修復ユーティリティ
Dr.Web CureIt! / CureNet! / FixIt!
説明資料

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。

Doctor Web Pacific（日本法人）について

Doctor Web Pacificは、2010年12月に設立された「Doctor Web Ltd.」の子会社です。
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。
マルウェアの検出・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）

製品コンセプト

修復ユーティリティとは？

**利用中のアンチウイルス製品およびネットワークの規模に関わらず、
インストール不要のマルウェア検出、駆除、調査、修復ツールです**

修復ユーティリティのDr.Web CureIt! / CureNet!は、Windows PC及びサーバーのウィルス検知・修復が行えます。 Dr.Web FixIt!は、データの収集・解析を行いインシデント調査を行い修復ツールの作成を補助します。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や標的型攻撃に使用されるプログラムを検出する非常駐型スキャナになります。他社アンチウィルスソフトがインストールされていても利用可能です。

・システム検査
・スキャン

・調査
・解析
・修復ツール作成

・駆除
・修復

Dr.Webが考えるエンドポイントセキュリティー

	ファイル スキャン	振る舞い 防御	イベント 検知	感染端末の 隔離	イベント 調査	デバイス 復旧
ESS	◯	◯	◯	◯	◯	◯
Cure Utilities	◯	-	-	◎	◎	◎

ソリューションを掛け合わせて
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 既存アンチウイルスと同居可能

point 2 インシデント調査が可能

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

既知の脅威を検出 **シグニチャー データベース** 1つのエントリで、亜種を含む数千個のウイルスを検知	未知の脅威を検出 **非シグニチャー型 テクノロジー** シグニチャーを使わずに高度な検知を実行する様々な分析技術
未知の脅威を検出 **機械学習を応用した マルウェア検出技術**	未知の脅威を検出 **予防的保護の テクノロジー**

Dr.Web CureIt! / CureNet! /FixIt!の特徴

特徴

Dr.Web CureIt! / CureNet!は、セキュリティ対策のセカンドオピニオンツールとして、緊急駆除/修復のために年間600万人以上ものユーザー（日本の警察機関やサイバーセキュリティ対策の専門会社等）での捜査、調査に利用頂いています。
※スキャンおよび調査、修復のためのユーティリティツールです。常駐監視保護（リアルタイムスキャン）機能はございません。

製品の利点

- インストール不要のマルウェア検出・駆除・修復ツール
  実行ファイル形式で提供するマルウェア検出・駆除・修復ツール
  そのため、他社アンチウイルソフトがインストールされていても動作可能
- Dr.Web独自技術による業界最高レベルの検出力
  独自の方法/ルートにより、日本国内における標的型攻撃等のマルウェア検体を収集
- Anti-rootkit技術により、ルートキットで隠されているマルウェアを検出
  暗号パッカー解読技術「FlyCode」およびエンドロビー理論に基づいた技術により、既存アンチウイルスソフトで発見でないマルウェアを検出
  診断ツールによる、データ収集、解析による修復メカニズムの生成
  診断ツールにより収集されたレポートに基づき、Dr.Webのスペシャリストが解析を行い、必要な修復コマンドを作成

スタンドアロン型

Dr.Web CureIt!

ローカルネットワーク型

Dr.Web CureNet!

インシデント調査

Dr.Web FixIt!

Dr.Web CureIt! ：スタンドアロン型

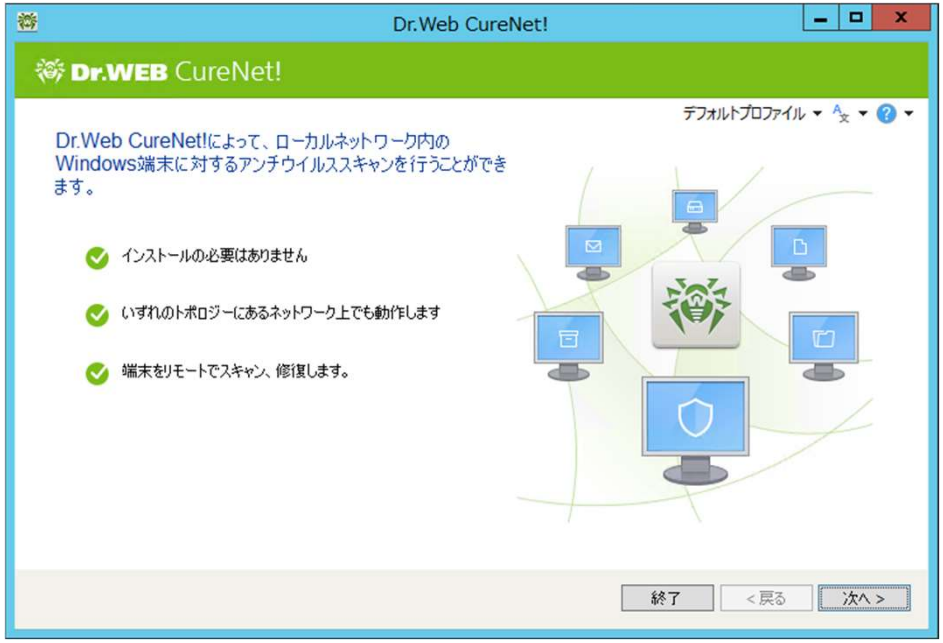
既存アンチウィルスが検知できずに潜んでいるマルウェアを炙り出し、
状況把握から駆除、修復まで行う非常駐型のアンチウィルスユーティリティです

