Dr.Web Desktop Security Suite
Dr.Web Security Space Ver.12
Dr.Web Anti-virus for Windows Ver.12
インストールガイド

株式会社 Doctor Web Pacific

初版 ： 2018/10/30
改訂 ： 2023/04/04

目次

この度は、株式会社 DoctorWebPacific の製品をご購入いただき、誠にありがとうございます。本ガイドは、初めて弊社製品をご利用いただくお客様向けに、弊社アンチウイルスソフトウェア(Dr.Web Security Space および Dr.Web Anti-virus for Windows)をインストールいただくための手順を説明する資料となります。なお、詳細な機能や操作の説明に関しましては、製品マニュアルをご参照ください。

1. はじめに

1.1 ライセンス証書の受領

ライセンス証書は、Doctor Web Pacific(以下、DWP)または、DWP パートナー企業より、電子メールか郵送もしくはその両方の方法で、お客様へ送付いたします。

1.2 ライセンス証書に含まれる内容

ライセンス証書には、以下のライセンスに関する情報が記載されておりますので、大切に保管してください。

- customer (お客様情報)
- product(購入製品名)
- serial number(製品用キーコード)
- license term(ライセンス期間)
- protected objects (購入ライセンス数)

※ “My Dr.Web”につきましては、日本ではご利用できません。

2. 環境前提条件

本書は、下記の環境で動作確認の上作成しております。

- OS：Windows 10 (64bit)
- ブラウザ ：Microsoft Edge

3. 準備

3.1 インストール環境の確認

- 他のアンチウイルスソフトウェアのアンインストール

  Dr.Web Security Space および Dr.Web Anti-virus for Windows のバージョン 12(以下、Dr.Web)のインストールを実行される前に、インストール対象の PC に他のアンチウイルスソフトウェア(異なるバージョンの Dr.Web 製品含む)がインストールされていないことをご確認ください。

  他のアンチウイルスソフトウェアがインストールされている場合、完全に削除(アンインストール)を実施後、Dr.Web バージョン 12 のインストールを実行してください。

- プロキシサーバーの利用

  プロキシサーバーを利用している場合、プロキシサーバーのアドレス、ポート等プロキシサーバーを利用する際に必要な情報を確認してください。

※ メモリ、HDD 容量等については、インストールマニュアルを参照してください。

3.2 ファイル

以下のファイルを用意してください。

インストールファイルおよび Key ファイルの入手方法については、「Dr.Web ダウンロード＆アクティベーションガイド」を参照してください。

1) インストーラー

Windows 用のインストールファイルを用意し、インストール対象の PC にコピーしてください。

※ お持ちのライセンスにより、以下のいずれかの Dr.Web 製品がダウンロードできます。

- Dr.Web Anti-virus (Dr.Web Desktop Security Suite, Anti-Virus, Dr.Web anti-virus for Windows)

  アンチウイルス機能のみが利用できます。

  利用可能な機能 ： SpIDer Guard(常駐保護)、スキャナー、SpIDer Mail、Preventive Protection(予防的保護)、Dr.Web Firewall 等

- Dr.Web Security Space (Dr.Web Desktop Security Suite, Complex protection)

  包括的保護として、アンチウイルス機能に加えさまざまな保護機能が利用できます。

  利用可能な機能 ： SpIDer Guard(常駐保護)、スキャナー、SpIDer Mail、Preventive Protection(予防的保護)、Dr.Web Firewall、アンチスパム、SpIDer Gate、デバイス制御、Parental Control、データ損失防止等

2) Key ファイル

インストール対象の PC にコピーしてください。

3.3 その他注意事項等

- インストール時に使用するユーザ名について

  インストール時に使用するユーザ名が全角で 17 文字以上の場合、インストールに失敗する場合があります。この場合は、インストール用に短い名前のユーザを追加していただき、追加したユーザでインストールを実施してください。

- 環境復元ソフトがインストールされている場合

  環境復元ソフトがインストールされている場合、環境復元ソフトを停止した状態(復元機能が実行されない状態)でインストールを実施してください。インストール完了後は、更新の設定において「データベースのみ」に変更してください。

  また、正常に定義ファイルの更新が行われている状況においても「Dr.Web ウィルスデータベースが最新ではありません」、「コンピューターが脅威に晒される可能性があります」等のメッセージが表示されることがありますが、実際にはディスク内の定義ファイルが読み込まれております。

  ディスク内の定義ファイルの状態につきましては、[ツール]-[サポート]-[詳細]から「プログラムについて」ウィンドウに表示された「ウィルスデータベース」よりご確認ください。

  ※ drwtoday.vdb の日付をご確認ください。

- URL フィルタリングソフトがインストールされている場合

  URL フィルタリングソフトがインストールされている場合、ホームページの閲覧等ができなくなる場合があります。その際は、SpIDer Mail、SpIDer Gate、Dr.Web for MS Outlook、Parental Control をアンインストールしてください。

- ライセンスの有効化

  インストール中およびインストール後に、Dr.Web ライセンスの有効化をする際は、必ず Key ファイルを使用してください。

  シリアル番号を用いたライセンスの有効化は、実行可能な回数に制限があります。

4. インストール

1) インストール対象の端末にコピーした、インストールファイルを実行します。

2) 「ユーザーアカウント制御」の画面が表示されたら、「はい」ボタンをクリックします。

図 1. ユーザーアカウント制御

※ プログラムが実行されると、下記の画像が表示されます。

図 2. プログラム開始

3) 以下の画面が表示されたら、ライセンス使用許諾契約を確認の上、「次へ」ボタンをクリックします。以下の 2 項目については、必要に応じてチェックを入れてください。

- Dr.Web Cloud に接続します
- Dr.Web Firewall をインストールする

≪注意≫Dr.Web Firewall は、**通信の全てを遮断し、PC 利用者の許可によって個々の通信の可否を設定する機能**です。設定には、PC やインターネット、ネットワークに関する知識が要求されますので、全体のセキュリティ対策状況を考慮の上、Dr.Web Firewall のインストールをご判断ください。

