Dr.WEB®
Made in Russia

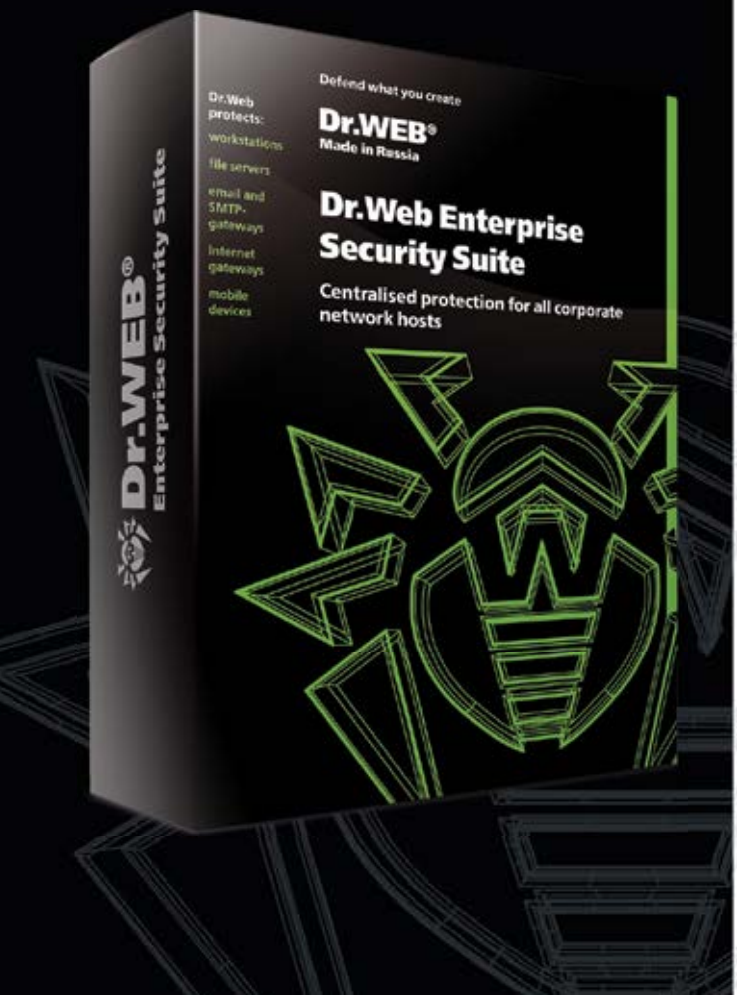
DEFEND WHAT YOU CREATE

Dr.Web Server Security Suite

Novell NetWare対応

www.drweb.co.jp

**ウイルスに対するファイル
ストレージ保護**



Dr.WEB®
since 1992

ファイルサーバーは、安定した事業活動に必要不可欠なものであると同時に、攻撃の対象にもなっています。

従って、サーバーおよび該当サーバー上のさまざまなサービスの安全な動作が、会社のビジネスにとって極めて重要なことです。サイバー犯罪者が、コンピューターを感染させた上で、次に狙うのがサーバーです。

Dr.Webアンチウイルスをインストールすると、サーバーが感染経路となることを防止できます。

Dr.Web for Novell NetWareの主な機能

サーバーボリュームのオンデマンドスキャンとスケジュールスキャン	ファイルシステムの監視	攻撃が実行された時点で未知なる脅威を検出します	ワークステーションから脅威が検出された場合、自動でサーバーからワークステーションを切断

Dr.Web for Novell NetWare の活用によって、企業のコスト削減および安定した事業活動が図られます。

Novell Netwareのあらゆるコンフィギュレーションを保護します
NetWareネームスペースのサポート。複数のネットワークプロトコルの同時サポート。

大量のデータを高速にスキャン
リアルタイムおよびオンデマンドスキャンにおけるシステムリソースを最小限に抑え、大量のデータを高速にスキャンします。
フォーマットを指定してファイルのスキャン、拡張子、ディレクトリおよびボリューム例外のリストを使用したすべてのオブジェクトをスキャンします。

ユーザーフレンドリー
スキャンおよび検出されたウイルスまたは疑わしいファイルに対するアクションの柔軟な設定。
容易なインストールを可能にしたほかに、ユーザーコントロールパネルも実装されます。

アンチウイルスの管理 サーバコン
ソールまたはリモートコンソールからのアンチウイルス管理：通知システムの設定、保護の監視、および設定の最適化

マルチスレッドスキャン
サーバー経由で転送される全てのファイルをオンザフライでスキャンします。
パックファイル、アーカイブファイル、メールファイルに対するスキャン、さらにはオンデマンドスキャン、スケジュールスキャンが用意されます。

スキャンプロセスの優先度の調整
スキャンプロセスの優先度の調整による、CPUリソース消費の管理

Dr.WEB®
since 1992

感染オブジェクトの修復、削除、隔離
ウイルスデータベースの自動更新

アンチウイルスのアクションログ
プロセスの稼働時間、スキャンされたファイルの数、検出されたウイルスに関するスキャンの統計。さらに、スキャンログ、ログの詳細を指定可能。

