

 **Dr.WEB®**
CureNet!

Defend what you create

クイックスタート

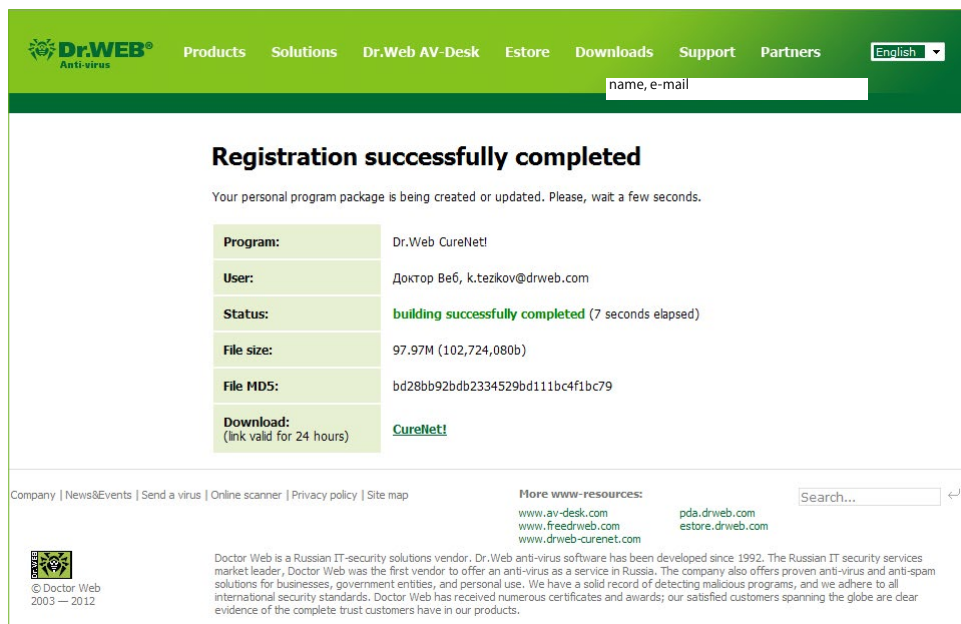


Dr.Web CureNet! は、スキャン対象となるシステム上にアンチウイルスソフトウェアをインストールすることなく、ネットワーク内のコンピューターを集中管理によってリモートスキャンすることが出来ます。また、あらゆるトポロジーのネットワーク内に含まれる、Microsoft® Windows®を搭載するコンピューター及びサーバーのスキャンを行います。

注意! Dr.Web CureNet!は常駐型のエンドポイントセキュリティを提供するものではありません。このソリューションがスキャンを行っていない間に、コンピューターが悪意のあるプログラムに感染してしまう場合があります。確かなアンチウイルスセキュリティを常時確立するにはDr.Web Security Space ProやDr.Web Enterprise Suiteなどの製品をお使いください。

Dr.Web CureNet! のダウンロード

Dr.Web CureNet!のディストリビューションファイルをダウンロードするには <https://products.drweb.co.jp/curenet/es+curenet/> ページでシリアル番号を登録してください。登録の完了と同時に個別のディストリビューションファイルが生成されます。「My Dr.Web CureNet!」からディストリビューションファイルをダウンロードしてください。



The screenshot shows the Dr.Web CureNet! registration success page. The header includes the Dr.Web logo and navigation links: Products, Solutions, Dr.Web AV-Desk, Estore, Downloads, Support, Partners. A search bar is present with the text 'name, e-mail'. The main content area displays 'Registration successfully completed' and a message: 'Your personal program package is being created or updated. Please, wait a few seconds.' Below this is a table with registration details:

Program:	Dr.Web CureNet!
User:	Доктор Веб, k.tezkov@drweb.com
Status:	building successfully completed (7 seconds elapsed)
File size:	97.97M (102,724,080b)
File MD5:	bd28bb92bdb2334529bd111bc4f1bc79
Download: (link valid for 24 hours)	CureNet!

The footer contains contact information, a search bar, and a disclaimer: 'Doctor Web is a Russian IT-security solutions vendor. Dr.Web anti-virus software has been developed since 1992. The Russian IT security services market leader, Doctor Web was the first vendor to offer an anti-virus as a service in Russia. The company also offers proven anti-virus and anti-spam solutions for businesses, government entities, and personal use. We have a solid record of detecting malicious programs, and we adhere to all international security standards. Doctor Web has received numerous certificates and awards; our satisfied customers spanning the globe are clear evidence of the complete trust customers have in our products.'

<http://support.drweb.com/get+cabinet+link/>でのシリアル番号登録完了後は、プログラムのインターフェースから「My Dr.Web CureNet!」にアクセスすることが可能です。

既にDr.Web CureNet!シリアル番号を登録されているユーザーは、そのまま「My Dr.Web CureNet!」にログインし、最新バージョンのディストリビューションファイルをダウンロードしてください。

システム要件

Dr.Web CureNet!によるコンピューターのリモートスキャン実行に必要な要件:

- 対象となるシステムがネットワークに接続されている
- Dr.Web CureNet!がリモートコンピューターに接続するためのアカウントが、必要な管理者権限によって作成されている
- 対象となるシステム上で139番ポート及び445番ポートが開いている
 - Dr.Web CureNet!によるネットワークスキャンの実行には、ワークステーション及びサーバーでの管理者権限が必要です。
 - コンピューターがドメインに属しており、ドメイン管理者アカウントが使用されている場合、リモートスキャンの実行にコンピューターの追加設定は必要ありません。