図 3. ライセンス同意

※ 画面下部の「インストールパラメータ」をクリックすると、以下の設定を行なうことができます。

- コンポーネント
  インストールするコンポーネントを選択できます。
- インストール
  プログラム本体のインストール先フォルダを変更できます。尚、定義ファイル等が保存されるフォルダは変更できません。
- アドバンスオプション
  インストール中の更新の実施の可否やデスクトップへのショートカットの作成等が選択できます。
- プロキシ
  プロキシサーバーへの接続設定を実施できます。

4) 「登録ウィザード」の画面が表示されたら、「有効なキーファイルのパスを指定する」にチェックを入れ、「参照」ボタンをクリックし、予め PC 上に保存した Key ファイル選択した後、「インストール」ボタンをクリックします。

≪注意≫クリックする前に、必ず他のアンチウイルスがインストールされていないことを確認してください。

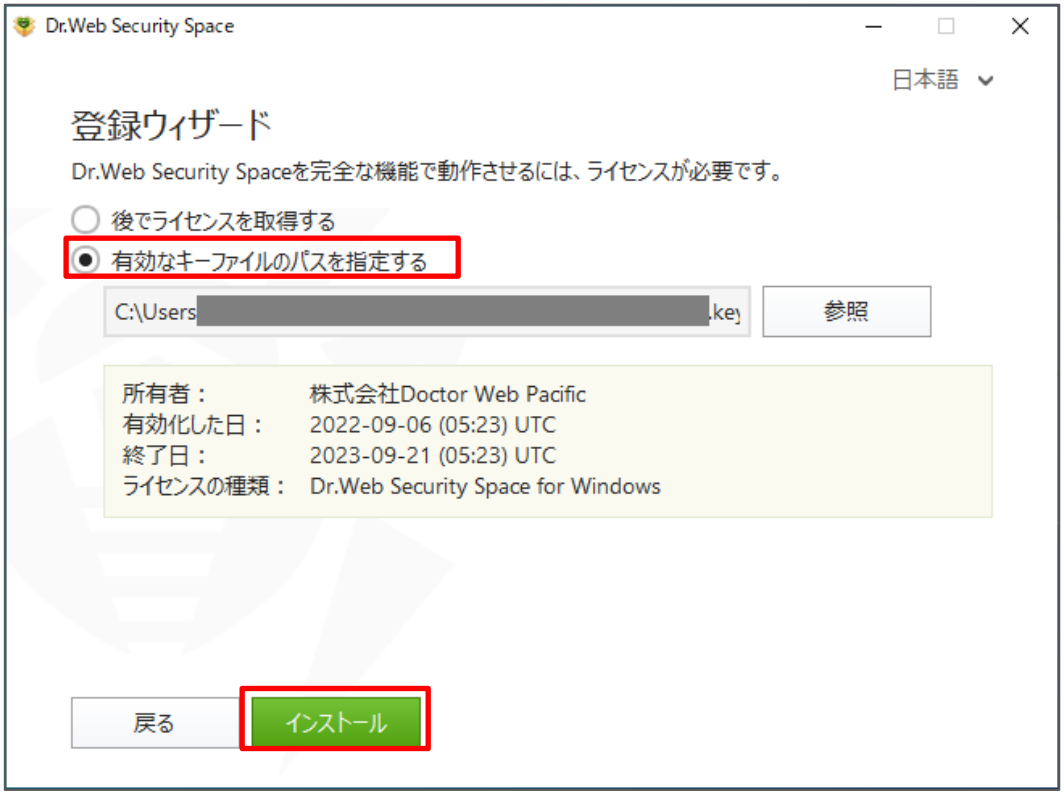

図 4. ライセンス登録&インストール開始

5) インストールが開始します。

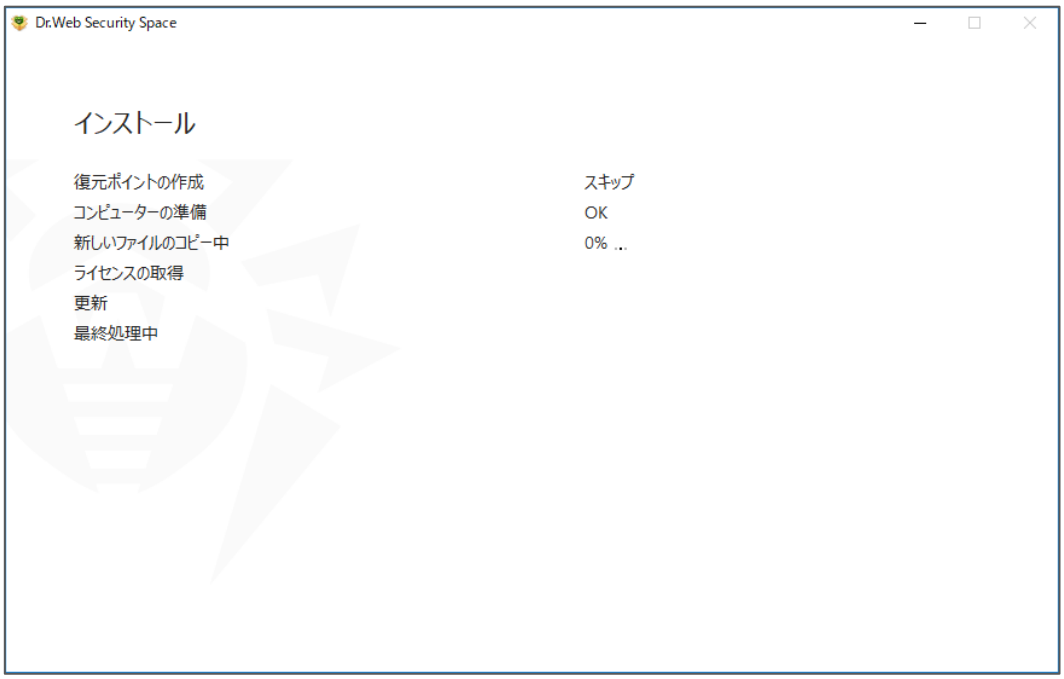

図 5. インストールプロセス

6) 「インストールが完了しました」と画面に表示されたら、「すぐに再起動」ボタンをクリックします。

※ PC が再起動した後に、Dr.Web が動作を開始(有効化)されます。

図 6. インストール完了 - 再起動要求

5. インストール後の Dr.Web の確認

インストールされた Dr.Web は、デスクトップ画面の右下の常駐アイコンにて表示されます。

Dr.Web の常駐アイコンが、以下のような状態でしたら問題なく動作しています。

