で自動対処・駆除までが想定されています。
もし、アラートを監視したいなどのさらなる要望には、Microsoft Defender ATP をご検討いただいています。

Intune の管理画面 [デバイス] – [モニター] – [脅威エージェントの状態]

Microsoft 365

参考資料 1
Microsoft Defender ウイルス対策の実績

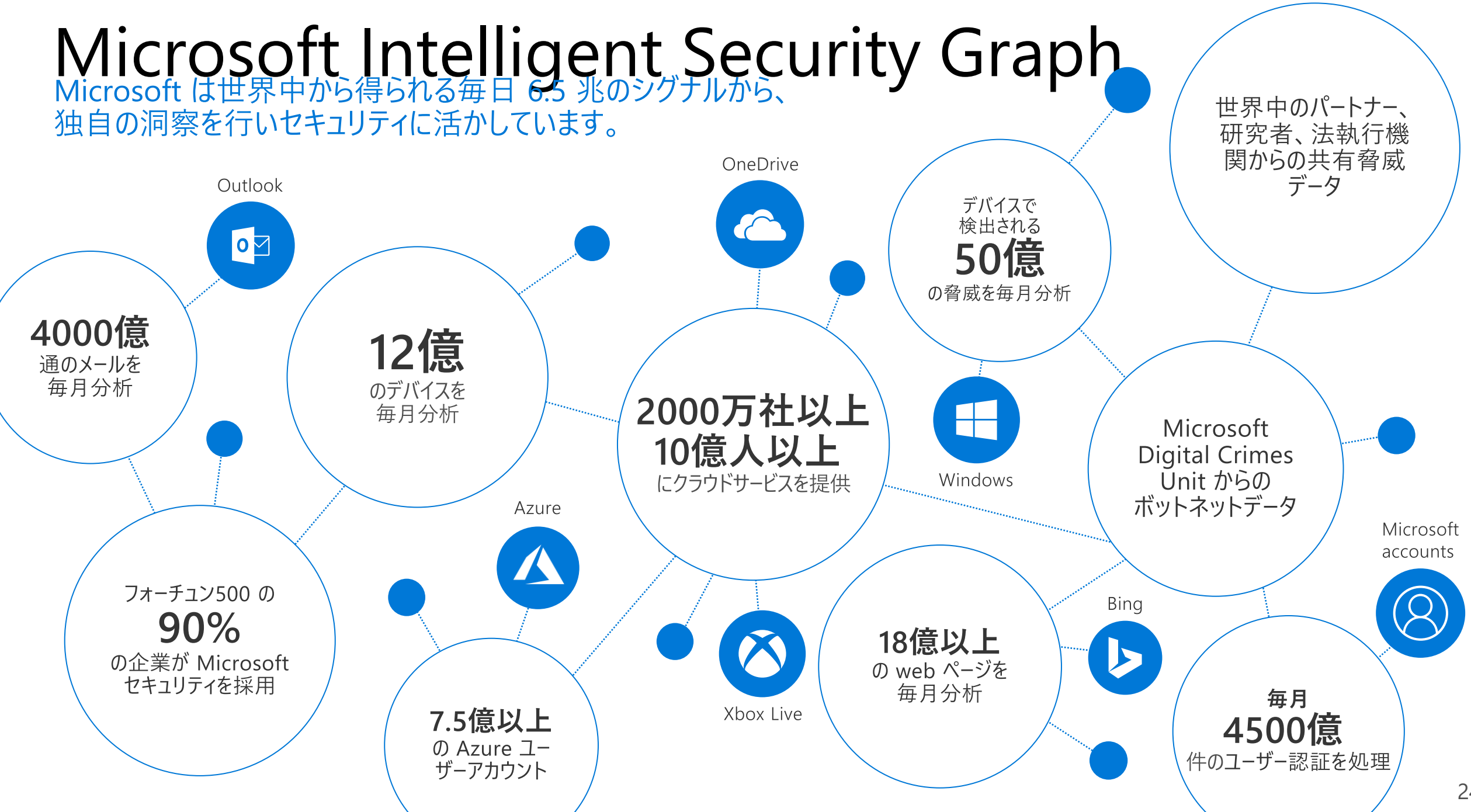
セキュリティへの年間の研究開発投資

1100 億円

Microsoft セキュリティは世界中の
お客様を守るのに役立っています

Microsoft Intelligent Security Graph