- インストール不要のマルウェア検出・駆除ツール
- お使いの他社アンチウィルスソフトが見逃した
  マルウェアを検知
- USB ストレージデバイスを含む
  リムーバブルメディアから起動することが可能
  対象端末がインターネットの接続不要

Dr.Web CureNet! ：ローカルネットワーク型

同一ネットワーク上にあるWindows PC、及びWindows サーバーに対して、
スキャン・修復を行うネットワーク型 非常駐アンチウィルスユーティリティです

- インストール不要のマルウェア検出・駆除ツール
- お使いの他社アンチウィルスソフトが見逃した
  マルウェアを検知
- USB ストレージデバイスを含むリムーバブルメディアや、
  ネットワークからスキャナ昨日の配布が可能
- 感染したオブジェクトの修復が可能
- ２次感染の防止を目的としたスキャン中の
  マシンネットワークの切断が可能
- 管理コンソールより、スキャンログの確認が可能



Dr.Web FixIt!：インシデント調査

「情報インフラへの不正侵入」「既に実行された攻撃の足跡」「現在実行中の攻撃」に対して、データ収集・解析を行い修復メカニズムを生成するためのコマンドを作成するユーティリティです

- 診断ユーティティにより以下のデータの収集、解析を実行
  「インストールされたプログラムおよびアップデート」「起動中のプロセス、または既に起動されたプロセス」
  「レジストリに書き込まれた不審なエントリの有無」「レジストリに書き込まれた不審なエントリと他のオブジェクトとの関係」
  「インストールされたドライバー、ブラウザ拡張」「プロセス上にダウンロードされたモジュール」
  「システムログ」「ブートキットに隠されたものを含むディスクのセクター」
- 解析されたデータを元に、悪意あるアクティビティに対してのコマンドツールを作成
- 悪意のあるオブジェクトに対するコマンドツールによる処理に応じて、修復ツールを作成

検出事例と導入事例

Dr.Web Cure Net!での検出事例

メーカー	検査台数	感染台数	感染割合
A社	**448台**	**190台**	**42.4%**
B社	**1,078台**	**387台**	**35.9%**
C社	**1,343台**	**452台**	**33.6%**

大手アンチウイルスソフト利用者でも感染率が高い

他社で検出されないマルウェアを検出可能

導入事例①

某公立大学 様

Windows末数	800台

以前からT社のアンチウィルスを利用。日頃から動作が重く、特にWindows10に入れ替えてから不具合が頻発。
そんな中、2017年初めにランサムウェアに感染し、検知漏れが発覚。移行を決心し評価開始。
Dr.Web CureIt!でスキャンした結果、既存アンチウィルスより良い検知結果が得られ、Dr.Webへの移行を決定。

point 1

検出率を体感

導入前に10台ほどのパソコンでDr.Web CureIt!のスキャン実施。多くのマルウェアが潜伏していた。

point 2

最新OSとの相性

Windows の最新OSに迅速に対応しており、他社で発生するような不具合がなく安定稼働が見込まれる。

導入事例②

エスケー化研株式会社様

Windows端末数	2,200台

（2024年5月末現在）

E社製品がバージョンアップとともに動作が重くなりブラウザの挙動も不安定に。また、いくつかのランサムウェアが検知されなかったことから、販売店経由での情報からをきっかけに、まずDr.Web CureNetでランサムウェアを検知。その後、Dr.Web Desktop Security Suite と 新鋭C社との比較検証を経て、誤検知が少なかったDr.Webの採用。海外含めた5拠点で計画的に段階導入を行い本番導入に至る。

point 1

動作が軽くなった

古いバージョンとの相性が問題であった が、Dr.Webでは解決。快適かつ高い精度でアンチウィルスを実現。

point 2

ランサムウェア対策

従来使っていた製品では検知出来なかったランサムウェアをしっかりと検知出来た。

導入事例③

某社様

Windows端末数	8,000台

従業員から利用中のPCの動作がおかしいという報告があり調査を行った。インストール済みのアンチウイルスソフトや診断ツールを使用しても情報が得られなかったのでDr.Web FixIt!での調査を行う。
対象PCのデータを収集、解析を行った結果APT攻撃であることが究明できた。 Dr.Web FixIt!で修復プログラムのツールを作成でき、オブジェクトに対して駆除、修復ができた。

point 1

メーカーを選ばない

元々、異なるメーカーのアンチウイルスソフトを稼働させていたが、データ収集、解析、駆除、修復が行えた。

point 2

専門知識が不要

インシデント調査に関する専門的な知識や技術を持っていなくても調査が可能だった。EDRを運用するためのような専門スタッフは必要としなかった。

今後とも宜しくお願い致します。

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