感染オブジェクト検出時の通知
メールによる管理者とそのグループへの即時通知。
通知のカスタマイズ。

Dr.Web for Novell NetWareライセンス購入のルール

ライセンスの種類	ライセンスのオプション
■ サーバー単位のライセンス	■ アンチウイルス ■ アンチウイルス +Control Center Control Centerライセンスが無料です。 ライセンス購入ルールの詳細はこち https://license.drweb.co.jp/sss/?lng=ja

購入される前のサポート	テクニカルサポート
■ Dr.Web製品の無料テスト ■ オンラインゼミナール、プレゼンテーション実施 ■ テクニカル要件定義書の作成をサポートします ■ Dr.Web製品管理に関する無料トレーニングコース	■ https://support.drweb.co.jp/?lng=jaにて問い合わせフォーム経由でのサポート可能 ■ ライセンス価格リストに記載された数量の範囲であれば、暗号化ランサムウェアに暗号化されたファイルの復号サービス、およびサポートを無料で提供します。 ■ ライセンス価格リストに記載のない数量の場合や無制限ライセンスの場合、サポート価格は別途決定されます。 ■ 有料VIPサポート

サービス

Dr.Web vxCube

- 不審なオブジェクトを解析するインタラクティブなクラウド型インテリジェントアナライザーです。
- 解析を実施後に、直ちに必要な修復ユーティリティのビルドを提供します。
- 情報セキュリティエキスパート、サイバー犯罪捜査官向け

ご利用のアンチウイルスによるスキャン結果では何も検出されていない状況でも疑問が残ったり、またアンチウイルスに保護されているネットワーク上に悪意のあるファイルが仕掛けられてしまった場合、クラウド型インテリジェントアナライザーDr.Web vxCubeが役立ちます。

スキャン開始から1分後には、ファイルの悪意の有無を明らかにするだけでなく、ファイルが行ったシステムへの改変、具体的なリソースとの連携、ネットワーク上の活動マップ等その挙動に関する詳細な報告を入手できます(ビデオフォーマット形式可)。

対象のオブジェクトが明らかに脅威であると判定された場合には、解析されたファイルが行った対処からご利用のシステムを修復するために、Dr.Web CureIt!の特別なビルドが提供されます(ライセンス内容に含まれる場合)。

Dr.WEB®
since 1992

Dr.Web vxCubeを利用すると、アンチウイルスの更新がダウンロードされる前に、最新タイプの脅威に即座に対応します。

Dr.Web CureIt!は、インストールが不要で、他社アンチウイルス(Dr.Webではないアンチウイルス)がインストールされているシステム上に動作することができるユニバーサルなタイプのユーティリティであるため、主要なアンチウイルスソリューションとして、まだDr.Webを利用していない企業にとって、本サービスの利用は非常に効果的です。

トライアル版はこちらhttps://download.drweb.co.jp/vxcube/?lng=ja

Dr.Web vxCubeについての詳細な情報はこちら https://www.drweb.co.jp/vxcube/

ウイルス解析サービス

Doctor Webのアンチウイルスラボのスペシャリストによる悪意のあるファイル解析

Dr.Web vxCubeが行った解析の結果、対象のファイルについてその悪意性が確実ではないということになり、ユーザーはその点で疑問を感じる場合、豊富な経験を積んだDoctor Webのアンチウイルスラボのスペシャリストに解析を依頼することができます。

本サービスには、下記のように、さまざまな悪意のあるファイルの解析および報告の作成が含まれます。

- マルウェア動作およびそのマルウェアのモジュールのアルゴリズムを解説します
- 明らかに悪意のある、悪意になる可能性がある(不審)等のカテゴリー別にオブジェクトを分類します
- ネットワークプロトコルを解析するほか、コマンドサーバーを検出します
- 感染されたシステムへの影響の解析および修復対策に関するアドバイスを提供します

ウイルス解析サービスの依頼はこのページで行ってくださいhttps://support.drweb.co.jp

ウイルス関連インシデント (VCI) の調査

御社はマルウェアのせいでダメージを受けており、ウイルスアナリストによる調査を希望される場合、Doctor Web特別部門が提供するサービスを是非ご検討ください。

ウイルス関連インシデント (VCI) の調査について: https://antifraud.drweb.co.jp/expertise?lng=ja

ウイルス関連インシデント (VCI) 調査の依頼: https://support.drweb.com/expertise

Doctor Webは、ロシアに本社を置く、『Dr.Webアンチウイルスソフトウェア』のデベロッパーです。その製品の開発は1992年に始まりました。

3rd street Yamskogo polya 2-12 A , Moscow, Russia, 125040
Tel.: +7 (495) 789–45–87 Fax: +7 (495) 789–45–97

https://www.drweb.co.jp • https://free.drweb.co.jp • https://curenet.drweb.co.jp