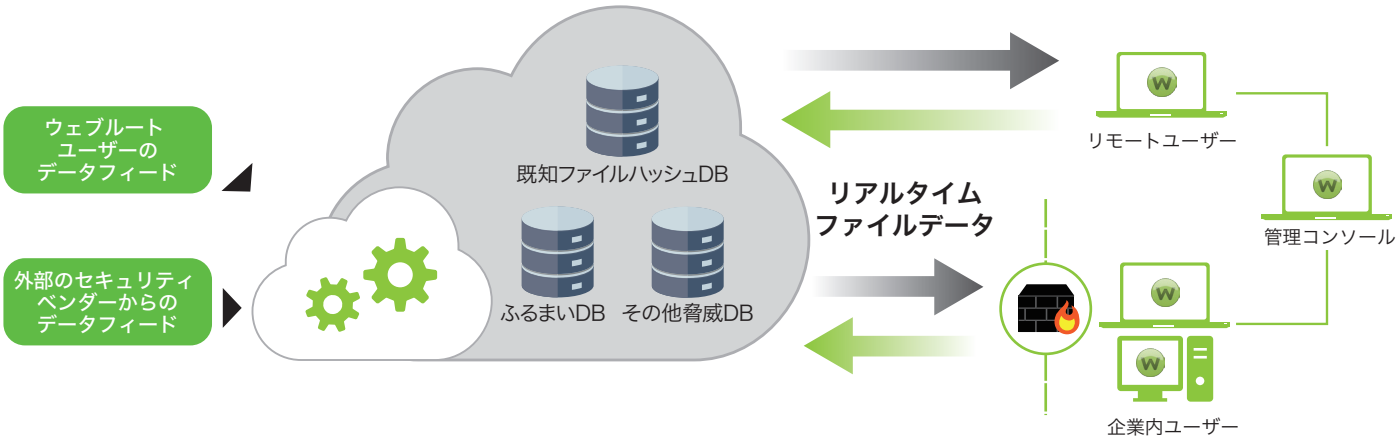
WEBROOT® SecureAnywhere

ビジネスエンドポイントプロテクション

Webroot SecureAnywhere Business エンドポイント プロテクションは、エンドポイントにおけるマルウェア防御の革新的なアプローチを提供します。ウェブルートの機械学習（AI）を用いたクラウド技術を活用し、他のアプローチに比べて、より効果的に既知の脅威に対応し、またゼロデイ攻撃を防止します。
エンドポイントにおけるスキャンは、脅威のスピードを実現するとともに、エンドユーザーのパフォーマンスの低下を防ぎます。リアルタイムなテクノロジーであるため、利用者のセキュリティ環境は常時最新状態に保たれ、定義ファイルの更新管理に煩わされることなく、あらゆる最新の脅威や攻撃から保護されます。

脅威情報インテリジェンスプラットフォーム

- ウェブルートの脅威情報インテリジェンスは、クラウド上に構築されたセキュリティ情報のデータベースです。マルウェアやウイルス、悪質なサイトのURL、IPアドレスなどの様々な膨大な情報をリアルタイムに自動的に収集しています。
- 収集された情報は、最先端のアルゴリズムに基づく機械学習や振る舞い分析により解析・分類されます。そのため分析結果の精度が人手による分析よりも高く大量の情報をごくわずかな時間で分析します。さらに異なる要素のデータを相関分析することにより、予測型のインテリジェンスを提供します。ウェブルートは、蓄積された脅威の情報を各セキュリティベンダー様に提供しており、脅威情報のフィードバックをいただくことにより、より精度の高いデータベースを構築しています。
- 脅威の情報は全てクラウド上にあります。世界のどこかにある1台のPCで悪意のあるファイルが新たに発見されるとその情報はただちにクラウド上のデータベースに反映されます。そして他のユーザーのPCもその瞬間に新たな脅威から保護されます。



ウェブルートが日々監視している項目

URLs	ドメイン	IPアドレス	ファイルの振る舞いレコード	モバイルアプリ	Connected Sensors
320億+	7.5億+	40億+	310億+	6千万+	6千万+