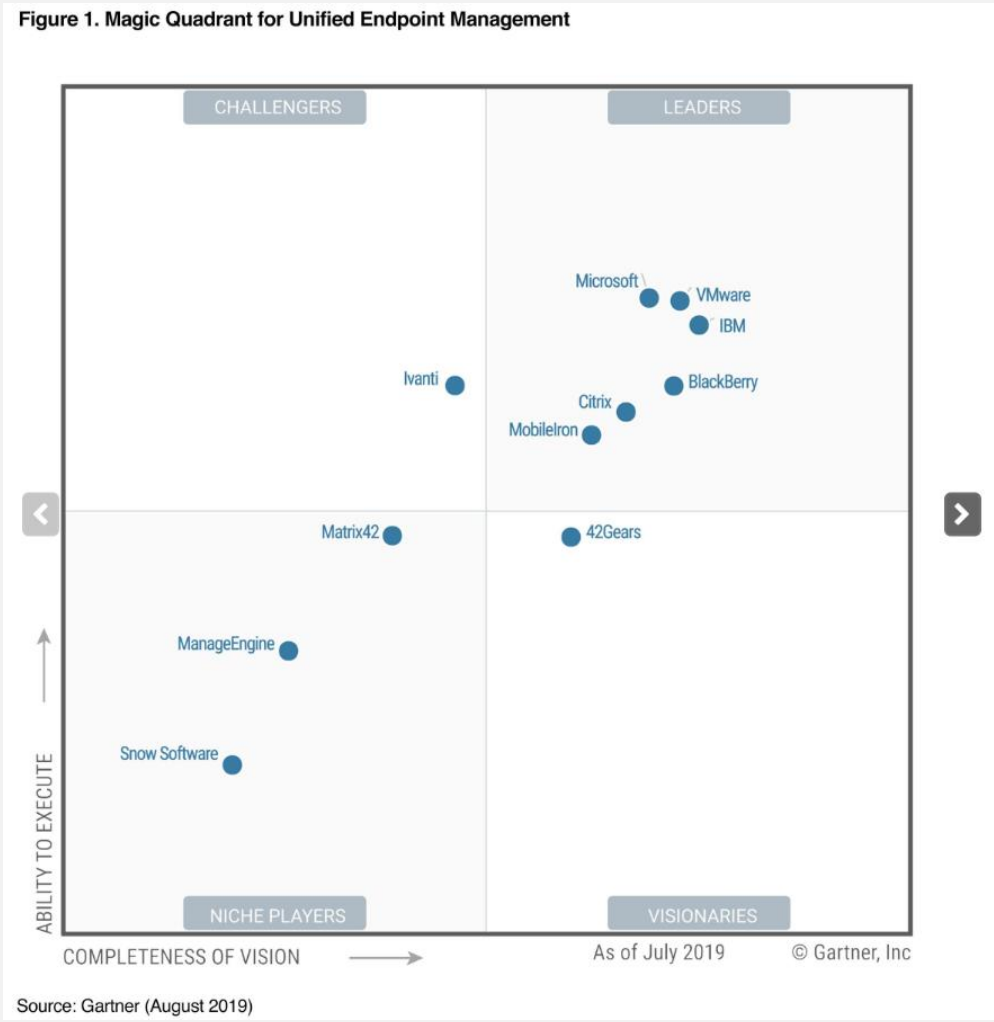
Microsoft は世界中から得られる毎日 6.5 兆のシグナルから、
独自の洞察を行いセキュリティに活かしています。



Gartner Magic Quadrants for Endpoint Security & Mgt

Whitepaper - [Modern management and security principles driving our Microsoft Endpoint Manager vision]

[Magic Quadrant for Endpoint Protection Platforms - August 2019]

