CMSのランサムウェア対策のご紹介

株式会社Doctor Web Pacific
代表取締役　　森　周

Doctor Web について

1992年　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。

Doctor Web Pacific について

Doctor Web Pacificは、アンチウィルス『Dr.WEB』の製品とサービスを約5,000を超す団体に販売。
警察機関、金融機関、サイバーセキュリティ会社と連携しながら国内のコンピュータ環境を保護しております。
マルウエアの検出・駆除能力および感染されたシステムを回復する能力を高く評価いただき、
日本国内においても5,000を超す団体で利用されております。

会社名	株式会社Doctor Web Pacific
英文表記	Doctor Web Pacific, Inc
所在地	東京都港区西新橋1-14-10西新橋スタービル 2F
代表者	森　周
TEL/FAX	03-6550-8770 /　FAX：03-6550-8771
業務開始日	2010/12/14
資本金	7300万円 （Doctor Web, Ltd.　100%出資）

自己紹介

- 森　周（もり　あまね）　48歳
- 商社系SIer → セキュリティソフト → データセンター → 現職
- 東京都文京区出身・府中市在住
- 家族：妻、長女、長男
- 趣味：スノーボード・料理・サッカー観戦・ゴルフ
- 最近ハマっていること
  - ・プロサッカーの観戦　・息子のサッカー観戦
  - ・三国志　・チャーシュー作り　・オーガニック

WordPressにおけるマルウェアリスク

Webサイトを感染させる、Linuxを標的としたバックドアマルウェア

- 2023年1月　当社がLinux向けの悪意のあるプログラムを発見しニュースリリース

  https://news.drweb.co.jp/show/?i=14646

- WordPress CMS上の19種の古いプラグインやテーマに存在する脆弱性を突いてハッキング
- ハッキングからの流れ：
  - ➡ Webサイトの管理者アカウントをハッキング。リモート操作を可能にする。
  - ➡ 攻撃者の望む別のサイトにリダイレクトさせ、悪意のあるプログラムをDLさせる
  - ➡ 悪用に成功した脆弱性と、未適用のパッチに関する情報をC&Cサーバに報告し繰り返し攻撃する
  - ➡ Webサイトから社内ネットワークへの侵入を試み、二次攻撃を開始する
  - ➡ 仮想通貨マイニングツールのリソースとしてWebサーバを流用
  - ➡トラフィックの転売や仲介による収益を得る

二次攻撃の1つの手段に過ぎないランサムウェア

Step 1 OS、ミドルウェアの脆弱性を突いて侵入し、管理者権限を奪取

Step 2 収益を目的とした犯罪行為 ➡ ランサムウェア配布、マイニング、DDoS など

Step 3 犯罪行為の拠点としてのサーバ活用（踏み台、C&Cサーバ）

誰でも簡単に作成可能!!!　ランサムウェアの作成用ポータルが存在

Ransomware as a Service（RaaS）はランサムウェアを「サービス」として提供する
ダークウェブ上のフォーラム/ポータルです。金銭でランサムウェアプログラム、
復号キー、ターゲットリスト、プログラム配布用のインフラを購入することが出来ます。