3. リモートコンピューターがドメインに属していない、又はローカルアカウントが使用されている場合、Windowsのバージョンによってはリモートコンピューターに追加設定が必要となります。ネットワークの設定については本書に記載された手順、又は動画による説明をご覧ください。
4. リモートコンピュータースキャンの設定によって、それらコンピューターのセキュリティが低下する場合があります。そのため設定を変更する前には、変更によるシステム動作への影響についてお読みいただくか、ドメインの無い又はローカルアカウントを使用しているリモートコンピューター上ではリモートスキャンを行わずにアンチウイルススキャンを実行することを推奨します。

Windows 2000システム設定:

5. 管理者アカウントを有効にする
6. ネットワークコンポーネントを設定する

重要! Pack 4 Rollup 1がシステム上にインストールされている必要があります。

Service Pack 4 for Windows 2000をダウンロード:

<http://www.microsoft.com/ja-jp/download/details.aspx?id=7506>

Update Rollup 1 for Windows 2000 SP4をダウンロード:

<http://www.microsoft.com/ja-jp/download/details.aspx?id=18997>

1. 管理者アカウントを有効にする

[スタート] – [設定] – [コントロールパネル] – [管理ツール] – [コンピュータの管理] – [ローカルユーザーとグループ] – [ユーザー] をクリックします。Administrator アカウントのパラメータを調整することも可能ですが、新しい管理者アカウントを作成することを推奨します。右のペイン内で右クリックし、コンテキストメニューから **新しいユーザー** を選択してください。

- ユーザー名に DrWebCurenet と入力します。
- パスワード 及び パスワードの確認入力 フィールドには強固なパスワードを入力してください。
- ユーザーは次回ログオン時にパスワードの変更が必要を無効にします。
- パスワードを無期限にする チェックボックスにチェックを入れます。
- 作成 をクリックした後、閉じる をクリックしてください。

作成されたDrWebCurenetアカウントをダブルクリックし、所属するグループ タブを開きます。Users を選択し 削除 をクリックします。グループの選択 ダイアログ内で Administrators を選択して 追加 をクリックしてください。次に OK をクリックし、DrWebCurenet プロパティウィンドウ内で 適用 → OK の順にクリックします。

2. ネットワークコンポーネントを設定する

[スタート] – [設定] – [ネットワークとダイヤルアップ接続] をクリックします。ネットワーク接続を選択して右クリックし、コンテキストメニューから プロパティ を選択してください。

次のコンポーネントが有効になっていることを確認してください。

- Microsoft ネットワーク用クライアント
- Microsoft ネットワーク用ファイルとプリンタ共有
- インターネットプロトコル (TCP/IP)

OK をクリックします。

ファイアウォールを使用する場合は139番ポート及び445番ポートを開いてください。

Windows XP (Windows 2003) システム設定:

1. 管理者アカウントを有効にする
2. ファイル共有を設定する (Windows 2003では必要ありません)
3. ローカルセキュリティポリシーを設定する
4. Windows ファイアーウォールを設定する
5. ネットワークコンポーネントを設定する

重要! Windows XPでは、Service Pack 2又は3 がインストールされている必要があります。

Service Pack 2 for Windows XPのダウンロード: <http://www.microsoft.com/ja-jp/download/details.aspx?id=28>

Service Pack 3 for Windows XPのダウンロード: <http://www.microsoft.com/ja-jp/download/details.aspx?id=24>

対応エディション:

- Windows XP Professional;

以下のエディションではプログラムのリモート実行がサポートされていないため、Dr.Web CureNet! を動作させることは出来ません。

- Windows XP Starter;
- Windows XP Home Edition.

Windows 2003では、Service Pack 1又は2 がインストールされている必要があります。

Service Pack 1 for Windows 2003のダウンロード: <http://www.microsoft.com/ja-jp/download/details.aspx?id=11435>

Service Pack 2 for Windows 2003 (推奨) のダウンロード:

<http://www.microsoft.com/ja-jp/download/details.aspx?id=41>

1. 管理者アカウントを有効にする

[スタート] – [コントロールパネル] – [ユーザーアカウント] – [ユーザー管理の詳細設定] – [ローカルユーザーとグループ] – [ユーザー] をクリックします。Administrator アカウントのパラメータを調整することも可能ですが、新しい管理者アカウントを作成することを推奨します。右のペイン内で右クリックし、コンテキストメニューから **新しいユーザー** を選択してください。ユーザー名に Dr.WebCureNET と入力します。パスワード 及び パスワードの確認入力 フィールドには強固なパスワードを入力してください。ユーザーは次回ログオン時にパスワードの変更が必要を無効にし、パスワードを無期限にする チェックボックスにチェックを入れます。作成 をクリックした後、閉じる をクリックしてください。作成されたDrWebCurenetアカウントアイコンをダブルクリックし、プロパティウィンドウを開きます。所属するグループ タブを開き、Users を選択して 削除 をクリックした後に 追加 をクリックします。開いた グループの選択 ウィンドウ内で 詳細設定 を選択して 今すぐ検索 をクリックしてください。表示されたリスト上で Administrators を選択し、OK をクリックします。グループの選択 ウィンドウ内でもう一度OKをクリックしてください。DrWebCurenet プロパティウィンドウ内で 適用 → OK の順にクリックします。