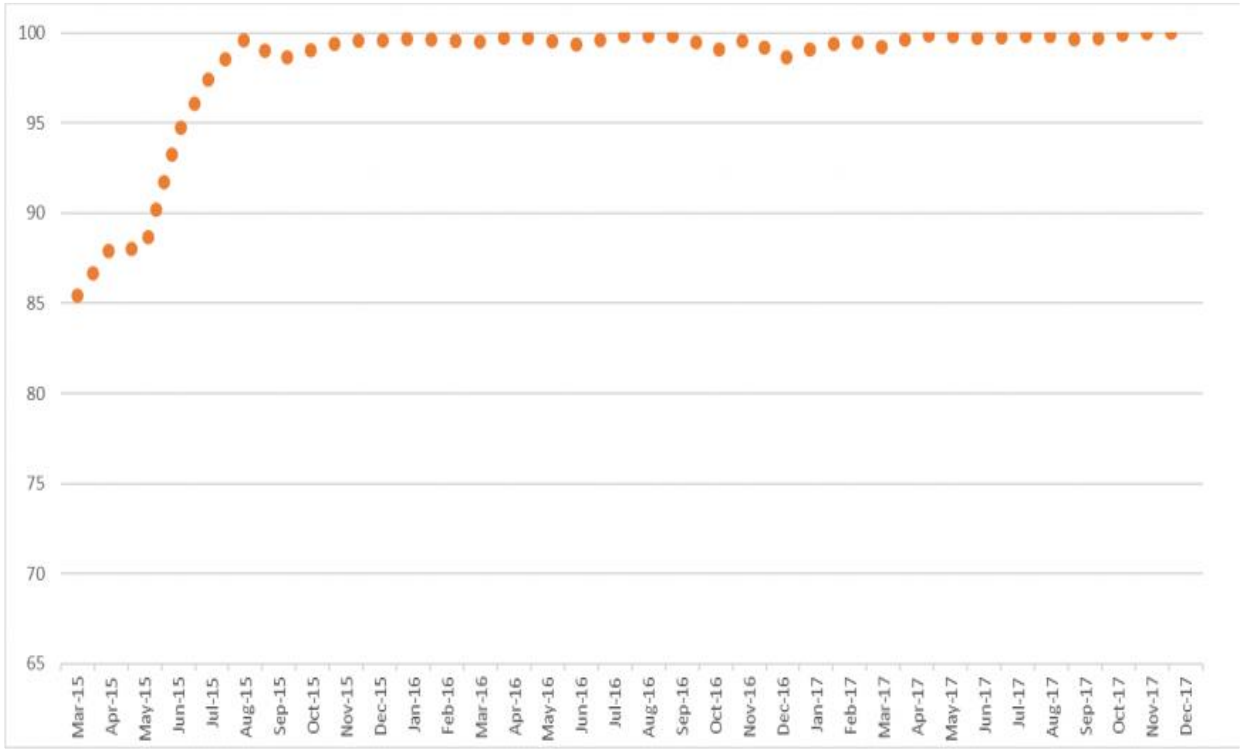


[Magic Quadrant for Unified Endpoint Management - August 2019]

