Dr.Webが誇るマルウェア検知テクノロジーについて

Doctor Web について

1992年　創業者 Igor Danilovが、Dr.WEBという名のアンチウイルスソフトを初めて開発

1999年　**世界初のふるまい検知**テクノロジSpIDer Nettingを開発

2003年　法人格「Doctor Web Ltd.」を設立

280人の従業員のうち、160人が開発および解析作業に従事。

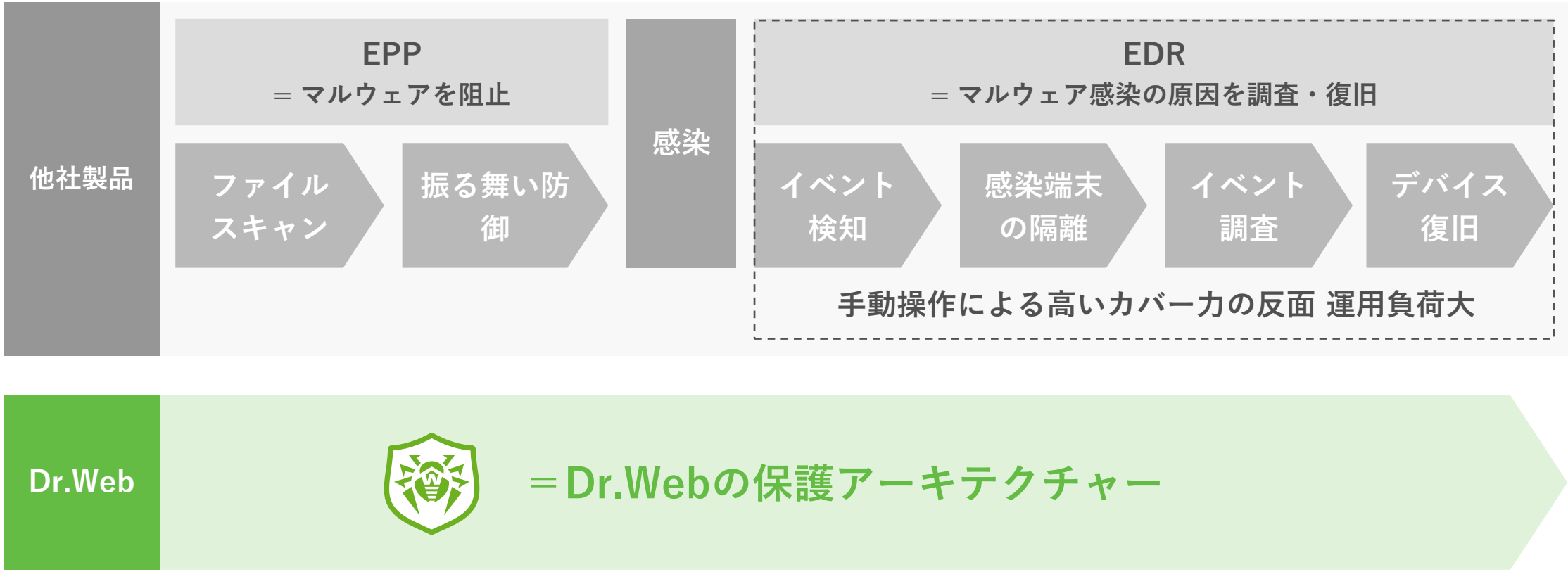
全世界の個人ユーザから大手企業まで利用され、

世界的なアンチウイルスソフトウェアに成長。

インターネットに潜む害虫(マルウェア)から
Spiderweb(クモの巣)が守ります。

製品コンセプト

Dr.Webが考えるエンドポイントセキュリティー