2. ファイル共有を設定する

[スタート] – [コントロールパネル] – [クラシック表示に切り替える] – [フォルダオプション] をクリックします。フォルダオプション ウィンドウが開きます。表示 タブを開き、簡易ファイルの共有を使用する チェックボックスのチェックを外してください。適用 → OK の順にクリックします。

3. ローカルセキュリティポリシーを設定する

[コントロールパネル] - [管理ツール] - [ローカルセキュリティポリシー] - [ローカルポリシー] - [セキュリティオプション] を開き、ネットワーク アクセス: ローカル アカウントの共有とセキュリティモデル 上にカーソルを合わせてエントリをダブルクリックします。クラシックオプションを選択し、適用 → OK の順にクリックしてください。ローカルセキュリティ設定 ウィンドウを閉じます。

4. ファイアウォールを設定する

Windowsファイアウォール以外のファイアウォールを使用する場合は、139番ポート及び445番ポートを開いてください。Windowsファイアウォールを使用する場合は [スタート] - [コントロールパネル] - [Windowsファイアウォール] をクリックし、例外 タブを開きます。ファイルとプリンタの共有 チェックボックスにチェックを入れ、OK をクリックしてください。.

5. ネットワークコンポーネントを設定する

[スタート] - [コントロールパネル] - [ネットワーク接続] をクリックします。ネットワーク接続を右クリックしてコンテキストメニューから プロパティ を選択し、開いたウィンドウの 全般 タブ内で以下のコンポーネントが有効になっていることを確認してください。

- Microsoft ネットワーク用クライアント
- Microsoft ネットワーク用ファイルとプリンタ共有
- インターネットプロトコル (TCP/IP)

OK をクリックします。

Windows Vistaシステム設定:

1. User Account Control を設定する
2. ファイル共有を設定する
3. 管理者アカウントを有効にする
4. Windows ファイアウォールを設定する
5. ネットワークコンポーネントを設定する
6. ローカルセキュリティポリシーを設定する

重要! Windows Vista では、Service Pack 1 又は 2 がインストールされている必要があります。

Service Pack 1 for Windows Vistaのダウンロード: <http://www.microsoft.com/ja-jp/download/details.aspx?id=910>

Service Pack 2 for Windows Vista (推奨) のダウンロード:

<http://www.microsoft.com/ja-jp/download/details.aspx?id=15278>

対応エディション:

- Windows Vista Business;
- Windows Vista Enterprise;
- Windows Vista Ultimate.

以下のエディションではプログラムのリモート実行がサポートされていないため、Dr.Web CureNet!を動作させることは出来ません。

- Windows Vista Starter;
- Windows Vista Home Basic;
- Windows Vista Home Premium.

1. UAC が有効になっている場合、以下の手順を実行してください。

- Windows+R キーを押します。開いたウィンドウ内で«Regedit»と入力 (引用符無しで) し、Enter キーを押してください。レジストリエディタ ウィンドウが開きます。
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] に移動します。
- レジストリエディタ ウィンドウ内右側のペインで右クリックし、コンテキストメニューから **新規** を選択した後32-bit DWORD value を選択します。パラメータ名に«LocalAccountTokenFilterPolicy»を指定します (引用符無しで)。
- 新規作成されたキーをダブルクリックします。開いた DWORD 編集ウィンドウ内で値に1を設定し、OK をクリックしてください。
- レジストリエディタ を閉じます。

2. ファイル共有を設定する

[スタート] – [コントロールパネル] – [ネットワークとインターネット] – [ネットワークと共有センター] – [共有と探索] を開き、ネットワーク探索 及び ファイル共有を有効にします。

3. 管理者アカウントを有効にする

[スタート] – [コントロールパネル] – [システムとメンテナンス] – [管理ツール] – [コンピューターの管理] – [ローカルユーザーとグループ] – [ユーザー] を選択します。Administrator アカウントのパラメータを調整することも可能ですが、新しい管理者アカウントを作成することを推奨します。中央ペイン内で右クリックし、コンテキストメニューから **新しいユーザー** を選択してください。

- ユーザー名に DrWebCurenet と入力します。
- パスワード 及び パスワードの確認入力 フィールドには強固なパスワードを入力してください。
- ユーザーは次回ログオン時にパスワードの変更が必要 を無効にします。
- パスワードを無期限にする チェックボックスにチェックを入れます。
- **作成** をクリックした後、**閉じる** をクリックしてください。

作成された DrWebCurenet アカウントをダブルクリックし、所属するグループ タブ内でUsers を選択して **削除** をクリックします。次に **追加** をクリックして グループの選択 ウィンドウを開きます。詳細設定 をクリックした後 **今すぐ検索** をクリックしてください。検索結果の中からAdministrators を選択して OK をクリックします。グループの選択 ウィンドウ内でも同様にOK をクリックし、DrWebCurenet プロパティウィンドウ内で **適用** → OK の順にクリックします。