1日に検出される脅威の数

25,000 悪意のあるURL	100万 新しいファイル	
10万 新しいマルウェア	6,000 フィッシングサイト	10万 悪意のあるIP

サービスの特徴

フルクラウド型の次世代セキュリティ
定義ファイルが不要のハッシュベースのクラウド型のシステムを採用、リアルタイムに最新の保護を提供します。定義ファイルの更新の必要がないため、見つかったばかりのマルウェアも即座にすべてのエンドポイントで対応することが可能です。

自動化により管理も容易に
クライアントエージェントをインストールしたすべてのエンドポイントを集中管理。SaaS型のセキュリティ管理と報告システムにより、サーバー用のハードウェアの導入や別ソフトウェアの導入など煩わしい管理が不要になります。

未知のマルウェアに対する最大限の防御
革新的なファイル形式&行動認証テクノロジーを採用。未知のマルウェアに対しても、行動を監視し、分析することで対応することが可能です。黒判定された際には、即座にクラウドのデータベースが更新され、他のユーザーにも展開されます。

社内ネットワーク外のユーザーも保護
ネットワークの処理能力を低下させる大容量のアップデートファイルが不要。社内ネットワークに未接続のユーザーもアップデートも不要で新しい脅威に対し全てのユーザーを直ちに保護します。

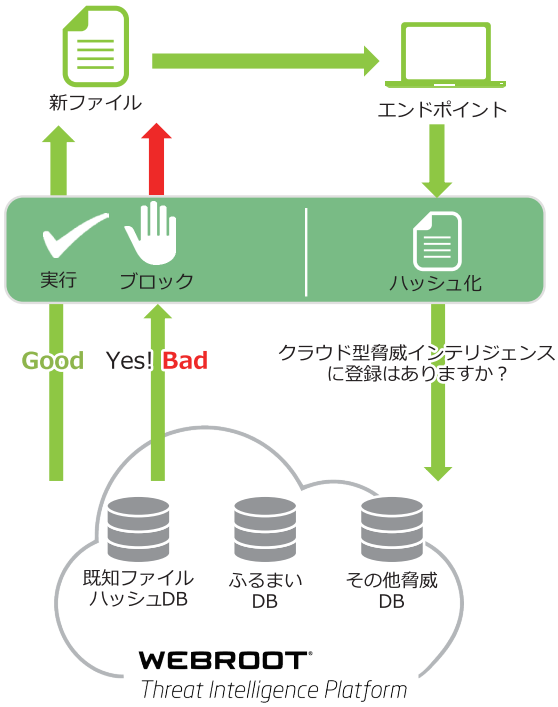
PCのスローダウンや生産性の低下からの解放
初回のスキャンは数分以内、その後のスキャンはさらに短縮されます。スキャン中のCPUの使用は最初限で、PCのパフォーマンスの低下を防ぎます。

超高速で手軽な配備が可能
業界最小クラスのエンドポイントセキュリティクライアント／エージェント（3MB）により、インストール時の所要時間は通常数十秒以内と高速。他社製品との共存も可能です。

多層防御／リアルタイムアンチフィッシング
ウェブルートはエンドユーザーの端末を多層的に防御しています。リアルタイムに悪意のあるサイトから守るために、URLチェックを実施し悪意のあるサイトからの攻撃を防ぎます。また、実行ファイルベースのファイルスキャンが最終的にクライアントで悪意のある行為が行われることを防ぎます。