※ Dr.Web の常駐アイコンが見当たらない場合は、△マークをクリックして、隠れているインジケーター内を確認してください。

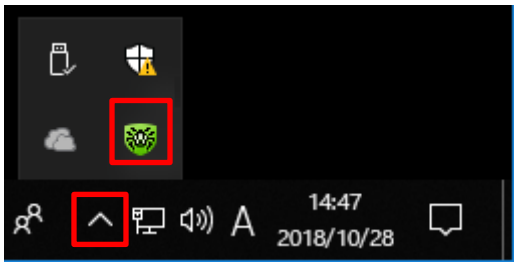

図 7. Dr.Web Anti-Virus アイコン(1)

6. ケーススタディ

6.1 設定変更可能モードへの切り替え

設定を変更する場合は、各設定画面の左下にある「錠」アイコンをクリックして、開錠された状態にする必要があります。

1) Dr.Web の常駐アイコンをクリックします。

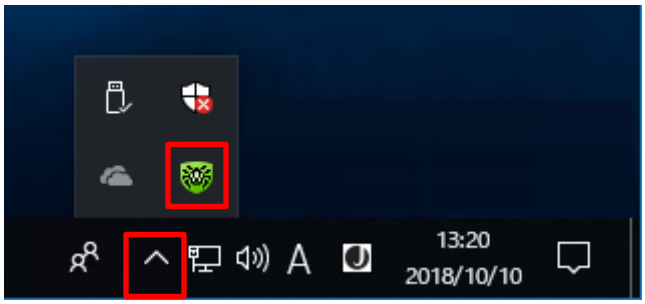

図 9. Dr.Web アイコン

2) 表示されたメニューから「Security Center」をクリックします。

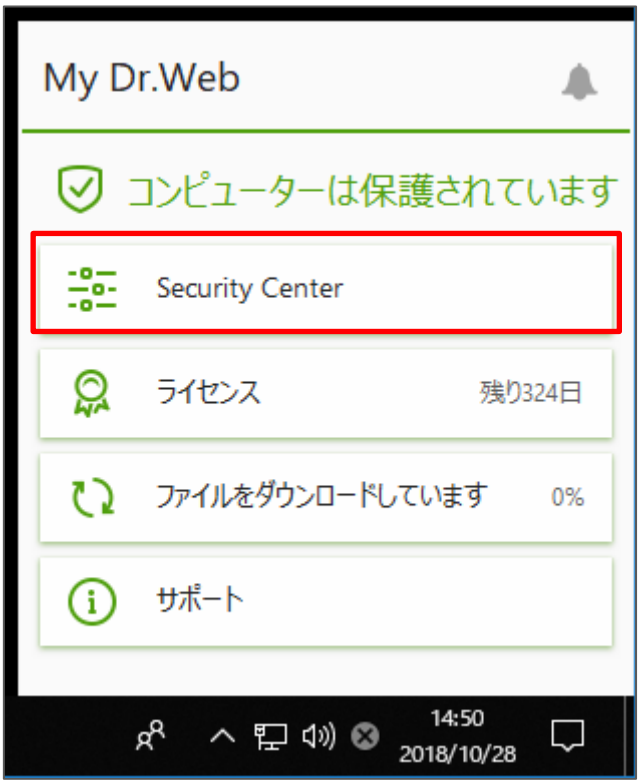

図 10. メニュー

3) 表示された画面左下の「錠」アイコンをクリックします。

図 11. Security Center

4) 「ユーザーアカウント制御」の画面で、「はい」ボタンをクリックします。

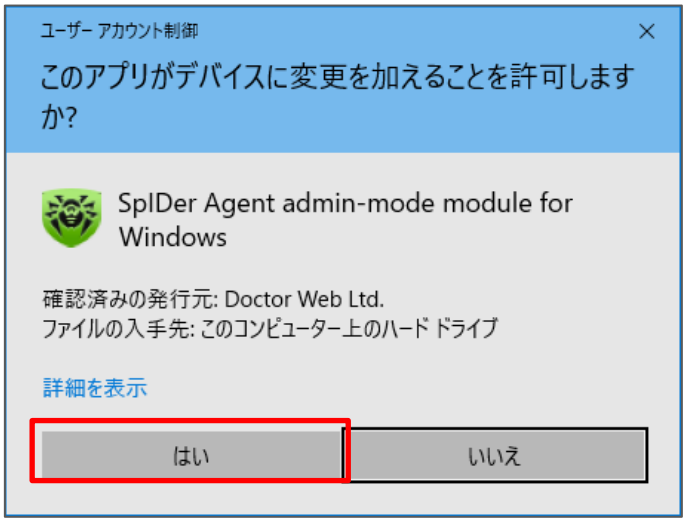

図 12. ユーザーアカウント制御

5) 画面左下の「錠」アイコンが、開いた状態であることを確認します。

図 13. Security Center

※ 画面を閉じると、「錠」アイコンが「施錠」状態となりますので、再度「開錠」状態にする必要があります。

6.2 プロキシサーバーの設定

1) 設定変更可能モードに切り替えます。

2) Security Center の画面右上にある「歯車」アイコンをクリックします。

図 14. Security Center

3) 「設定」画面が表示されたら、「ネットワーク」をクリックします。

図 15. [設定]-[一般]

