



エムアール・イーピー

MR・EP®

BUSINESS ENDPOINT PROTECTION

WEBROOT
SecureAnywhere®

Technol

革新的なセキュリティアプローチ、 最高のパフォーマンスを最小の管理負荷で

～ エムアール エンドポイントプロテクション ～

はじめに

MR-EPは、ウェブルート セキュアエニウェア ビジネスエンドポイントプロテクションをベースにしたセキュリティサービスです。ウェブルート セキュアエニウェア 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ための革新的なアプローチを提供します。ウェブルート ブランドの新しい“ファイルパターン&行動認証テクノロジー”を、クラウドコンピューティングのパワーと組み合わせることにより、他のアプローチに比べ、より効果的に既知の脅威をブロックし、ゼロデイ攻撃を防止します。

業界最軽量かつ最速のエンドポイント セキュリティ クライアントを使用したスキャンは、驚異のスピードを実現（通常数分以内）。決してエンドユーザーのパフォーマンスをダウンさせません。本テクノロジーは、真にリアルタイムであるため、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。

フルクラウドシステム



最新の情報を各ユーザーに提供・保護

概要

既知&未知のマルウェアに対する最大限の防御

- 革新的なファイルパターン&行動認証テクノロジー
- PCの動作が安全か危険かを認証
- 新しい脅威に対する脆弱性を実質的に排除

超高速で手軽な配備

- 業界最小のエンドポイント セキュリティ
- インストールにかかる所要時間は通常数秒以内
- 他のセキュリティやソフトウェア アプリケーションと共存可能

PCのスローダウンや生産性の低下を招かない

- 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使用は最小限
- 最新の修復機能が、リカバリー等システムイメージの再適用を排除

常に最新状態で保護

- 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
ファイル無し
- 社内ネットワークに接続していないユーザーも保護しアップデートも
不要
- 新しい脅威に対し全てのユーザーを直ちに保護

容易な管理

- MR-EP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
- 自動化されたセキュリティ管理と報告システム
- サーバーハードウェアの導入や別ソフトウェアの導入などの管理不要