二次攻撃の1つの手段に過ぎないランサムウェア

Step 4 PC端末に不正プログラムを広げ認証情報を獲得。ボットネットを作成

Step 5 ファイルサーバに侵入し、ランサムウェアによる暗号化を実施

Step 6 さらに上位のサーバに侵入し、個人情報を窃取

アンチウイルスの世界における
Dr.Webの位置づけ

Dr.Webのアンチウイルスソフト

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

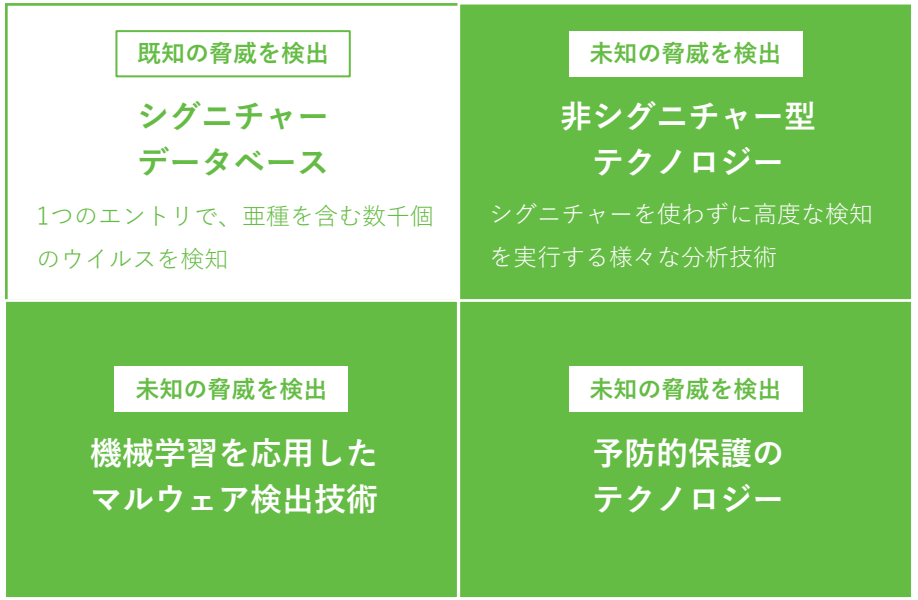
Dr.Webで 快適
最適化された機能群
使いやすさによる運用コストを低減

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 検出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の特長

ランサムウェアへの強み	ランサムウェア専門チームが持つ 豊富なノウハウによる検知力
高い コストパフォーマンス	安価ながら機能性と運用性を提供
EDRを必要としない アーキテクチャー	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
ユニークな ソリューション	他社アンチウイルスと同居可能なセカンドオピニオン製品を提供 シグニチャーレス型もご用意