4. ファイアウォールを設定する

Windowsファイアウォール以外のファイアウォールを使用する場合は、139番ポート及び445番ポートを開いてください。Windowsファイアウォールを使用する場合は [スタート] – [コントロールパネル] – [セキュリティ] – [Windowsファイアウォール] を開き、Windowsファイアウォールによるプログラムの許可 をクリックします。Windowsファイアウォールウィンドウ内で **例外** タブを開き、ファイルとプリンタの共有 チェックボックスにチェックを入れて OK をクリックしてください。

5. ネットワークコンポーネントを設定する

[スタート] – [コントロールパネル] – [システムとメンテナンス] – [ネットワークと共有センター] – [ネットワーク接続の管理] をクリックします。ネットワーク接続アイコンを右クリックし、コンテキストメニューから プロパティ を選択します。以下のコンポーネントが有効になっていることを確認してください。

- Microsoft ネットワーク用クライアント
- Microsoft ネットワーク用ファイルとプリンタ共有
- インターネットプロトコルバージョン4

6. ローカルセキュリティポリシーを設定する

[スタート] – [コントロールパネル] – [管理ツール] – [ローカルセキュリティポリシー] – [ローカルポリシー] – [セキュリティオプション] を開き、ネットワーク アクセス: ローカル アカウントの共有とセキュリティモデル 上にカーソルを合わせてエントリをダブルクリックします。開いた プロパティ ウィンドウ内で クラシックオプションを選択し、OK をクリックしてください。

Windows 7 (Windows 2008、Windows 2008 R2) システム設定:

1. User Account Control を設定する
2. ファイル共有を設定する
3. 管理者アカウントを有効にする
4. Windows ファイアーウォールを設定する
5. ネットワークコンポーネントを設定する
6. ローカルセキュリティポリシーを設定する

重要! 対応エディションは以下のとおりです。

- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate.

以下のエディションではプログラムのリモート実行がサポートされていないため、Dr.Web CureNet!を動作させることは出来ません。

- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium

Windows 2008では、Service Pack 2がインストールされている必要があります。

Service Pack 2 for Windows 2008のダウンロード: <http://www.microsoft.com/ja-jp/download/details.aspx?id=15278>

1. UAC が有効になっている場合、以下の手順を実行してください。

- Windows+R キーを押します。開いたウィンドウ内で「Regedit」と入力（引用符無しで）し、Enter キーを押してください。レジストリエディターが開きます。
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] に移動します。
- レジストリエディター ウィンドウ内右側のペインで右クリックし、コンテキストメニューから **新規** を選択した後32-bit DWORD value を選択します。パラメータ名に「LocalAccountTokenFilterPolicy」を指定します（引用符無しで）。
- 新規作成されたキーをダブルクリックします。開いた DWORD 編集ウィンドウ内で値に1を設定し、OK をクリックしてください。
- レジストリエディター を閉じます。

2. ファイル共有を設定する

[スタート] – [コントロールパネル] – [ネットワークとインターネット] – [ネットワークと共有センター] – [共有の詳細設定の変更] を開き、該当するネットワークプロファイル内で **ネットワーク探索を有効にする** 及び **ファイルとプリンターの共有を有効にする** を選択します。変更の保存 をクリックします。Windows 2008又はWindows 2008 R2の場合、ネットワーク探索を有効にする オプションは使用しないでください。

3. 管理者アカウントを有効にする

[スタート] – [コントロールパネル] – [システムとセキュリティ] – [管理ツール] – [コンピューターの管理] – [ローカルユーザーとグループ] – [ユーザー] を選択します。Administrator アカウントのパラメータを調整することも可能ですが、新しい管理者アカウントを作成することを推奨します。中央ペイン内で右クリックし、コンテキストメニューから **新しいユーザー** を選択してください。

ユーザー名に DrWebCurenet と入力します。

- パスワード 及び パスワードの確認入力 フィールドには強固なパスワードを入力してください。
- ユーザーは次回ログオン時にパスワードの変更が必要 を無効にします。
- パスワードを無期限にする チェックボックスにチェックを入れます。
- 作成 をクリックした後、閉じる をクリックしてください。

作成された DrWebCurenet アカウントをダブルクリックし、所属するグループ タブ内でUsers を選択して **削除** をクリックします。次に **追加** をクリックして グループの選択 ウィンドウを開きます。詳細設定 をクリックした後 **今すぐ検索** をクリックしてください。検索結果の中からAdministrators を選択して OK をクリックします。グループの選択 ウィンドウ内でも同様にOK をクリックし、DrWebCurenet プロパティウィンドウ内で **適用** → **OK** の順にクリックします。

4. ファイアーウォールを設定する

Windowsファイアーウォール以外のファイアーウォールを使用する場合は、139番ポート及び445番ポートを開いてください。Windowsファイアーウォールを使用する場合は [スタート] – [コントロールパネル] – [システムとセキュリティ] – [Windowsファイアーウォール] – [Windowsファイアーウォールを介したプログラムまたは機能を許可する] を開き、設定の変更 をクリックします。ファイルとプリンターの共有 チェックボックスにチェックを入れて OK をクリックしてください。

5. Configure network components

[スタート] – [コントロールパネル] – [ネットワークとインターネット] – [ネットワークと共有センター] – [アダプターの設定の変更] をクリックします。該当するネットワーク接続アイコンを右クリックし、コンテキストメニューから **プロパティ** を選択します。以下のコンポーネントが有効になっていることを確認してください。

