Dr.WEB

Dr.Web FixIt!

インシデント調査の新たなソリューション

情報インフラへの不正侵入、既に実行された攻撃の足跡、
現在実行中の攻撃を検知し、システムを修復。

Dr.Web FixIt!サービス

Dr.Web FixIt!は、潜在的な脅威や検知された感染を修復するツールです。Microsoft Windowsが動作するPCおよびサーバのセキュリティを解析します。インストールは不要で、既存のアンチウイルス製品と競合しません。

Dr.Web FixIt!の実行は、以下のフェーズから構成されます:

1. システム検査: ユーザーシステムからデータを収集

2. 取集されたデータの解析および修復に必要なメカニズムの策定

3. システム修復: 検出された感染済みオブジェクトの駆除、情報セキュリティポリシー違反の修復、標的型攻撃からシステムの修復

1. システム検査

本サービスは、**診断ユーティリティDr.Web FixIt!** をビルドします。
このユーティリティは、下記のデータを収集・解析をします。

- 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、
  その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

Dr.WEB

2. 収集されたデータの解析

診断ユーティリティにより作成されたレポートは、Dr.Web FixIt!上にアップロードされた後、 お客様が収集したデータの解析を行います。
その際、Dr.Web FixIt! では**フィルター**が用いられます。過去にユーティリティを起動したことがある場合、システム状態に関する前回レポートとの比較を行います。結果、悪意性のあるアクティビティが検出され、オペレーターはそのオブジェクトに対する処理を選択します。

> Doctor Webのスペシャリストによって開発されたフィルターにより、 IT スペシャリストのチーム全体が作業を行い、段階的にデータを収集し、感染ターゲットを分析して修復メカニズムを生成することが出来ます。

Dr.WEB

3. 修復

選択された悪意のあるオブジェクトに対する処理に応じて、修復ユーティリティ Dr.Web FixIt! がビルドされます。その後、インシデントによる影響が完全に修復されるまで、システムの検査が繰り返し実施されます。

> 修復ユーティリティ Dr.Web FixIt! のビルドは、特定の状況に対応するユニークなものです。診断ユーティリティにより収集されたレポートに基づき、その状況において必要なコマンドを実行します。

ウイルスデータベースを使用して既知の悪意のあるプログラム (またはそれに類似したプログラム) を検出するよう設計された製品とは異なり、Dr.Web FixIt! は他のどのツールでも検出不可能な、まったく新し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します。

本サービスでは、Doctor Webのスペシャリストにより策定されたプリインストールフィルター、またはお客様が指定した独自のフィルターを使用して、収集されたデータを解析します。

Dr.WEB

Konstantin Yudin
コンスタンチン・ユーディン

Doctor Web
プロジェクトマネージャ

“システム感染、検知パターンや脅威の修復に関する社内の知識を蓄積するためのサービスを開発するアイディアが生まれました。

Dr.Web FixIt!は、ユーザーのシステムに関する膨大なデータを収集します。具体的な目的によって、オペレーターは解析に必要なデータを選択できるため、システム上で必要な修復を迅速に実施できます。

Dr.Web FixIt!において一番重要なものは、ユニークなフィルターです。このフィルターを用いて、膨大なデータから必要なデータ、感染、不具合、異常を特定します。”

Dr.WEB

Dr.Web FixIt!ライセンス購入のルール

- 本サービスは、タスク単位でライセンスされます。

> **タスク** とは、1台のPCまたはサーバーにて、Dr.Web FixIt!による3つのフェーズ(データ収集、データ解析、修復) を実行する単位をいいます。

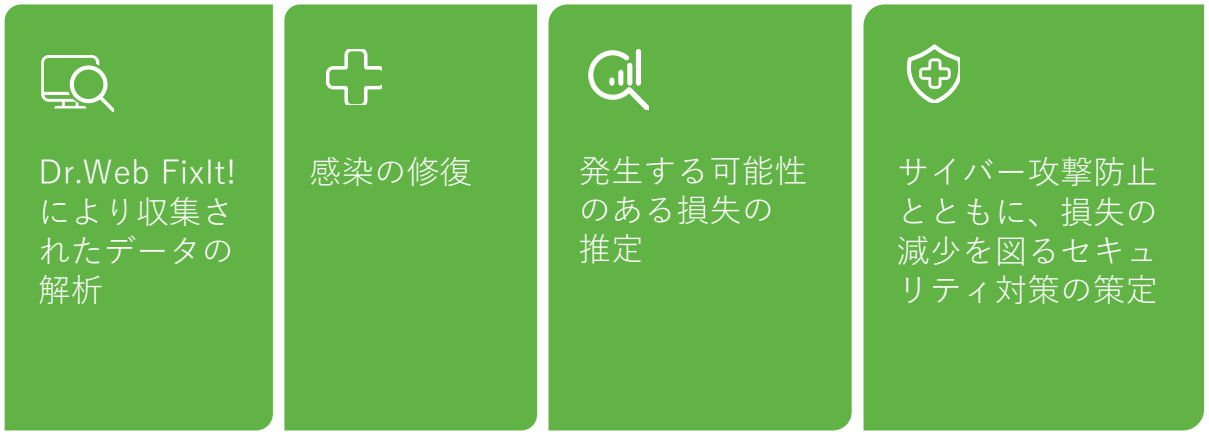
- Dr.Web FixIt!ライセンスは、指定された数量(1, 10 , 20 , 50 ,100)のタスクが含まれるパッケージとして購入可能です。ライセンスの有効期間は1年です。