特長①　ランサムウェアへの強み

成功報酬型のランサムウェア被害救済サービス

お使いのアンチウイルスソフトを問わず、Dr.Webユーザーなら無償で利用可能な
ランサムウェアによる暗号化被害ファイルの復号化サービス

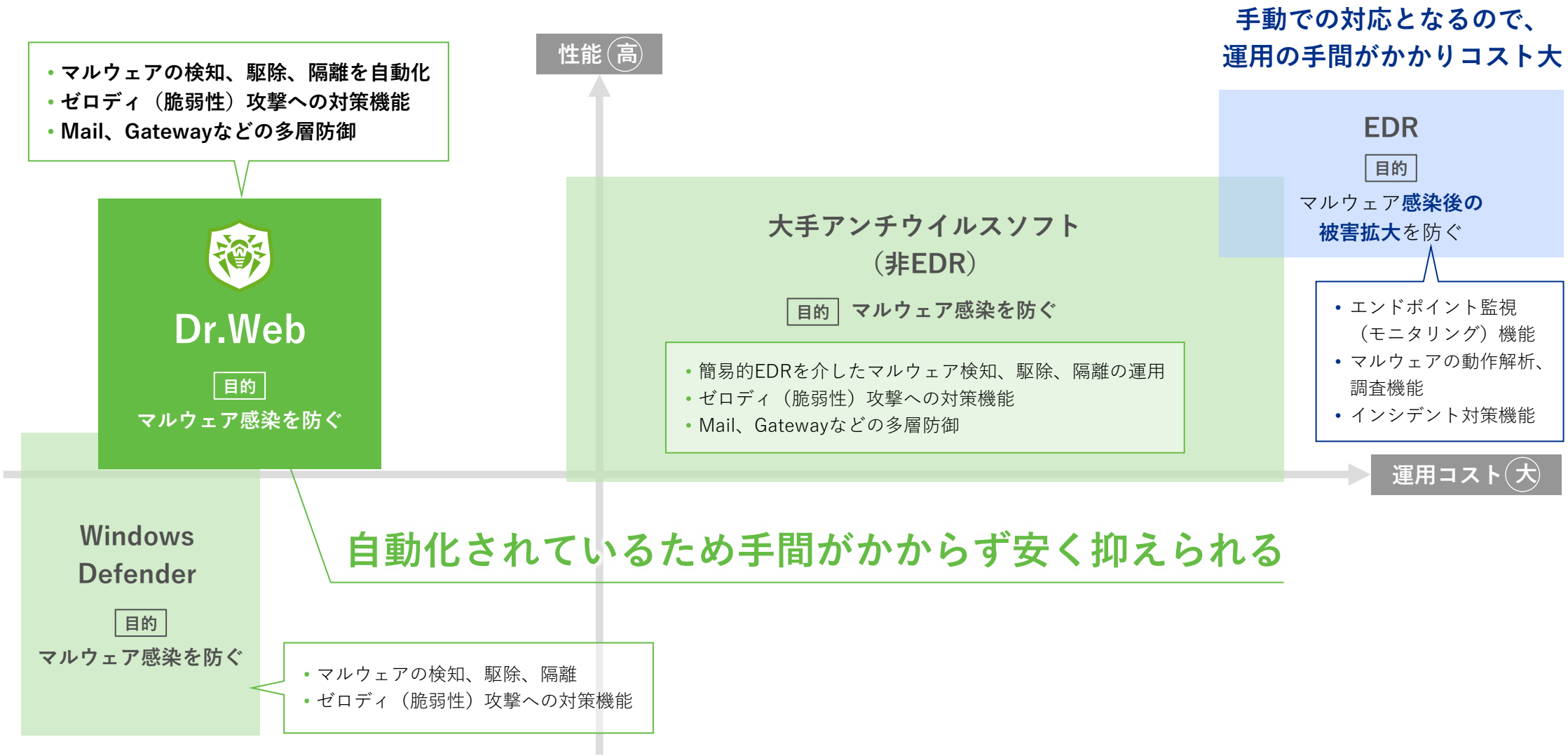
point 1　10年以上のノウハウ

2014年からファイル復号化ルーチンを徹底的に研究
マルウェアインテリジェスで得られる情報を掛け合わせ、
高い確率で多くの暗号化ファイルを救済

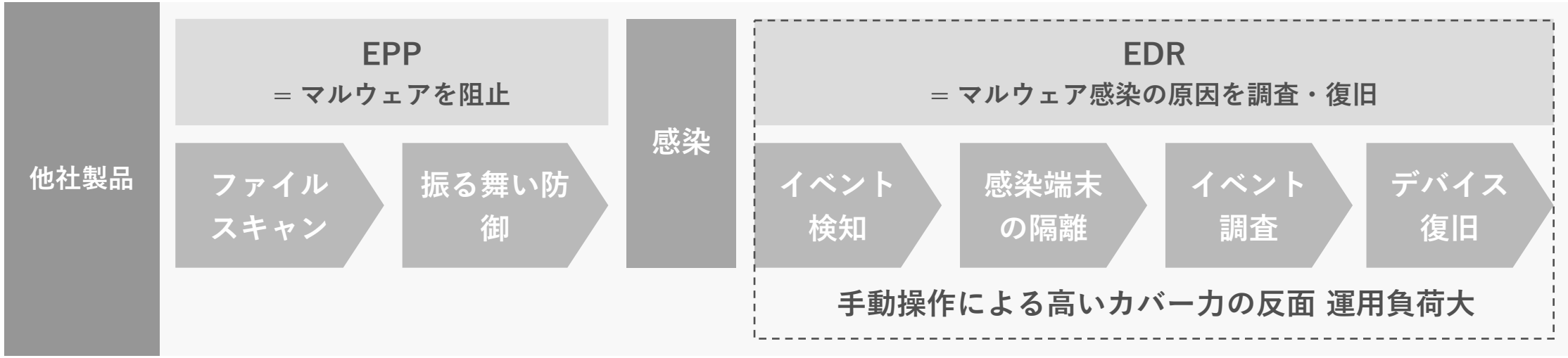
point 2　成功報酬型による低コスト化

Dr.Webユーザーなら無償で利用可能
復号に成功した場合のみ、18,000円で
「復号キー、復号ツール、2年分のライセンス」をご提供

特長②　シンプルなエンドポイントセキュリティ



特長③　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

特長④　ユニークなソリューション

Dr.Web CureIt! / CureNet!