- Microsoft ネットワーク用クライアント
- Microsoft ネットワーク用ファイルとプリンター共有
- インターネットプロトコルバージョン4 (TCP / IP v4)

6. ローカルセキュリティポリシーを設定する

[スタート] – [コントロールパネル] – [システムとセキュリティ] – [管理ツール] – [ローカルセキュリティポリシー] – [ローカルポリシー] – [セキュリティオプション] を開き、ネットワーク アクセス: ローカル アカウントの共有とセキュリティモデル 上にカーソルを合わせてエントリをダブルクリックします。開いた プロパティ ウィンドウ内で クラシック を選択し、OK をクリックしてください。

Dr.Web CureNet!の起動

1. ダウンロードしたCureNet!.exe ファイルを実行します。

注意! 2回目以降のDr.Web CureNet!の開始方法は次項を参照してください。

注意! Dr.Web CureNet!は他ベンダーのアンチウイルスソリューションと競合することはありませんが、Dr.Web CureNet!によるシステムのスキャン中には、スキャン速度を向上させるためにそれらのソリューションを無効にしておくことを推奨します。

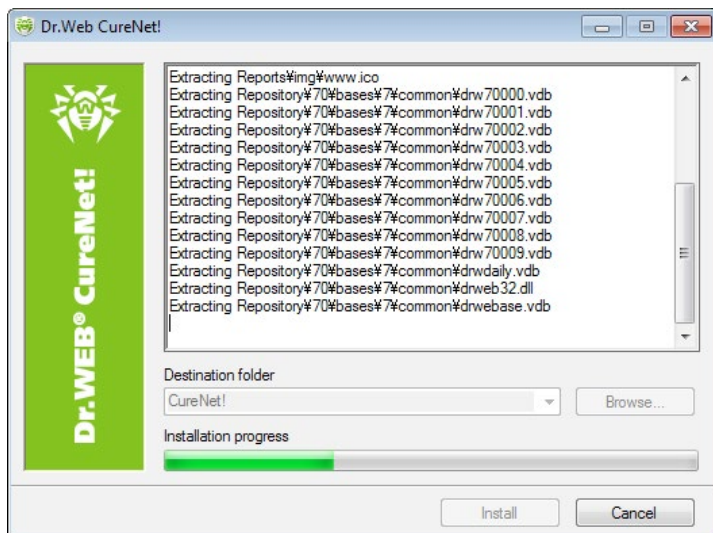
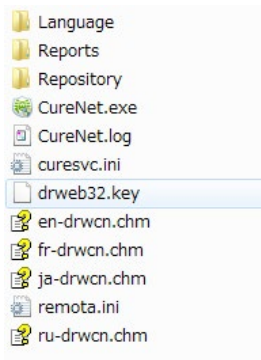
2. インストールを続けるには Install ボタンをクリックしてください。



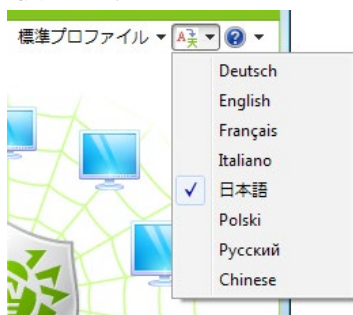
3. デフォルトのディレクトリではなく、指定した場所にDr.Web CureNet!ファイルを保存したい場合は、Browse ボタンをクリックします。

CureNet!.exe は自己展開型アーカイブで、インストールは必要ありません。ユーザーはアーカイブコンテンツの展開先を選択するだけです。デフォルトのフォルダ名はCureNet!ですが、自由に変更することが出来ます。アーカイブファイルをUSB フラッシュドライブやその他のリムーバブルストレージデバイス上に展開することでDr.Web CureNet!を持ち運ぶことができ、必要な時にいつでも利用することが可能です。

製品リポジトリファイル及びキーファイルが展開先フォルダ内に展開されます。



4. 右上端にある ボタンをクリックし、言語を選択します。

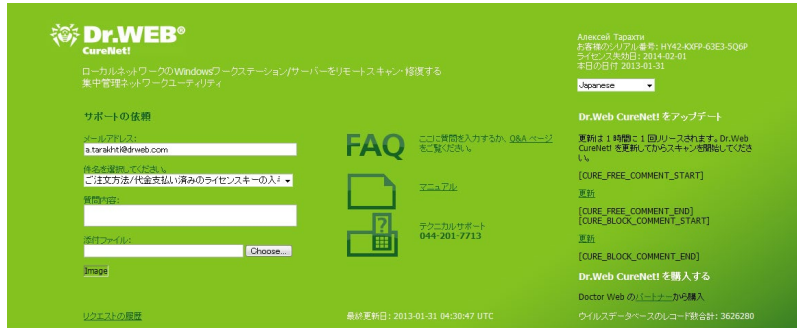


前回のスキャンセッションで保存した設定ファイルがあり、そのファイルを使用したい場合は右上端の 標準プロファイル ボタンをクリックしてファイルをロードしてください。



操作に関する不明な点については ボタンをクリックしてコンテキストメニューから ヘルプ を選択し、開いたユーザーマニュアルを参照してください。My Dr.Web を選択するとユーザーの専用ページが開き、そこからサポートリクエストを送ることが出来ます。