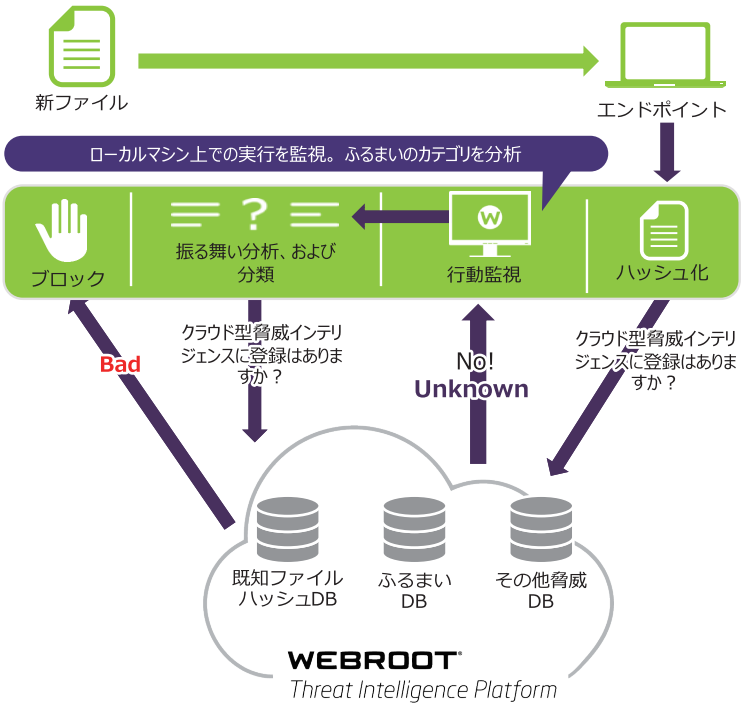
リアルタイム脅威モニタリング

静的判定



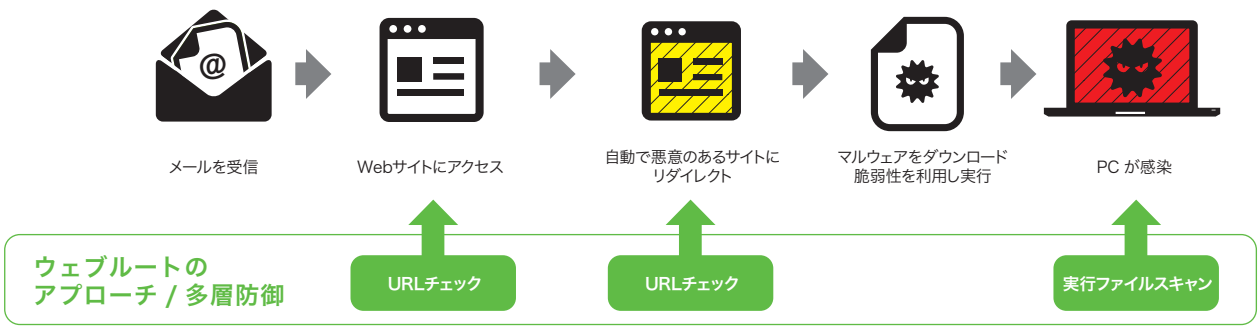
ローカルのエンドポイントからファイルのハッシュ値をクラウドに送り、そのハッシュ値がウェブルートのデータベースにあるかどうかを確認します。
その結果、ファイルを実行させるかもしくはブロックするかの判定をローカルにフィードバックします。
端末でファイルの白黒の判定を行わないので、PCのパフォーマンスへの影響は最小限です。

動的判定



ローカルのエンドポイントからファイルのハッシュ値をクラウドに送り、ウェブルートのデータベースになかった場合は、ローカルマシン上でそのファイルの動作を監視・記録します。
振る舞いを分析し、その振る舞いが黒と判定された時点で、ブロックを実施し、その行動の履歴に基づき、ファイルが行った変更を元に戻します。未知の脅威への対策に非常に大きな効果があります。