4) 「プロキシサーバを使用する」を「オン」に変更します。

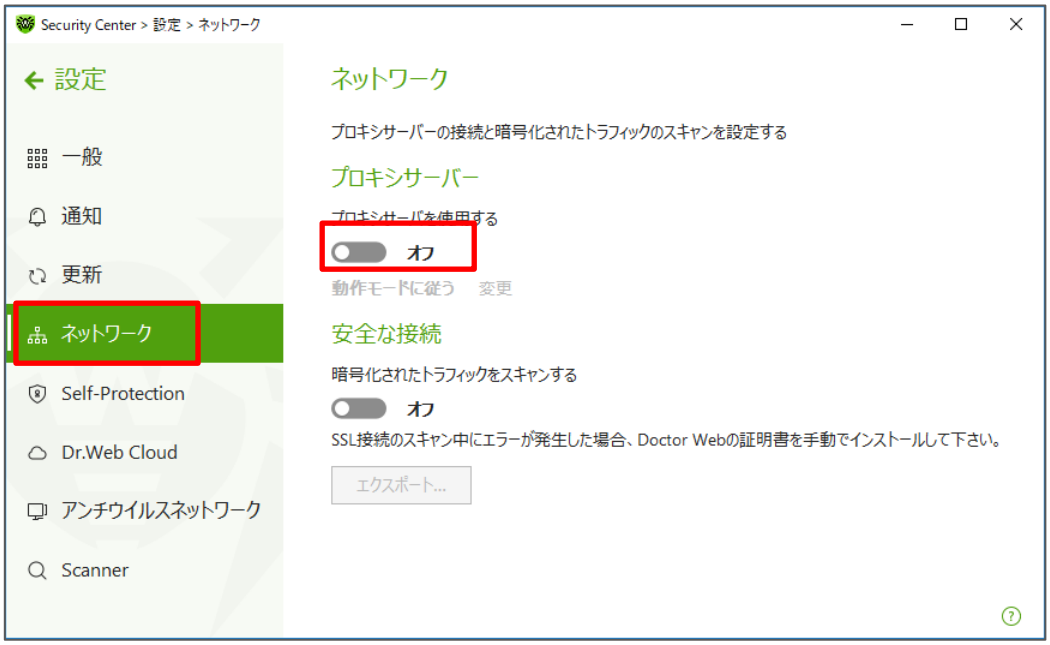

図 16. [設定]-[ネットワーク]

5) 「プロキシサーバーのパラメータ」画面が表示されるので、プロキシサーバーのアドレスやポート等を入力し、「OK」ボタンをクリックします。

図 17. プロキシサーバーのパラメータ

6) 「メイン」画面にて、以下を確認し閉じます。

- 「プロキシサーバーを使用する」が「オン」に変更されたこと。
- 指定したプロキシサーバーのアドレス

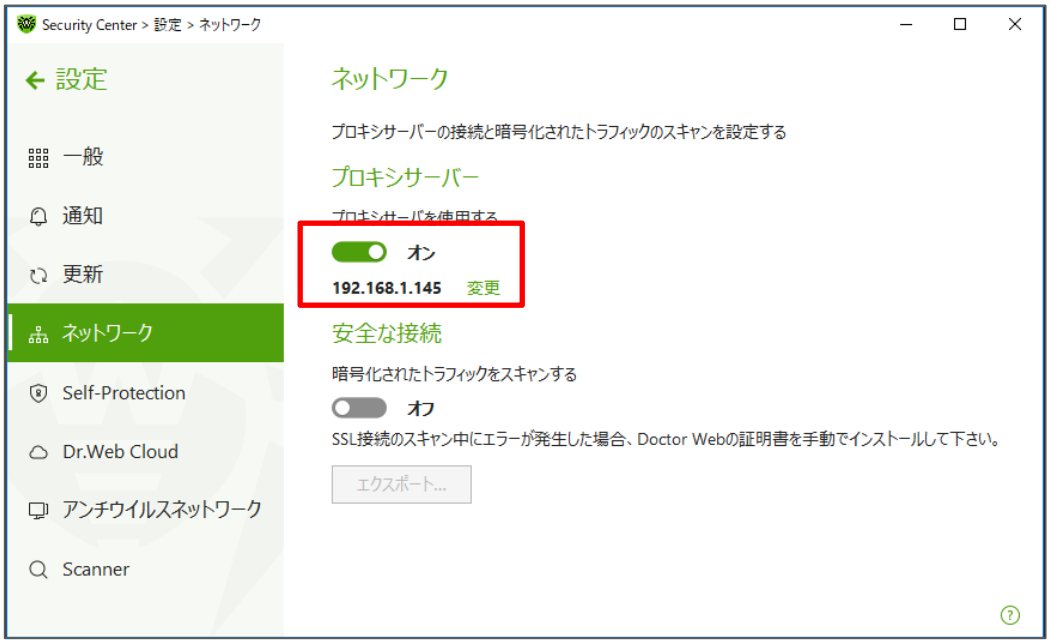

図 18. [設定]-[ネットワーク]

6.3 更新頻度の変更

Dr.Web では、ウイルス等のデータベースやコンポーネント等の更新頻度を初期値の 30 分から変更することができます。

1) 設定変更可能モードに切り替えます。
2) Security Center の画面右上にある「歯車」アイコンをクリックします。
3) 「設定」画面が表示されたら、「更新」をクリックします。
4) 「更新を受け取る」のプルダウンリストから、設定したい更新頻度を選択し閉じます。

図 19. [設定]-[更新]

6.4 更新されるコンポーネントの変更

Dr.Web では、ウイルス等のデータベースのみを更新するように設定することができます。

1) 設定変更可能モードに切り替えます。
2) Security Center の画面右上にある「歯車」アイコンをクリックします。
3) 「設定」画面が表示されたら、「更新」をクリックします。

4) 「アドバンス設定」をクリックします。

図 20. [設定]-[更新]

5) 「更新されるコンポーネント」で「データベースのみ」を選択し、閉じます。

図 21. [設定]-[更新](アドバンス設定)

6.5 hosts ファイルを変更するアプリケーションのインストール

アプリケーションのインストール時に hosts ファイルを変更するもの(例えば、VMware Horizon View Client 等)をインストールされる場合、Preventive Protection(予防的保護)の Behavior Analysis により hosts ファイルの変更がブロックされアプリケーションのインストールに失敗します。