Microsoft Defender ウイルス対策の第三者機関の評価

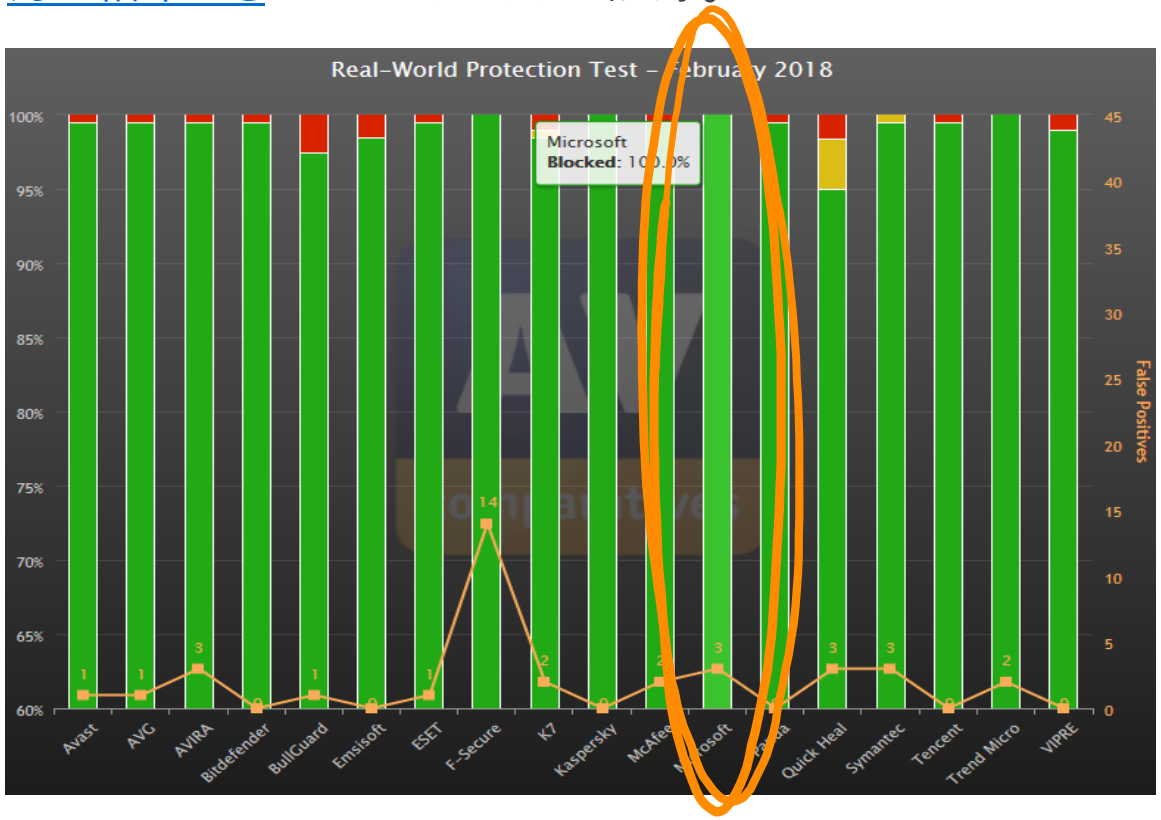
AV-TEST

2015 年 3 月よりスコアが急速に上昇。**2015 年 8 月には 100 %を達成。**それ以来一貫して高スコアを維持。



AV-Comparatives

5 ヶ月連続してマルウェアサンプルをすべて検出。2018 年 2 月の結果でも 100 % ブロックを記録。



Microsoft Defender ウイルス対策の企業環境でのシェア

Windows 10

50% 以上

Windows 10 デバイスのうち、法人の 50% 以上が
Microsoft Defender ウイルス対策を使用しています。

Windows 7

Windows 8

18% 以上

Windows 7 / 8 のデバイスのうち、18 % 以上が
Windows Defender ウイルス対策を使用しています。

Why Windows Defender Antivirus is the most deployed in the enterprise
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/22/why-windows-defender-antivirus-is-the-most-deployed-in-the-enterprise/

日本の法人企業での代表的な採用理由

業種	事業内容	PC 台数
卸売 / 小売	総合小売	45,000 台
	情報、エネルギー、金属	15,000 台
	衣類	2,200 台
金融 / 保険	銀行・信託	20,000 台
	生命保険	23,000 台
	損害保険	40,000 台
	その他	16,000 台
輸送用機器	自動車	100,000 台
	自動車	12,000 台
電気機器	半導体	20,000 台
	デジタルプロダクツ	200,000 台
石油・石炭	石油精製販売事業	22,000 台
	石油製品	10,000 台
情報通信	通信	50,000 台
	IT	10,000 台
	ゲーム	4,000 台
陸運	旅客	9,000 台
公共	大学	2,000 台