＜Web サイトからの感染例＞

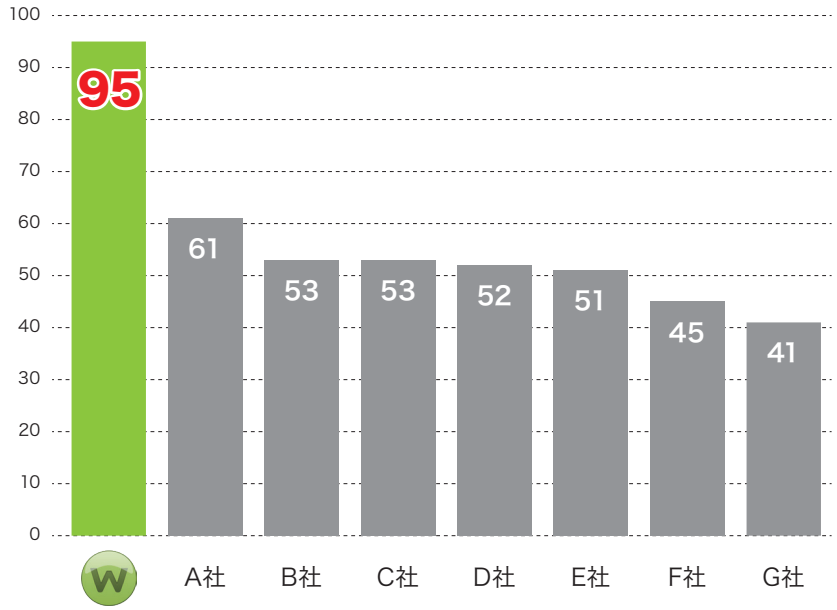


従来型製品の問題点に対するウェブルートのアプローチ

	従来型アンチウイルス製品の問題	Webrootのアプローチ
管理者	サーバー等のオンサイトでの運用インフラストラクチャが必要	SaaS型のクラウドコンソールを標準で提供
管理者	すべてのユーザに定義ファイルを配布するのに時間がかかる	定義ファイルの配布は不要で、常に最新の保護を提供
管理者	社内LANの外にいると端末状態の把握が出来ない	ロケーションフリーで全ての端末の状態把握が可能
管理者	製品の展開(インストール)に時間がかかる	インストール時間はたった数十秒・初期スキャンも数分で完了
管理者	インストール・モジュール (数十～数百 MB)が大きすぎる	インストールモジュールはわずか3MB強
管理者	サポート依頼時に対応に時間がかかる	製品内サポート機能(チケット)を使用することで、迅速な対応が可能
エンドユーザー	スキャン時にPCに負担がかかり、作業の生産性が低下している	超高速で、パフォーマンスにインパクトの無いスキャン
エンドユーザー	常に新しい定義ファイルを取得して、端末に適用する必要がある	定義ファイルを使わず、クラウドの脅威情報をベースにしたハッシュ検知を利用し、リアルタイムに保護を提供
エンドユーザー	ゼロデイ脅威などにはシグネチャベースでは対応ができない	シグネチャは不要で、ビヘイビアベースにより新しい攻撃の検出
エンドユーザー	基本的に自社の脅威情報をベースにマルウェアに対抗している	グローバルセキュリティ／ネットワークベンダー約100社と脅威情報の共有
エンドユーザー	新しい脅威の検出から全てユーザのアップデートに2週間かかる	新しいマルウェアを特定したあと、すべての顧客をリアルタイムで保護

パフォーマンス比較

最終スコア



パフォーマンス結果測定

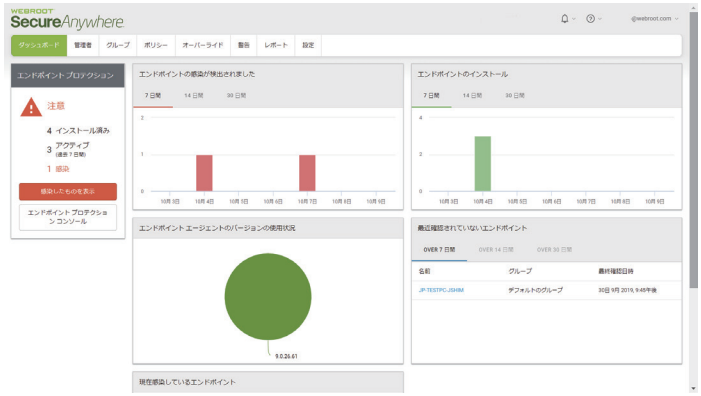
起動時間	1位
ブラウズ時間	1位
アイドル時のCPU利用量	3位
スキャン時のCPU利用量	5位
ファイルの圧縮／解凍	1位
ファイルのコピー/移動/削除	1位
ファイルの書き込み、ファイルを開く、ファイルを閉じる	1位
インストール サイズ	1位
インストール時間	1位
最初のスキャン実行時のメモリ使用量	1位
予約スキャン実行時のメモリ使用量	1位
システム アイドル時のメモリ使用量	1位
ネットワークのスループット	1位
予約スキャン実行時間	1位