このようなアプリケーションをインストールされる場合は、以下を無効化(停止)した状態でインストールを実施してください。

- セルフプロテクション
- Behavior Analysis

6.6 隔離されたファイルの確認・復元

6.6.1 隔離されたファイルの確認

1) 設定変更可能モードに切り替えます

2) Security Center から「ツール」をクリックします。

図 22. Security Center

3) 「ツール」画面から、「隔離マネージャ」をクリックします。

図 23. ツール

4) 「隔離マネージャ」画面が開き、隔離されているファイルの一覧が表示されます。

図 24. [ツール]-[隔離マネージャ]

6.6.2　隔離されたファイルの復元

1) 6.6.1 の手順にて「隔離マネージャ」を開きます。

2) 復元したいファイルを選択し、「復元」アイコンをクリックします。

図 25.　[ツール]-[隔離マネージャ]

3) 「隔離から復元」画面が表示されるので、表示されている内容を確認し、「復元」ボタンをクリックします。

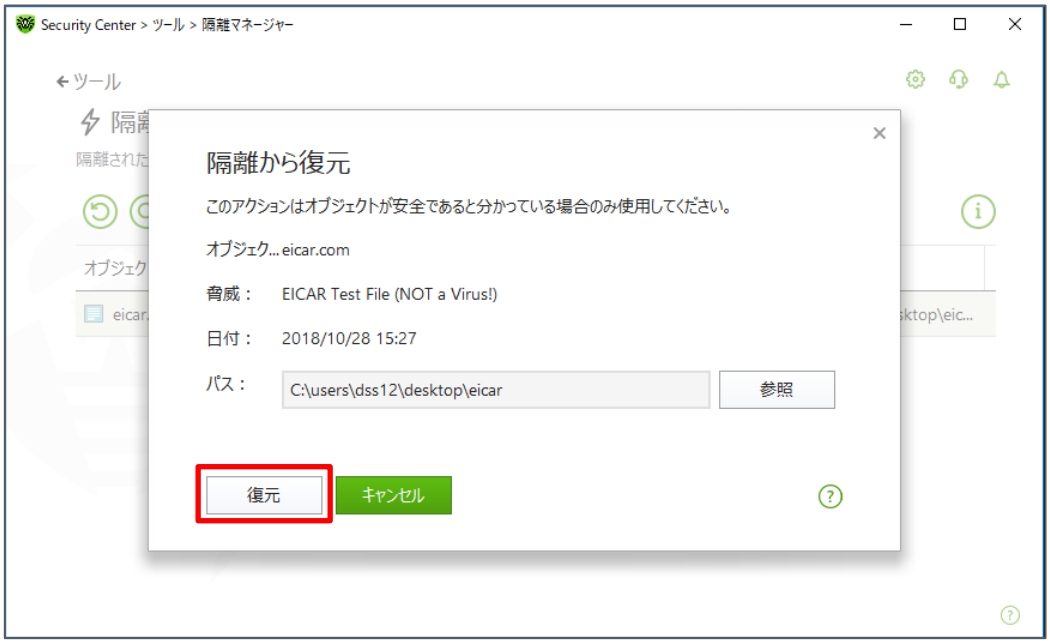

図 26.　隔離から復元

6.7 除外設定

6.7.1 SpIDer Guard、SpIDer Mail、SpIDer Gate、Dr.Web Scanner の除外設定

1) 設定変更可能モードに切り替えます。
2) Security Center から「除外」をクリックします。
3) 「除外」画面が表示されます。

※ ご利用のライセンスにより、表示される項目が異なります。

- ファイルとフォルダの除外

  「除外」画面から、「ファイルとフォルダ」を開きます。「ファイルとフォルダ」画面で「+」アイコンをクリックして、除外したいファイルやフォルダを指定します。

図 27. [除外]-[ファイルとフォルダ]

➢ アプリケーションの除外

「除外」画面から、「アプリケーション」を開きます。「アプリケーション」画面で「+」アイコンをクリックして、除外するアプリケーションを指定します。

図 28. [除外]-[アプリケーション]

6.7.2 Preventive Protection の除外設定

6.7.2.1. Behavior Analysis の除外設定

1) 設定変更可能モードに切り替えます。
2) Security Center から「Preventive Protection」をクリックします。
3) 「Preventive Protection」画面から「Behavior Analysis」をクリックします。

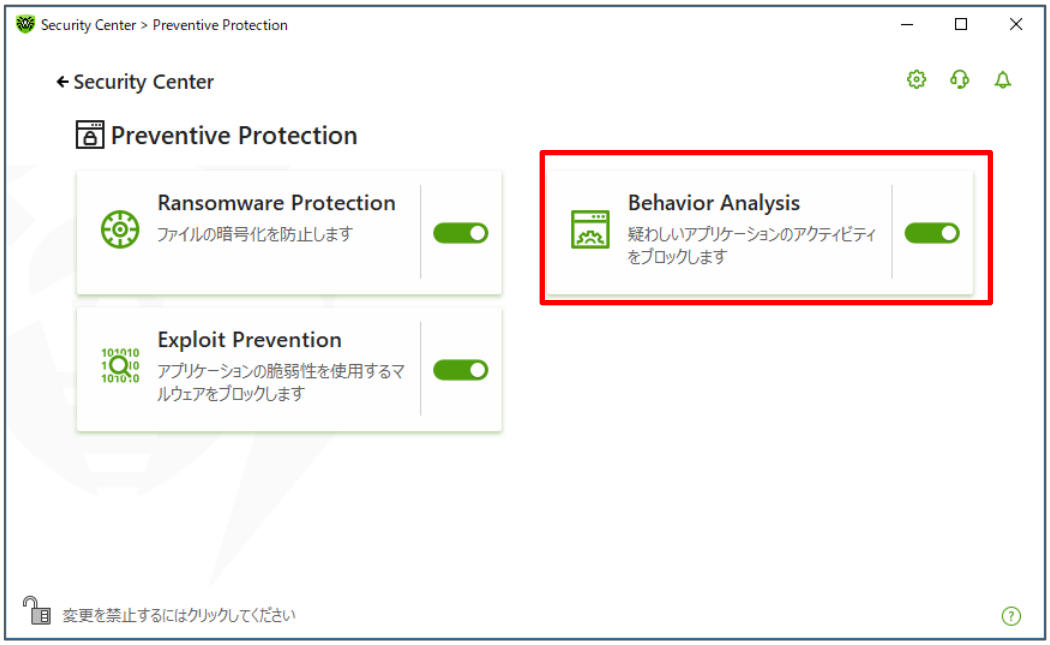

図 29. [Preventive Protection]