(Software)

PC及びサーバーのウィルス検知・修復。
既存アンチウィルスソフトでは検知出来ないマルウェアを炙り出す非常駐スキャナ。
インストール不要なセカンドオピニオンツール。

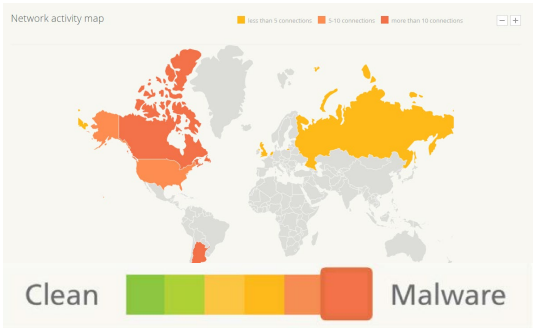
他社アンチウィルスと共存可能

Dr.Web Katana

(Software)

ふるまい検知機能 DPH（Dr.Web Process Heuristic）のみを実装した、シグニチャーレス型アンチウィルス製品

他社アンチウィルスと共存しながら未知の脅威を検知



Dr.Web vxCube

(Service)

クラウドサンドボックス型マルウェア解析サービス
ブラウザ上でファイルを指定して
簡単に解析。未知の脅威と判断された場合、
Dr.Web CureIt!の特別ビルドで修復可能

金融機関や
セキュリティサービス業者が活用

アンチウイルスソフトの価値に関する問題提起

-アンチウイルスに知名度は必要か？-

問題提起① 著名なセキュリティーソフトほど攻撃の拠点とされる

アンチウィルスにとって知名度は必ずしもメリットではありません

Doctor Webは、「アンチウイルス自体を保護するセルフプロテクション」に注力
著名になることよりも、顧客のコンピュータ資産を守ることを優先します

著名なほど、標的になりやすく、シェアも大きいため実被害が大きくなる傾向にある

大手アンチウイルスソフトの管理サーバーの無力化

⇒アンチウィルスの無力化により、
総合電機メーカM社がランサムウェア被害にあい、機密情報や個人情報のファイルが流出(2020年)

標的型攻撃の対象となりADの管理者権限はく奪

⇒OS、大手アンチウイルスの脆弱性を突かれ標的型攻撃を受けADの管理者権限がはく奪され、国内総合病院で電子カルテ情報漏洩（2019年）

Windows Defenderに脆弱性が判明する

⇒Windws7から10の間の長期間にわたって脆弱性が存在することが判明
実際に攻撃も確認されている(2021年)

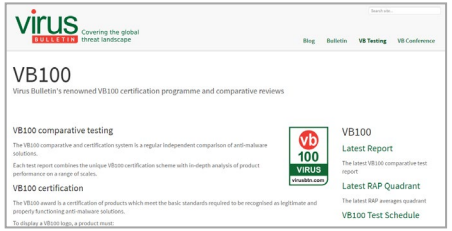
問題提起② アンチウイルスの第三者評価のプロセスは公平とは言えない

第三者評価に頼らないアンチウイルス選びをご提案

Doctor Webは「アンチウイルスを評価するのは第三者ではなくお客様」と考えてます

評価プロセスの公平性を考慮し、当社は第三者評価への参加を辞退しています

アンチウイルスの第三者評価のプロセスの現状



メーカーが調査費用を払う

再試験が可能

対象メーカーの偏り調査機関によるバラつき

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 Premium サブスプリクションサービス PC / Mobile / Server OS / MacOS	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	Windows向けはふるまい検知搭載 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 Premiumサブスプリクションサービス	Windows ／ Linux ／ macOS	欧州初のクラウド型 アンチウイルス