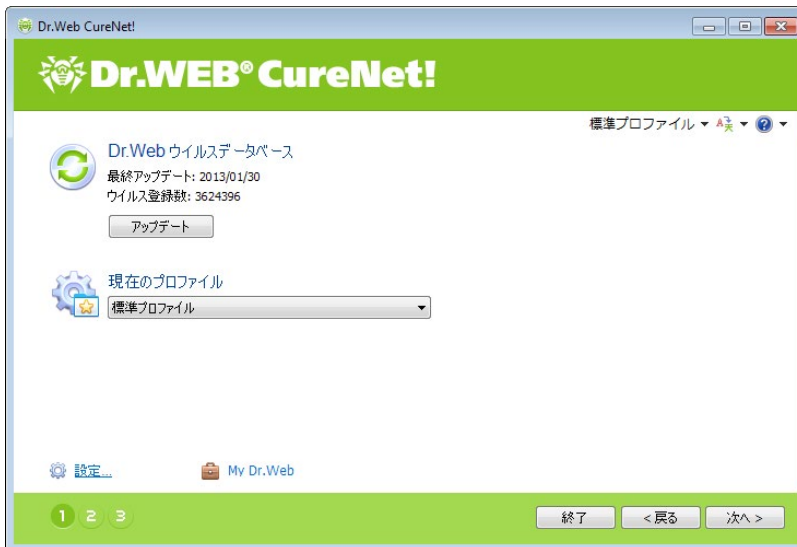
又、このメニューで このプログラムについて を選択し、お使いのライセンスに関する情報を見ることも可能です。



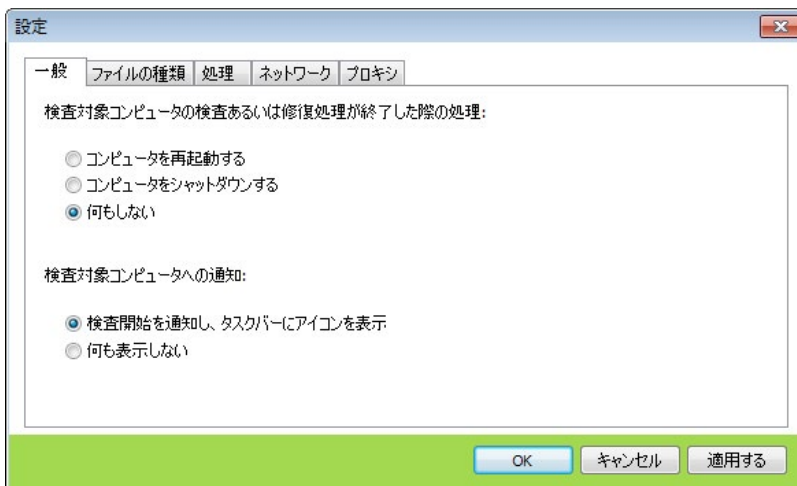
次へ をクリックして先へ進みます。

5. アップデート ボタンをクリックしてウイルスデータベースをアップデートします。

注意! データベース内のウイルス定義は、ウイルスの検出及び駆除の成功に大きく関与します。そのため、Dr.Web CureNet!の起動時には常にデータベースをアップデートすることを強く推奨します。



デフォルト設定を変更する場合は 設定 をクリックしてください。

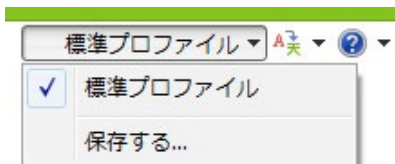


処理 タブでは、異なるタイプの悪意のあるオブジェクトに対してアクションを設定することが出来ます。検出時のデフォルトアクションは、ほとんどのタイプのオブジェクトで 隔離 になっています。

適用可能なアクションは悪意のあるオブジェクトのタイプによって異なります。例えば、感染オブジェクトに対するアクションには レポート、修復、削除、名前の変更、隔離 が含まれていますが、修復不可能なオブジェクトに対しては 修復 は使用できません。

注意! 多くのウイルスの修復にはシステムの再起動が必要になりますが、強制再起動はユーザーの作業を妨げてしまう場合があるため、再起動 オプション (一般 タブ) はデフォルトで無効になっています。システム上でウイルスが検出された場合はユーザーに対して通知を行い、ネットワーク内にある残り全てのシステムをスキャンすることを推奨します。

設定を保存するには 標準プロファイル をクリックし、保存する を選択してください。



注意! 全てのDoctor Web 製品は、デフォルト設定で最適なパフォーマンスを実行するようになっているため、それらの設定は変更せずに使用することを推奨します。

プロファイルを保存してある場合は 現在のプロファイル をクリックし、使用するプロファイルを選択してください。

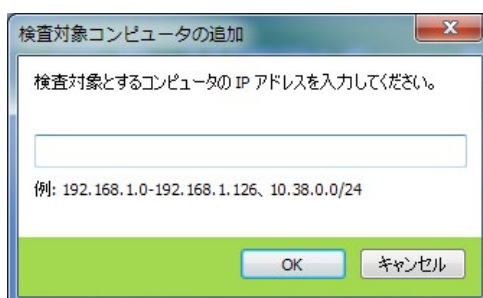


次へ をクリックして先へ進みます。

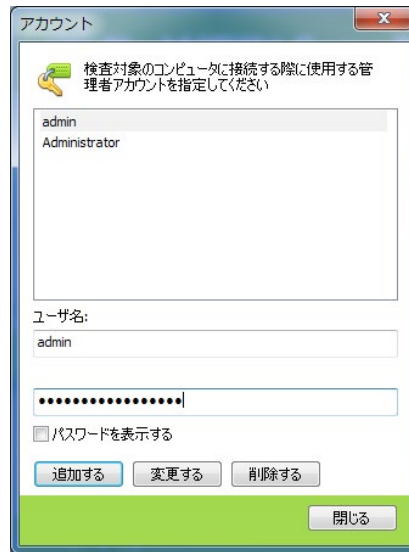
6. 次のウィンドウで、ウイルススキャンの対象となるネットワーク内のコンピューターのリストを作成してください。