4) 「Behavior Analysis」画面から「アプリケーションアクセス」をクリックします。

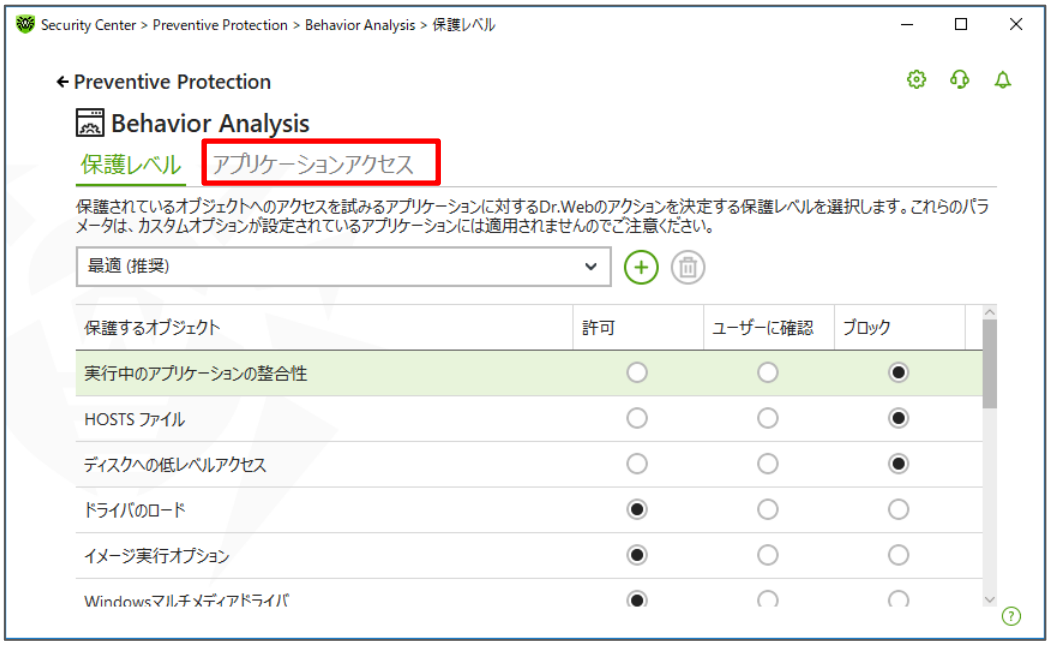

図 30. [Preventive Protection]-[Behavior Analysis]

5) 「アプリケーションアクセス」の画面で、「+」アイコンをクリックし除外したいプログラムを指定します。

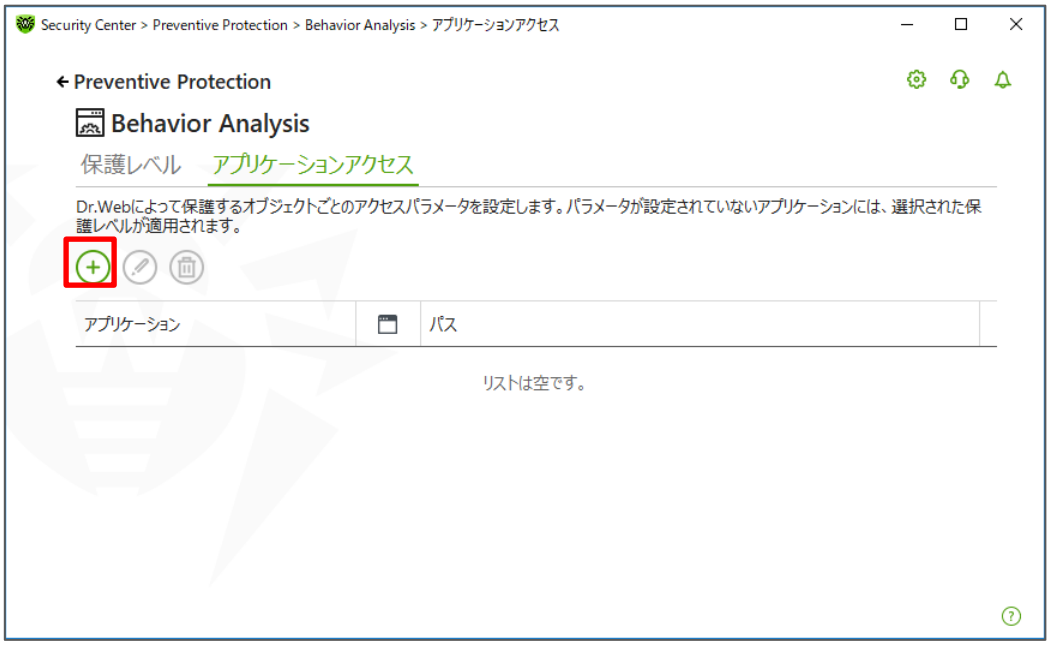

図 31. [Preventive Protection]-[Behavior Analysis]

6) 「アプリケーションルール」画面が表示されたら、「参照」ボタンをクリックし、除外したいプログラムを選択した後、「保護するオブジェクト」に対するアクションを変更し、「OK」ボタンをクリックします。