Dr.Webひとつでエンドポイントセキュリティーを全てカバー

Dr.Webの製品コンセプト

使いやすさを追求したシンプルなアンチウイルスソフト

Dr.Webで 安心
あらゆる潜んだ未知の
マルウェアを検知

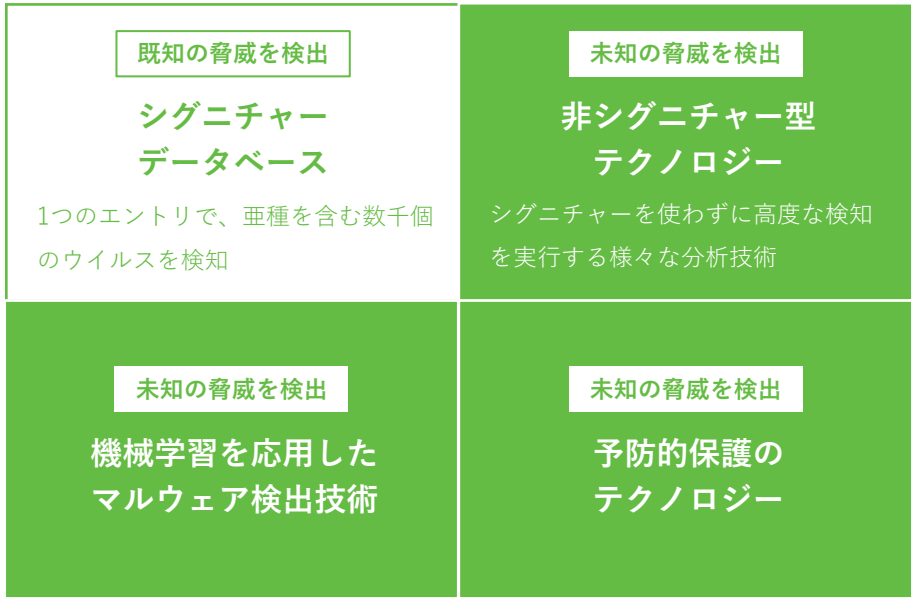
Dr.Webで 快適
最適化された機能群。
使いやすさによる運用コストを低減

安全・快適に特化することで下記メリットを提供いたします。

point 1 ランサムウェアの検知力

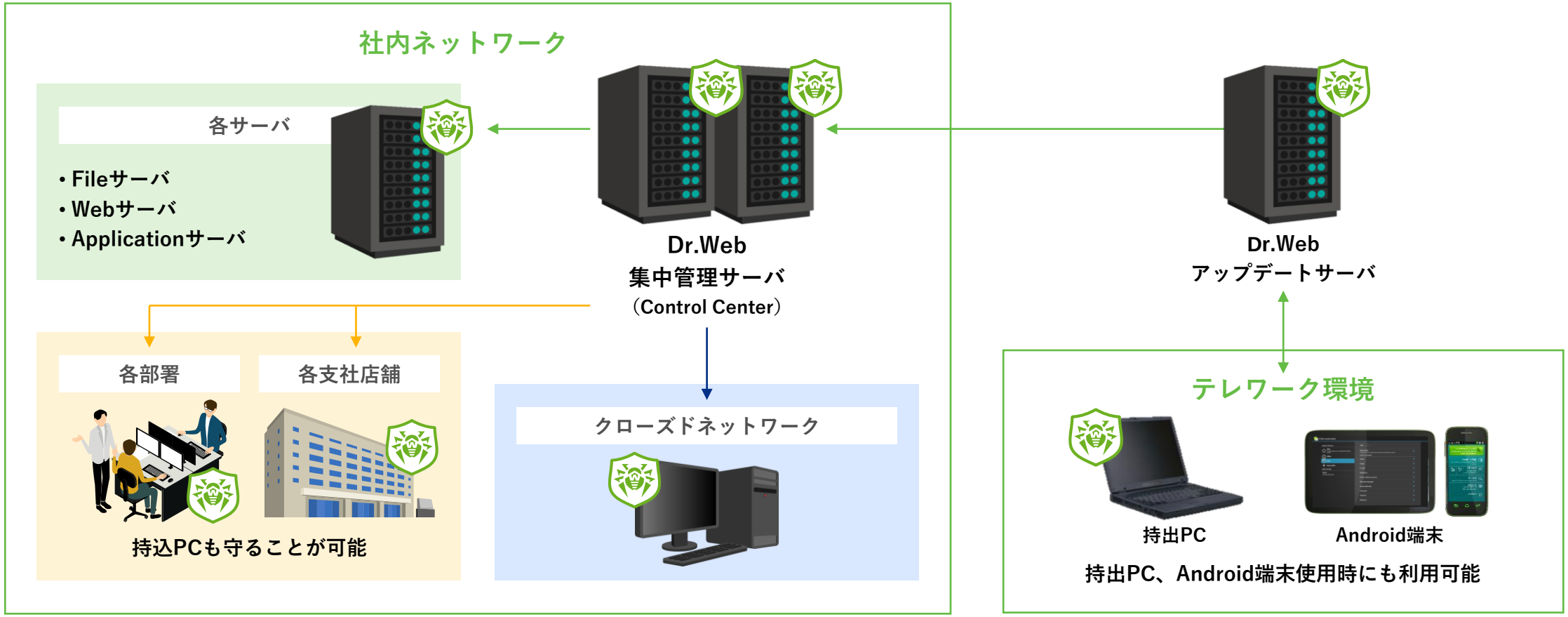
point 2 PCのリソースの大幅な削減

信頼性の高いテクノロジーで
快適なセキュリティ運用を実現します



Dr.Webの利用イメージ

様々なクライアント OS、サーバー OSに対応した製品でエンドポイントを守る



Dr.Web 製品の検知テクノロジー

Dr.Web 製品の検知テクノロジー

悪意のあるソフトウェアに対する検出方法

以下の５つのマルウェア検知テクノロジーについてご説明します。

1. Origins Tracing™（オリジンズ・トレーシング）
2. Dr.Web Heuristic Analyzer（ヒューリスティック解析）
3. Dr.Web Cloud（クラウドベース検知）
4. SplDer Guard™（リアルタイム保護）
5. HyperVisorベースの防御

セキュリティ企業Doctor Webが開発・提供するアンチウイルスおよびマルウェア対策ソフトウェアで、そのマルウェア検知テクノロジーにはいくつかの独自の特徴があります。