オンライン&オフライン時の防御

- オフライン時のエンドポイント使用管理用ユーザー
ポリシー制御を別途設定可能
- USBやCD、DVDドライブなどのポートやデバイスの
ロックダウン機能

主な特徴



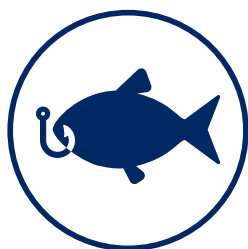
クラウドベースで
定義ファイルが不要
パソコンの動作を妨げません！



グレー判定により
未知のファイルもしっかり監視！



ジャーナル&ロールバック
機能により
感染前の状態に戻します！



ID シールドによりブラウザ経由の
脅威から個人情報を保護！



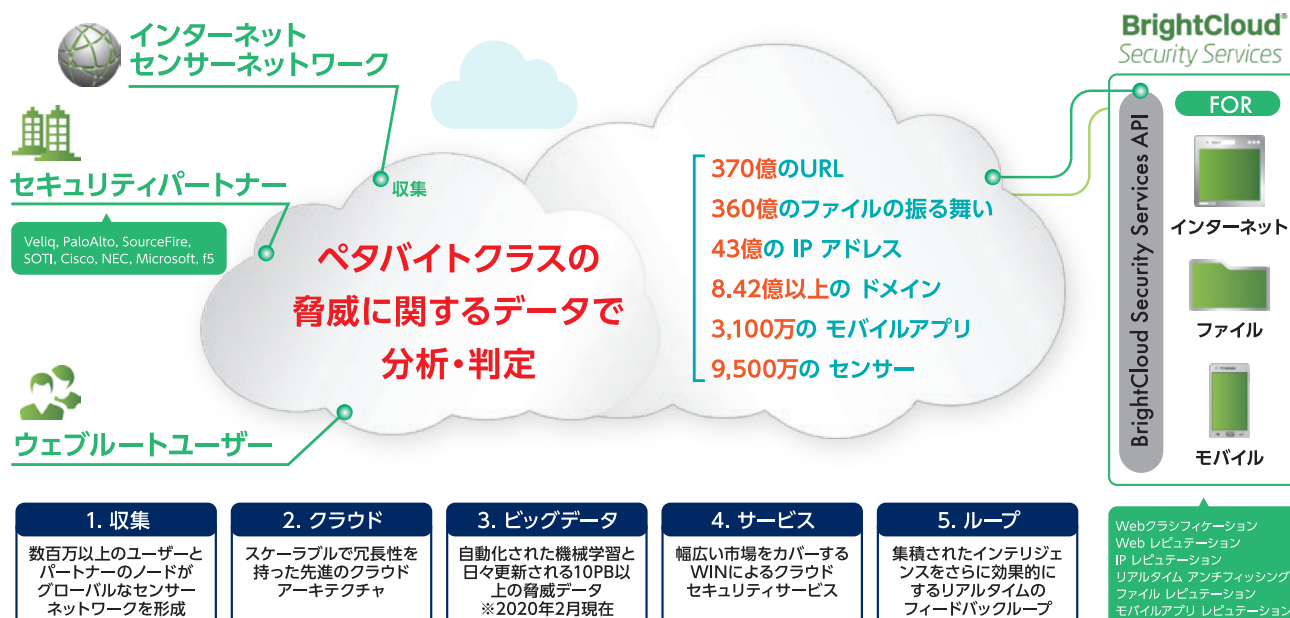
無償で使える
クラウド管理コンソール！

ウェブルート インテリジェンス ネットワークについて

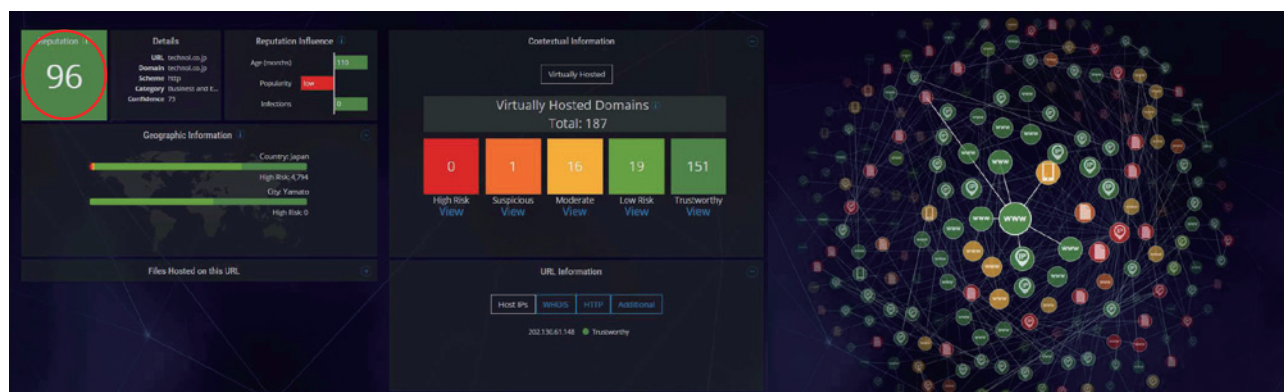
ウェブルート社の脅威対策エンジン

ウェブルート インテリジェンス ネットワーク(WIN)は、未知の脅威や標的型攻撃に対する画期的な次世代アプローチの主要な構成要素です。ウェブルートの超効率的なエンドポイントエージェントであるMR-EPとWINが一体となり、その結果生まれたソリューションは、今発生したばかりの攻撃に対しても、危害が及ぶ前に確実に防御します。

ウェブルート インテリジェンス ネットワーク



ウェブルートはインターネットの95%以上のIPを
一日3回スキャンし、連続的に分類とスコアリングを行う。
また、IPv4の全てと利用されているIPv6を監視。



主要な導入メリット

～ ハッシュ方式のメリット ～

対応の迅速さ

従来の
シグネチャ方式
の場合



ウィルスを発見



解析して
定義ファイルを作成



最短1日、長いと5日くらい
かかるとわれています

最近では数秒にいくつかの
ウィルスが発生しており、従来の
方式では対応出来ません。



発見から最短5分で世界中に配布

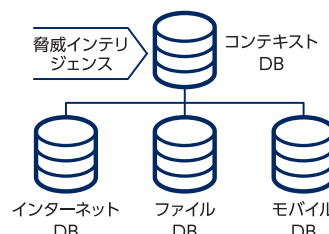
ハッシュ方式
の場合



ハッシュ (データの指紋) を採取



AIを利用した機械学習
により精査



従来のシグネチャ方式

従来のシグネチャ方式



判断する場所が違うので
他社ソフトと共存も可能



PC端末にシグネチャを持ってくることで動作が重くなり
更に判断もPCで負担するため負荷が大きい

PCはハッシュ (1K位の小さなデータ) をクラウドに送るだけ。
Cloud上でデータを判断するためPC端末に負荷がかかりません!