- タスクの処理は、Dr.Web FixIt!のお客様専用ページ経由で行われます。ライセンス有効化後、お客様専用ページへのアクセスが付与されます

- タスクの有効期間は、作成後10日(暦日)以内となります。

スペシャリストによるサポート提供

Doctor Webスペシャリストに依頼可能なオプションサービス：



Doctor Webのスペシャリストによるサポートを受けるには、サポート用サーティフィケイトを購入する必要があります。
1つのサーティフィケイトで1タスクがフォローされます。
サーティフィケイトに有効期間はありません。

Dr.Web FixIt!の利用者とは?
本サービスの活用例について

状況

PCはマルウェアに感染しています。
感染したシステムの迅速な修復が必要です。

解決

Dr.Web FixIt! は、診断ユーティリティを用いて
マルウェアの痕跡を迅速に検出し、修復ユーティ
リティが感染や潜在的な脅威を駆除します。

状況

企業ネットワーク内にマルウェアが仕掛けられている疑いがあります。

ネットワークのセキュリティ状態を早急に調査する必要があります。

解決

Dr.Web FixIt! は、不正侵入の痕跡を早急に解析し、サーバーやPCのデータを収集します。そして、注意すべき箇所を特定したうえで、感染や潜在的な脅威を駆除するユーティリティをビルドします。

状況

情報セキュリティ部門はインシデント発生を検知し、それを修復しました。しかし、その発生原因は不明なままです。

インシデント発生原因究明のために、発生に至った経緯を調査し、発生原因を特定する必要があります。

解決

Dr.Web FixIt! を用いて、ログを含む発生原因のデータを収集し、遡りで解析を行い、クリティカルなサービスやプログラムの振る舞いを辿ります。また、 Dr.Web vxCubeを利用してラボで不審なファイルを解析するために、そのファイルをアップロードできます。

状況

従業員から社内PCの動作がおかしいという報告がありました。しかし、情報セキュリティ部門は、その原因を究明できません。また、インストール済みのアンチウイルスや診断ツールを使用しても、有益な情報を得ることができませんでした。

異常な動作の原因を究明する必要があります。

解決

Dr.Web FixIt! を用いると、他社製のアンチウイルスがインストールされている場合でも、ユーザーのPCを解析し、システム動作の異常性を究明し、それを修復することができます。

Dr.WEB

状況

社内に、セキュリティ面で極めて重要なPCがあります。
企業ネットワーク内に存在するそのPCに対して、
定期的検査を行う必要があります。

解決

Dr.Web FixIt! を用いると、対象となるPCの動作を検査
することで、PCを定期的かつ隠蔽し実施される APT攻撃
（持続的標的型攻撃）を検知できます。

Dr.WEB

状況

現状、情報セキュリティ部門ではインシデントの発生を徹底調査するための知識や技術を十分に持っていません。そのため、感染したシステムの早急な修復、潜在的な脅威への防止対策、インシデント発生原因の究明などを提供するソリューションが必要となります。

解決

Dr.Web FixIt!は、セキュリティインシデントの発生を調査する以外に、発生原因究明やシステム修復を行います。
社内ネットワーク全体を診断する必要は無く、また高額なEDRソリューションで必要とされるような膨大なインシデント管理業務、そのための専任スタッフを必要としません。

状況

リモートワークを行う従業員は、個人所有PCで業務を行う場合があります。こういった場合においても、PCの脅威検査を行う必要があります。

解決

Dr.Web FixIt!を用いて、従業員はリモートでビルドされた診断用ユーティリティを自身のPC上で起動することができます。これにより、システム保護の問題の有無をチェックできるほか、感染を修復できます。検査を定期的に実施することが可能です。

状況

企業で働く社外スタッフのPCにおいて、情報セキュリティポリシーの違反が発生している疑いがあります。
情報セキュリティポリシーの違反（例えば、OSの設定不備、制限対象のソフトウェアの利用など）をチェックする必要があります。

解決

Dr.Web FixIt! を用いると、社内情報セキュリティポリシーの違反を早急に検知し、システム修復を行えます。

Dr.WEB

例：

- Dr.Web FixIt!の100 タスクの価格：
  ¥38,500
- Dr.Web FixIt!のサポート用
  サーティフィケイト(1タスクごと)x1
  の価格：
  ¥35,000

Dr.WEB

Dr.Web FixIt!によって、各国の様々な政府機関に対する標的型攻撃を検知しました。

被害を受ける前に潜在的な脅威を検出することが今やマストとなります!

fixit.drweb.com/login