ネットワーク内のコンピューターを自動で検索するには 自動検索 をクリックします。リストを手動で作成する場合は 追加する をクリックし、対象となるコンピューターのアドレス又はその範囲内でコンピューターが検索されるアドレスの幅を入力します。



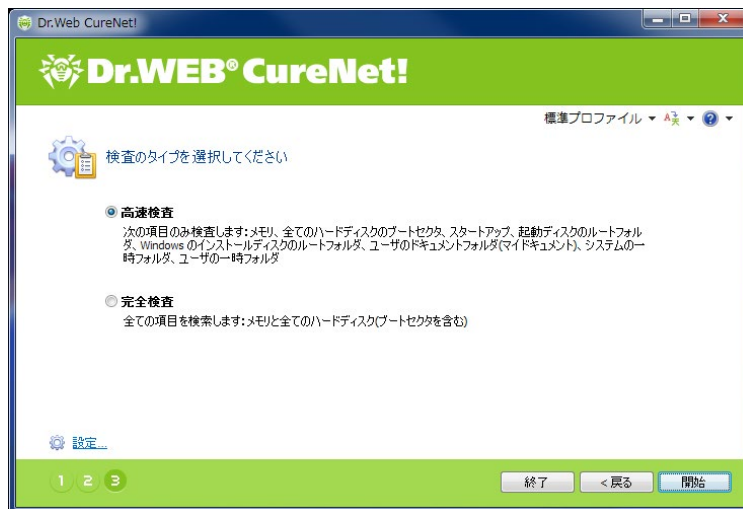
ネットワーク内のコンピューターがドメインに属していない場合、アカウント一覧 をクリックし、開いたウィンドウ内で、対象となる各コンピューターに対してアクセスパスワードを指定してください。



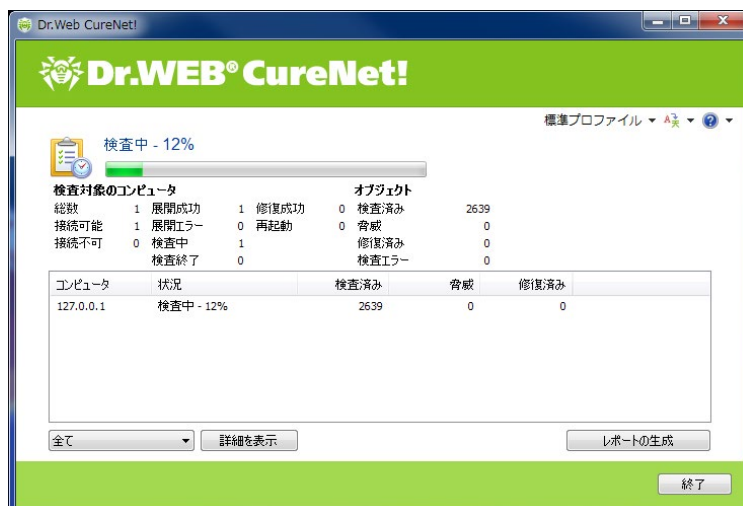
次へ をクリックして先へ進みます。

7. 次のウィンドウで、スキャンのタイプ (高速検査または完全検査) を選択します。

注意! 高速検査 を選択した場合、スキャンの対象となるのはシステムディレクトリ及び動作中のプロセスのみであるため、スキャンや修復 (感染が検出された場合) は完全ではないことがあります。例えば、システム内で活動中のウイルスが、既にスキャン済みの感染していないファイルを感染させてしまう場合もあります。