Dr.Web 製品の検知テクノロジー

Origins Tracing™（オリジンズ・トレーシング）

Dr.Web独自の静的解析エンジンで、マルウェアの「起源」に基づいてコードを分析します。

この技術は、新種や亜種などのバリエーションが多いマルウェアを検出するのに非常に効果的で、シグネチャに頼らずに未知の脅威を検知できるという特徴があります。

また、Dr.Web ヒューリスティックアナライザにより誤検出を劇的に減らすことができる特徴があります。

Dr.Web 製品の検知テクノロジー

Dr.Web Heuristic Analyzer（ヒューリスティック解析）

未知のマルウェア検知に特化した高度な解析エンジンになります。

シグネチャ（既知のウイルス定義）に依存しない検知メカニズムであり、ゼロデイ脅威や変種マルウェアの早期発見に極めて有効な検知テクノロジーになります。

「未知の脅威を予測して防ぐ」ためのコア技術になり、クラウド未接続の環境や、リアルタイム防御が難しい状況でも真価を発揮する防御層です。

既知のシグネチャファイルに頼らない柔軟な防御が必要な場面では、活躍する技術になります。

Dr.Web 製品の検知テクノロジー

Dr.Web Cloud（クラウドベース検知）

リアルタイムで柔軟な脅威対策を提供するために設計されたクラウド連携型マルウェア検出技術になります。

従来のローカルデータベースだけでは対応しきれない新種・変種マルウェアやフィッシングサイトをオンラインスキャンにより、即座に分析できる仕組みになります。

オンラインスキャンのため、端末の負荷を減らすことができます。

ユーザーが許可した場合のみ、検出データをDr.Web クラウドに送信され、脅威分析の学習データとして蓄積されます。

Dr.Web 製品の検知テクノロジー

SpIDer Guard™（リアルタイム保護）

リアルタイム保護モジュールになり、ユーザーのシステム上で発生するあらゆるファイルアクセスや操作を常時監視し、マルウェアの即時検出・阻止を行います。

ヒューリスティック解析とOrigins Tracing™による動的検知により、未知の脅威（ゼロデイ攻撃）を防ぎます。

Dr.Web Cloudとの連携により、未知マルウェアにも即時対応できます。

Dr.Web 製品の検知テクノロジー

HyperVisorベースの防御

高度なマルウェア、特にルートキットやカーネルレベルで動作する脅威に対抗するために設計されたセキュリティ技術になります。
従来のセキュリティ機構では検出・排除が難しいマルウェアを「OSよりも低い階層（HyperVisor層）」から監視・防御します。

マルウェアに対しては「検知されない監視者」として機能し、セキュリティソフトの存在を回避しようとする攻撃や仮想環境での検出を回避する攻撃にも有効です。

ドライバのインジェクション、APIフック、プロセス偽装などのカーネルレベルの改ざんをリアルタイムで検出し、正常な状態に強制的に復元します。

Dr.Web アンチウイルス

製品群

Dr.Web ソリューションマップ

エンドポイント / ゲートウェイ アンチウイルス	Dr.Web Enterprise Security Suite PC / Mobile / Server OS / MacOS / Proxy / Mail Server	オンプレミス アンチウイルス
	Dr.Web サブスプリクションサービス PC / Mobile / Server OS / MacOS/ Proxy / Mail Server	クラウド/サブスク型 アンチウイルスサービス
アドオン / セカンドオピニオン	Dr.Web Cure Utilities	インストールレスアドオン
	Dr.Web KATANA	常駐型アドオン（シグニチャーレス）
スレットインテリジェンス	Dr.Web y-Tracker	高度なスレッドポータル
	Dr.Web Threat investigation service	個別調査サービス
EDR-like	Dr.Web vxCube	クラウド型解析

本来のアンチウイルスの役割として、グレーなものも含め検知・駆除し、システム運用者の負担を軽減します。
エンドポイント製品では極力コンパクトな設計にすることで挙動の軽さを実現します。
運用上負担となりがちな「解析・追跡」の要素は外出しし、クラウド型のオンデマンドサービスとして提供しております。

Dr.Web プロダクトラインナップ

用途	製品名	対応OS等	コメント
エンドポイント	Dr.Web Desktop Security Suite	Windows ／ Linux ／ macOS	ふるまい検知を搭載したPC端末用 総合アンチウィルス
	Dr.Web Katana	Windows	ふるまい検知のみ提供
モバイル	Dr.Web Mobile Security Suite	Android	世界で1億6000万DLの実績
サーバー	Dr.Web Server Security Suite	Windows ／ Linux ／ macOS	国内ISP/CATVでも実績多数
メールサーバ	Dr.Web Mail Security Suite	Unix	国内ISP/CATVでも実績多数 アンチスパムオプションあり
修復ユーティリティ	Dr.Web CureIt! ／ Dr.Web CureNet!	Windows	他社AV搭載の環境で簡単スキャン セカンドオピニオン
無制限ライセンス	オフィスマルチパック	Windows ／ Linux macOS ／ Android	中小企業向けデバイス無制限パック
	公共マルチパック		公共期間向けデバイス部制限パック
	小中高等学校向け無制限ライセンス		学校向け無制限パック（学校単位）
	大学専門学校向け無制限ライセンス		大学向け無制限パック（人数単位）
インテリジェント アナライザー	Dr.Web vxCube	Windows ／ Android	オブジェクト解析クラウド 未知の脅威に対するワクチン提供
サブスクリプション	Dr.Webサブスプリクションサービス	Windows ／ Linux macOS／ Android	欧州・ロシア初のクラウド型 アンチウイルス

Dr.WEB®

今後とも宜しくお願い致します。

Doctor Web Pacific, Inc
http://www.drweb.co.jp/