図 32. アプリケーションルール

7) 指定したプログラムが表示されていることを確認した後、画面を閉じます。

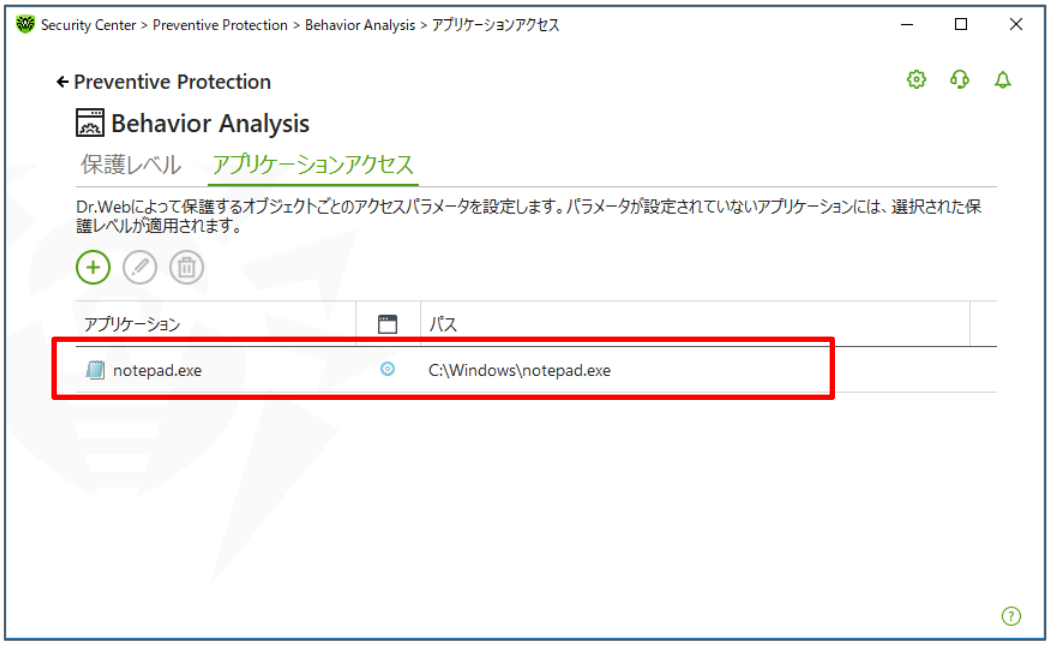

図 33. [Preventive Protection]-[Behavior Analysis]

6.7.2.2. Ransomware Protection の除外設定

1) 設定変更可能モードに切り替えます。
2) Security Center から「Preventive Protection」をクリックします。
3) 「Preventive Protection」画面から「Ransomware Protection」をクリックします。

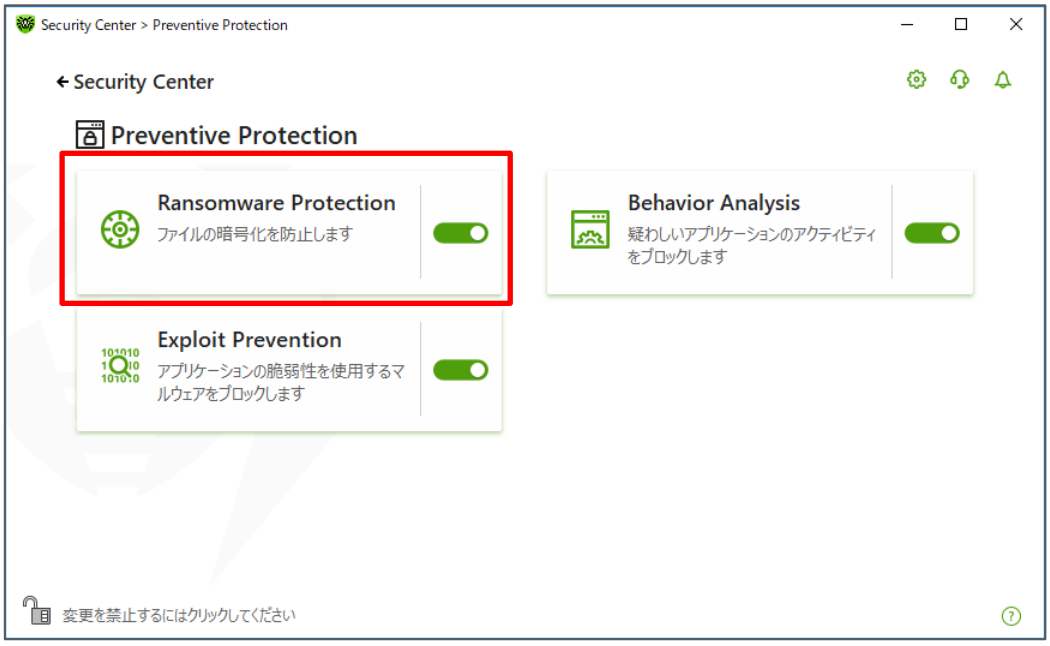

図 34. [Preventive Protection]

4) 「Ransomware Protection」の画面で、「+」アイコンをクリックし除外したいプログラムを指定します。

図 35. [Preventive Protection]-[Ransomware Protection]

5)　追加されたことを確認した後、画面を閉じます。

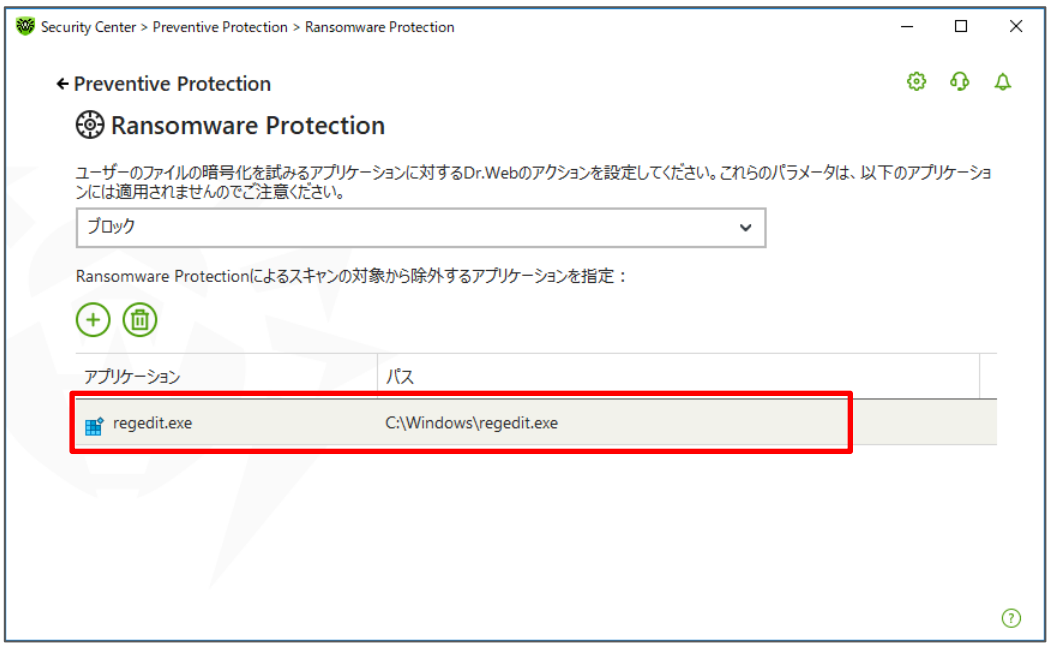

図 36.　[Preventive Protection]-[Ransomware Protection]