よくある採用理由

コスト削減

Windows 10 導入の**タイミングでライセンスや**
インフラコスト削減のために他社製ウイルス対策から
乗り換え

運用面での負荷

Windows セキュリティ製品の**バージョンマッチングや**
検証負荷の削減。
OS 標準機能を利用することによる**展開・配布・管理**
の工数を削減

信頼性

MS が保有する様々なデータ、長期間にわたる
Windows Defender の実績や他社事例、
実際に評価を実施した結果から採用

Microsoft 365

参考資料 2
Windows 10 機能マトリクス

Windows 10

エディションによる機能の比較

		Pro Education	Education A3	Education A5
管理と展開				
モバイル デバイス管理 (MDM)	持ち出し端末の管理方法	●	●	●
ドメイン参加、Azure Active Directory 参加	オンプレミス AD や Azure AD に参加し、ID を管理	●	●	●
モバイル アプリケーション管理 (MAM)	アプリの分離やデータの保護	●	●	●
ビジネス向け Microsoft ストア	自社独自のアプリ管理、配布	●	●	●
管理されたユーザー エクスペリエンス	スタートやタスク バーのカスタマイズと管理	●	●	●
Microsoft ストア アクセス管理	Microsoft ストアの利用制限やプライベート ストアのみの提供		●	●
コンシューマー エクスペリエンス管理	Microsoft からのおすすめ情報やコンシューマー向けアプリのインストール制御		●	●
Cortana 管理	Cortana の利用制限		●	●
Microsoft 動的管理	条件に応じて適用ポリシーを動的に変化		●	●
ロックダウン機能	ディスクへの書き込み制限等、デバイスの利用制限		●	●
高度なテレメトリー制御	アプリのクラッシュ情報などの送信を制限		●	●
AppLocker	ホワイト リスト/ブラック リストによるアプリの起動制限		●	●
BranchCache	ネットワーク データをキャッシュし、ネットワーク トラフィックを削減		●	●
Microsoft Application Virtualization (App-V)	アプリのカプセル化、アプリの異なるバージョンを管理する		●	●
Microsoft User Environment Virtualization (UE-V)	OSやアプリケーションのユーザー設定を複数デバイス間で同期		●	●
分析とサービスのサポート				
Desktop Analytics	アプリやドライバーの互換性情報と移行支援、更新プログラム適用状況の可視化		●	●
Windows Update for Business	Windows Update からの更新適用タイミングを制御	●	●	●

Windows 10 エディションによる機能の比較

		Pro Education	Education A3	Education A5
セキュリティと識別情報				
Windows Hello / Windows Hello for Business	顔や指紋などによる生体認証	●	●	●
BitLocker / BitLocker to Go	内蔵ディスクや外付けディスクの暗号化	●	●	●
Windows Information Protection	端末内のアプリやデータを分離/暗号化し、企業データの持ち出しを防ぐ	●	●	●
Microsoft Defender ウイルス対策	企業利用レベルのウィルス対策、クラウドを活用したゼロデイ攻撃対策	●	●	●
Microsoft Defender Exploit Guard	未知の攻撃に対する緩和策やランサムウェア対策	○ ※1	○ ※1	●
Microsoft Defender Device Guard	端末起動時からのデバイス保護やホワイトリストベースのアプリケーション制御		●	●
Microsoft Defender Credential Guard	資格情報を別のマイクロ OS に格納し、標的型攻撃から対抗		●	●
Microsoft Defender Application Guard	Web ブラウザーを仮想化し、端末内でインターネット分離を実現	○ ※2	●	●
Microsoft Defender ATP	エンドポイントの予防的な保護、ふるまい検知、自動化された調査と対応			●
Software Assurance 特典				
将来と過去の LTSCs バージョン利用	10 年 OS 固定化モデル		●	●
サービシングモデルの混在（SAC / LTSC）	LTSC は Enterprise のみの使用権利		●	●
MBAM, AGPM, DART	BitLocker の管理ツール、GPO の承認ワークフロー、診断修復ツール		●	●
仮想化の権利	シンクラ用途のアクセス権		●	●
24x7 延長ホットフィックスサポート	Microsoft のサポートの使用権		●	●
トレーニングバウチャーとe-learning	トレーニングの利用権		●	●

Network Protection　Attack Surface Reduction

Enterprise Mode (URL による自動切り替え機能) や最新機能

エンドポイントの多層防御

必要な対策例	とある構成例	Windows 10
不審な挙動の検知 (EDR for IOA)	- なし –	Microsoft Defender ATP
高度な攻撃の検知 (EDR for IOC)	C 社 (8,000円前後*)	Microsoft Defender ATP
脆弱性/マクロ悪用対策/ ネットワーク保護	- なし -	Windows Defender Exploit Guard
未知のマルウェア検知 (Reputation Check)	B 社 (約2,500～12,000円*)	Windows Defender ウイルス対策 Windows Defender Smart Screen
既知のマルウェア検知 (Antivirus Scan)	A 社 (1,000円前後*)	Windows Defender ウイルス対策
資格情報の保護	- なし -	Windows Defender Credential Guard
HDD 暗号化	D 社 (3,000円前後*)	BitLocker
ブートレコード保護	- なし -	Windows Defender Device Guard

Microsoft 365