フルクラウドが実現する圧倒的に高いパフォーマンス

Passmark Software Performance Benchmark August 2017

95

61

53

53

52

51

45

41

MR-EP
WEBROOT

A社

B社

C社

D社

E社

F社

G社

MR-EP の未知の マルウェア対策について

グレー判定による未知のマルウェアに対する最大限の防御

WEBROOT
BrightCloud® Threat Intelligence

送られてきた
ハッシュ情報を分析して
白・黒・グレーの
判定結果を
返します

①クラウドに問い合わせして
結果をもらう

白 (安全) 実行許可



②白判定ならそのままPCに残す
黒判定なら削除

黒 (マルウェア) 実行拒否 & 隔離



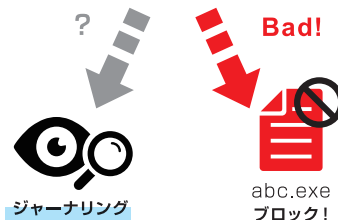
⑥ジャーナル (記録) を基に
感染前の状態に戻します

ランサムウェアであれば、暗号化された
ファイルが元の状態に戻ります

グレー (不明・未知)



③わからないものは
サンドボックス化して監視



④監視中にクラウドで
黒判定されれば削除

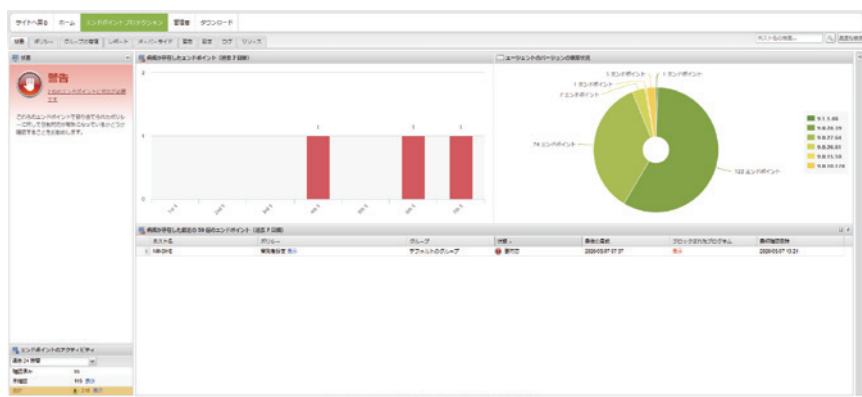
⑤ふるまいを観察し怪しい
動きを検知したら削除

クラウド判定が
黒になった時点や、
悪意のある挙動が
確認されるとブロックし、
ファイルの変更を
元に戻す

監視下におかれ、
ファイルの
変更を記録

管理者にとってうれしいクラウド管理コンソール

クラウド管理コンソールで完結



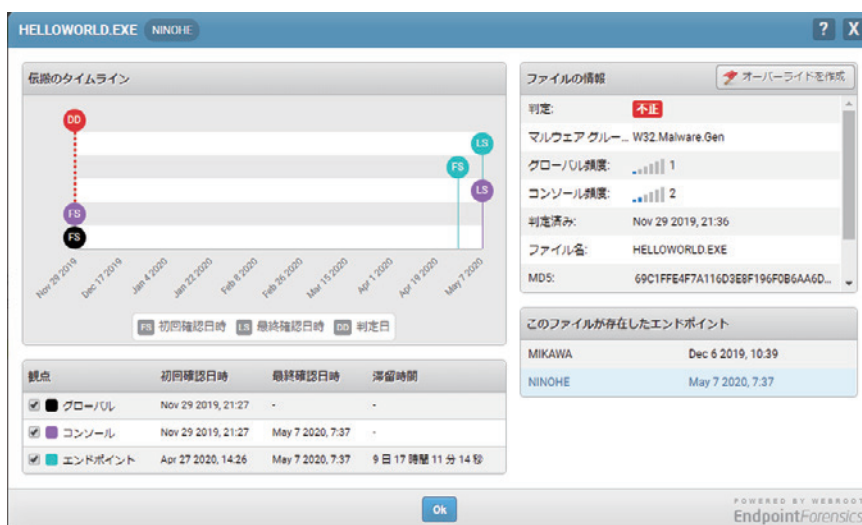
クライアントの状況一覧

- エージェントのバージョン一覧
- 1週間の感染状況
- 感染端末一覧
- 感染したファイル一覧
- 一覧から必要情報にアクセス可能

ホスト名	ポリシー	初回確認日時
1 ASUS-TAKIN-DEMO	Test 5	2016/04/14 00:41
2 DELL-K3-2F957E5D	Test 5	2017/09/29 15:32
3 DEMO-PC	Citrix Policy	2018/09/13 09:46
4 DESKTOP-SBAN8E4	デモポリシー (中村) ASUS DE...	2018/04/27 11:03
5 HDL-ZWMC	Test 5	2017/08/22 14:27
6 HDL-ZWPI	Test 5	2017/08/23 15:50
7 KI2.	ivP	2017/09/26 14:57
8 KI33.	ivP	2015/09/30 17:09
9 KMORI-7084L-TKO2	Test 5	2015/02/20 02:39
10 MMB2012	Test 5	2016/11/17 15:46
11 Taki Mac	Test 5	2015/04/02 15:55
12 VAIO	Test 5	2017/05/20 13:39
13 WEBROOT.PC	hamada test	2017/04/06 17:52
14 XP-SP2	推奨デフォルト設定	2012/05/15 17:32