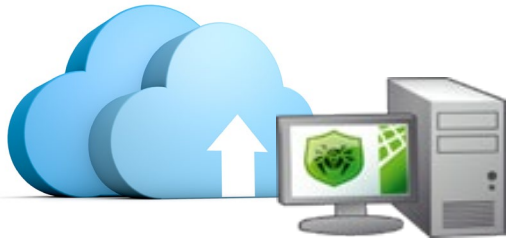
Dr.Web アンチウイルス

導入実績

Dr.Webによる様々な国内ビジネス実績-1

- ✓ 携帯電話キャリアと連携し、大手物流会社の業務用スマートフォンに「Dr.Web」を搭載。約4万人以上の宅配ドライバーの業務端末を保護

- ✓ 中学生向けのデジタル教材タブレットに「Dr.Web」を標準搭載
- ✓ さつき製電子黒板「コラボン」に「Dr.Web」を標準搭載



- ✓ 日本全国のインターネットプロバイダー、CATV、クラウドプロバイダーが提供するIaaSやメールサービスを「Dr.Web」で保護

Dr.Webによる様々な国内ビジネス実績-2

全国50社のリセラーネットワークを通じて、北海道から沖縄まで
約3,500の小中学校・高等学校・大学様向けにアンチマルウェアを提供

- ✓ 某県教育委員会　県立高校120校、合計3,5000台のPCを保護
- ✓ 某県立大学　生徒・教員・職員の合計3,000台のPCを保護
- ✓ 某国立大学　生徒・教員・職員の合計30000台のメールを保護

古いOSを使わざるを得ないエンドポイント環境を保護

Windows XP, Windows Server 2008, 多様なLinux 等の古いOSをサポート

古いOSや古いアプリケーションの脆弱性を突いた悪意あるプログラムをブロック

工場などに設置されたオフライン端末

廃止できない古いアプリケーションが稼働する専用端末⇒工場、オフィス、店舗

古いインフラの脆弱性を埋め、継続利用をサポート

導入事例（他社からの乗換）

某物流会社様

社員数	15,000名	PC	12,000台

他社製品を5年間使っていたが、ウイルス検知が少なすぎることから、乗換を考えていた。使っている製品の値上げとWindows10への入れ替えを機に、ウイルス対策の見直しを検討開始した。残されたWindows XPのために部分的に先行導入したDr.Webの検知力が優れており、未知のウイルスへのふるまい検知を活発に行うことから、4製品と比較検証を行った結果、Dr.Webの全社導入を決定した。

point 1

Webサーバの保護も

Dr.Webを社内のLinuxサーバに展開。Webサーバや、業務系のWebフロントサーバにも導入し一元的なウイルス対策を実現。

point 2

高品質低格面

従来使っていた製品の値上げにコストが増大。
Dr.Webは導入したらすぐにウイルスを検知。
そのうえ以前よりコストを抑えることが出来た。

導入事例（Windows）

某県教育センター 様

県立高校	119校	端末数	約20,000台

T社製品を利用していたが、実装すべきセキュリティ対策の項目が増え予算が圧縮。また、検知漏れによる現地からの問合せもありプロダクトの変更を検討。検証フェーズに入った。検証して利用した途端に、ウイルス検知があり検知精度の高さを実感。また、管理画面の使いやすさや細かいセキュリティ機能の豊富さに納得し、またコストダウンも図れると判断した。

point 1

マルチOS

Windows端末だけでなく、Linuxサーバを学校毎に配備。Linux向けDr.Webを活用し、ファイルサーバ等の貴重な情報資産を守っている。

point 2

分かりすい管理GUI

前回使っていた製品と比べ、管理GUIが使いやすく学校毎のどの端末で何が・・・というログやインシデントの管理も容易になった。

おさらい

脆弱性リスク回避	OSおよびWordpressプラグイン・テーマを最新のものにUpdate
アンチウイルス選び	ランサムウェアに強いアンチウイルスをチョイス
アンチウイルス選び	古いOSをカバーしてくれるアンチウイルスをチョイス
最悪の事態	ランサムウェア復旧サービスを利用する

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/