WEBROOT

ダウンロード先 :https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/4914/9944/0155/Webroot_SecureAnywhere_Business_vs_Competitors_2017_JP.pdf

管理コンソール

Webベースの管理コンソール1つで、全てのエンドポイントの集中管理が可能です。
直感的なインターフェースを利用したエンドユーザーのポリシー管理が容易に行えます。



- 管理サーバのハードウェアやソフトウェアの購入・インストール保守は不要です。
- セキュリティポリシーの策定・管理をグループ単位で実施可能です。
- ホワイトリスト/ブラックリストやオーバーライドファイルの管理が一つのコンソールで可能です。
- 発生したばかりの脅威に対する対応やエージェントのアップデートは自動で行われます。

製品トライアル / 移行

エンドポイントにインストールされている他のセキュリティ製品と競合しないので、トライアルや移行に際して既存のソフトウェアのアンインストールが不要です。並行して手軽に配備、インストールが行えます。

従来の移行ステップ

- 従来のセキュリティ製品を新しくインストールする際には、既存の製品のアンインストールが必要。
- 以降する際にセキュリティがインストールされていない空白の時間が発生。
- アンインストールしてから、新しい製品のインストールが必要なので移行の実施に時間が必要。

ウェブルートの移行ステップ

- ウェブルートエンドポイントプロテクションを新しくインストールする際には、既存の製品のアンインストールは不要。
- セキュリティソフトがインストールされていない空白の時間がありません。
- 製品をインストールしてから、既存の製品のアンインストールができるので、効率的に移行を完了することが可能。
- トライアルのキーコードを引き継いで、製品版への移行ができるので、検証から配備までの時間を削減可能。

提供要件

Windows® 10：32 ビットおよび 64 ビット
Windows 8、8.1：32 ビットおよび 64 ビット
Windows 7：32 ビットおよび 64 ビット
Windows Vista®：32 ビットおよび 64 ビット
Windows XP®** 3：32 ビットおよび 64 ビット
Windows XP** Embedded Mac OS X 10.7 (Lion®)
＊＊必須条件：SHA-2 への対応

OS X 10.9 (Mavericks®)
OS X 10.10 (Yosemite®)
OS X 10.11 (El Capitan®)
macOS 10.12 (Sierra®)
macOS 10.13 (High Sierra®)
macOS 10.14 (Mojave®)

Windows Server® 2012 R2 Standard、R2 Essentials
Windows Server 2008 R2 Foundation、Standard、Enterprise
Windows Server 2003＊＊ Standard、Enterprise、32 ビットおよび 64 ビット（必須条件：SHA-2 への対応）
Windows Small Business Server 2008、2011、2012
Windows Server Core 2003＊＊、2008、2012
Windows Server 2003＊＊ R2 for Embedded Systems
Windows Embedded Standard 2009 SP2 Windows XP Embedded SP1、Embedded Standard 2009 SP3
Windows Embedded for POS バージョン 1.0
Windows Server® 2016 Standard, Enterprise and Datacentre
＊＊必須条件：SHA-2 への対応

※上記の提供要件は 2019 年 9 月時点になります。
最新の提供要件は弊社ホームページでご確認お願いいたします。

お問い合わせ

WEBROOT®

ウェブルート株式会社　www.webroot.com/
〒107-0062 東京都港区南青山 3-13-18 313 南青山 8F