グループ管理機能

- 各クライアントをグループ振り分け可能
- グループ毎のポリシー設定
- グループに対するコマンド実行
- AD情報を反映可能



滞留状況の確認機能

- 自社コンソール内での
伝播状況の確認
- マルウェアの詳細内容の確認
- 世界中でいつ見つかった脅威で、
いつ自社ネットワークに入ってきたか
確認可能

- その他エンドポイントへの配置や、シャットダウンコマンドの送信、ホワイトリスト管理
- アンインストール信号の送信など、様々な管理ツールを備えております。

対応OS及び動作環境

PC オペレーティング システム

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® SP3 ※ (32ビットおよび64ビット)
Windows XP® Embedded ※

※必須条件:SHA-2への対応

Mac オペレーティング システム

Mac OS X 10.15 (Catalina®)
Mac OS X 10.14 (Mojave®)
Mac OS X 10.13 (High Sierra®)
Mac OS X 10.12 (Sierra®)
Mac OS X 10.11 (El Capitan®)
Mac OS X 10.10 (Yosemite®)
Mac OS X 10.9 (Mavericks®)
Mac OS X 10.8 (Mountain Lion®)
Mac OS X 10.7 (Lion®)

WindowsServer

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)
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 パージョン 1.0
Windows Server® 2016 Standard、Enterprise and Datacentre

※必須条件:SHA-2への対応

VM環境

VMware® / vSphere®5.5以前 (ESX®/ESXi5.5以前) /
Workstation 9.0以前 / Server 2.0以前 / Citrix® /
XenDesktop®5 / XenServer®5.6以前 / XenApp®6.5以前 /
Microsoft®Hyper-V® / Server 2008 / 2008 R2 / VirtualBox

ブラウザ

Google Chrome® 11 以降
Internet Explorer® バージョン 7 以降
Microsoft Edge® (サポートは部分的)
Mozilla® Firefox® バージョン 3.6 以降
Safari 5 以降
Opera 11 以降

システム構成

Intel®Pentium® / Celeron®ファミリーまたはAMD® K6 / Athlon™
Duron™ ファミリーまたはその他の互換プロセッサ
128 MB 以上のRAM(最小) 10 MBのハードディスク領域インターネット環境

お問い合わせは

Technol

株式会社テクノ [MR-EP担当]
TEL 0178-47-8311
青森県八戸市廿三日町2番地 YSビル3F