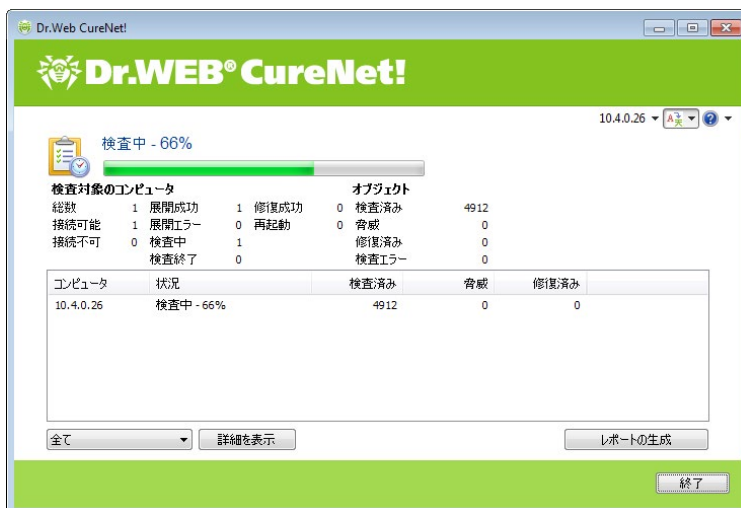
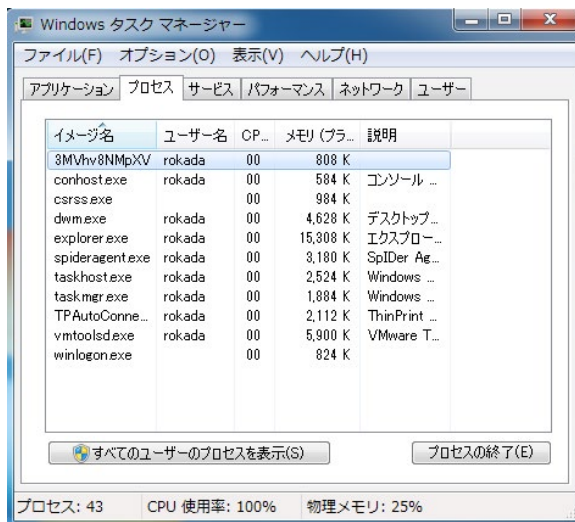
開始 ボタンをクリックします。



このウィンドウでは、リモートコンピューター上で実行中のスキャンの進捗およびその結果が表示されます。統計情報はコンピューター間における接続状態の影響を受けません。接続が切断された場合でも、Dr.Web CureNet!は再接続と同時に統計情報を更新します。

注意! スキャンを完了前に停止することは推奨されません。

実行中のスキャンプロセスには、自身をマルウェアから保護するためのセルフ保護メカニズムが備わっています。



ネットワークスキャンに関するレポートを作成するには レポートの生成 ボタンをクリックしてください。



プログラムを終了するには 終了 をクリックしてください。

製品およびその設定、スキャン、プロファイルの使用方法などに関する詳細はマニュアルを参照してください。

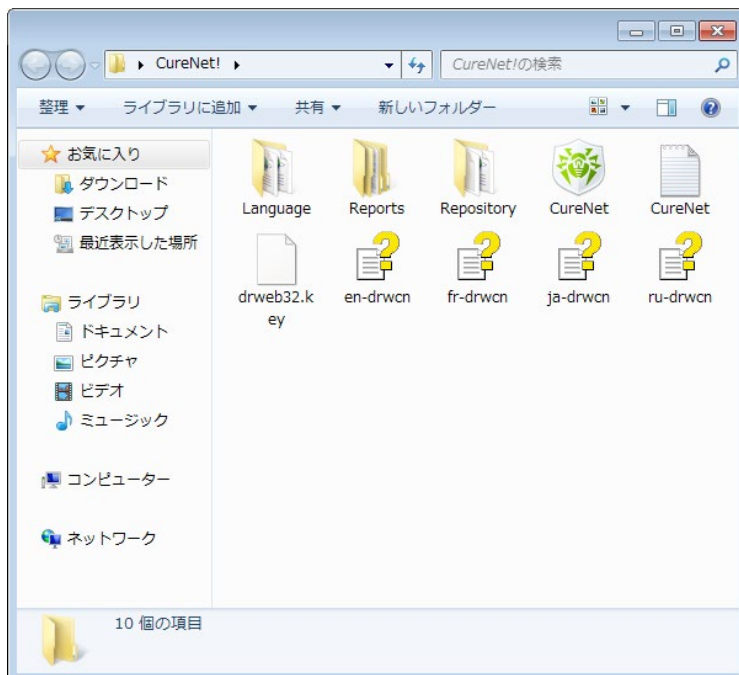
[Dr.Web CureNet! 管理者マニュアル](#)

Dr.Web CureNet!を使用する

アンチウイルススキャンは定期的に行うことを推奨します。特に、ファイルモニターによってスキャンされたディスク上のファイルは、スキャン時点ではアンチウイルスにとって未知であったウイルスを含んでいる場合があります。

スキャンを実行する

1. 初回起動時にDr.Web CureNet!ファイルが保存されたフォルダを開きます。デフォルトでは、デスクトップ上のCureNetフォルダです。



2. Windows 7を使用している場合は、プログラムの起動を許可するためはい ボタンをクリックしてください。




Dr.Web CureNet!の起動後は前述の手順でスキャンを実行することが出来ます。



製品の動作確認

1. ブラウザを立ち上げ、下図アドレスにてテストウイルスを入手します。

 http://www.eicar.org/anti_virus_test_file.htm

2. ページ内で下へスクロールし、下図のテキストを見つけてください。

Download area using the standard protocol http			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes
Download area using the secure, SSL enabled protocol https			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

ダウンロード可能なファイルを選択します (例:最初のファイル [eicar.com](#) を選択)。

3. ダウンロードしたファイルを対象となるコンピューターのデスクトップ上に保存します。

注意! 他ベンダーのアンチウイルス製品が導入されているコンピューター上でDr.Web CureNet!を使用する場合は、ファイルを保存する前にそれらを無効にしてください。

4. Dr.Web CureNet!を起動し、アンチウイルススキャンを実行してください。



© Doctor Web, 2003 – 2012

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi,
Kanagawa-ken 210-0005

Tel.: +81(0) 44-201-7711

www.drweb.co.jp