6.7.3　　業務用のアプリケーションが脅威として検知された場合

業務用アプリケーションが脅威として検知された場合、検知されたファイルを下記 URL より弊社にご送付ください。弊社にて確認後、誤検知であった場合には、検出されないよう対処します。

https://support.drweb.co.jp/support_wizard/

※　プログラムのバージョンが変更となった後、再度検出された場合は、当該ファイルをお送りください。

上記の弊社対応には時間をいただきますので、ファイルを弊社にお送りいただくとともに、6.6.1 および 6.6.2 を参照していただき、SpIDer Guard と Dr.Web Scanner の除外設定を行なっていただけますようお願いいたします。

- SpIDer Guard
  当該ファイルを「ファイルとフォルダ」および「プログラムとプロセス」に登録してください。
- Dr.Web Scanner
  当該ファイルを「スキャン対象外となるファイル・フォルダ」に登録してください。

6.7.4　業務用のアプリケーションの起動等が遅くなった場合

業務用アプリケーションの起動等が明らかに遅くなった場合、SpIDer Guard によるリアルタイムスキャンが影響している可能性があります。

その場合は、6.6.1 を参照していただき、SpIDer Guard の除外設定を行なっていただけますようお願いいたします。

”**プログラムとプロセス**”　：　起動等が遅くなったアプリケーションの実行ファイル等を指定

※　複数ある場合は、複数の実行ファイルをフルパスで指定してください。

”**ファイルとフォルダ**”　：　起動等が遅くなったアプリケーションのワークフォルダ、テンポラリフォルダやログファイル等を指定

≪事例≫

事　象 ：Dr.Web Agent インストール後から、TWAIN ドライバを使用しているスキャナーの取り込みが非常に遅くなった。

原　因 ：スキャナー取り込み時に TWAIN.LOG ファイルが更新されるが、その更新の都度 SpIDer Guard によるスキャンが実行される為。

対　処 ：TWAIN.LOG ファイルを SpIDer Guard が除外する”ファイルとフォルダ”に登録する。

登録例 ：C:¥Users¥*¥AppData¥Local¥Temp¥TWAIN.LOG

※　Windows7 や Windows8 の場合

6.8 通知設定の変更

1) 設定変更可能モードに切り替えます。
2) Security Center の画面右上にある「歯車」アイコンをクリックします。
3) 「設定」画面が表示されたら、「通知」をクリックします。
4) 「通知のパラメータ」をクリックします。

※ 「通知」を無効にする場合は、「通知をデスクトップに表示」と「通知をメールで送信」を「オフ」にしてください。

図 37 [設定]-[通知]

5) 「通知のパラメータ」画面にて、通知タイプと通知方法を選択します。

図 36 通知のパラメータ

6.9 ライセンス更新

※　更新されたライセンスキーファイルを用意した上で実施してください。

1) 設定変更可能モードに切り替えます。

2) Security Center から「ツール」をクリックします。

3) 「ライセンスマネージャー」をクリックします。

図 37. ツール

4) 「ライセンスマネージャー」画面で、「有効化」ボタンをクリックします。

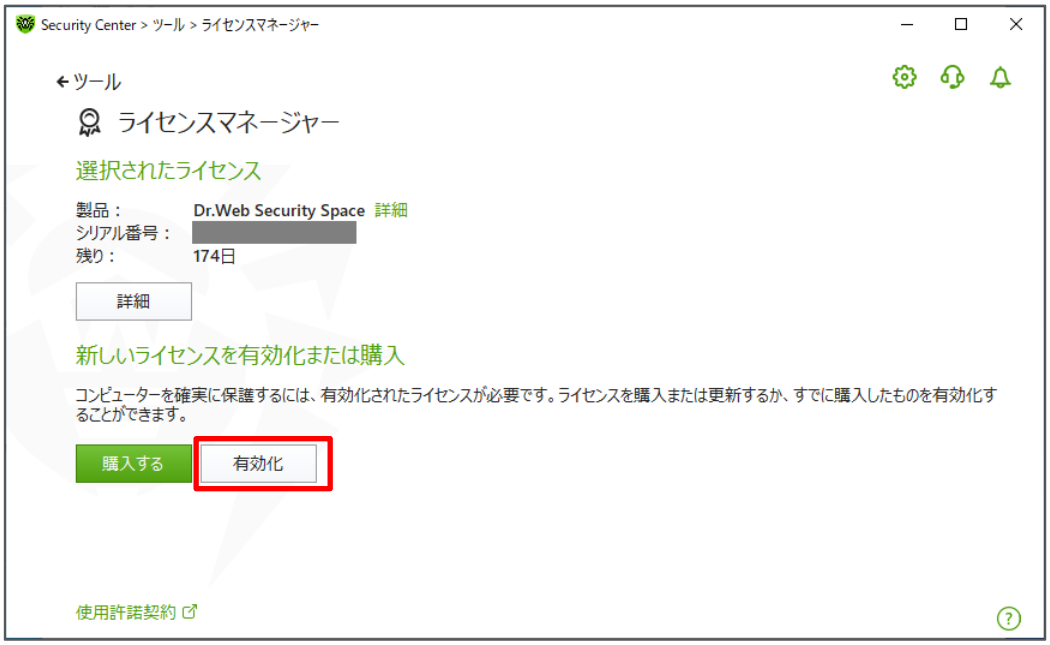

図 38. [ツール]-[ライセンスマネージャー]

5) 「ライセンスの有効化」画面が表示されたら、「キーファイル」ボタンをクリックします。

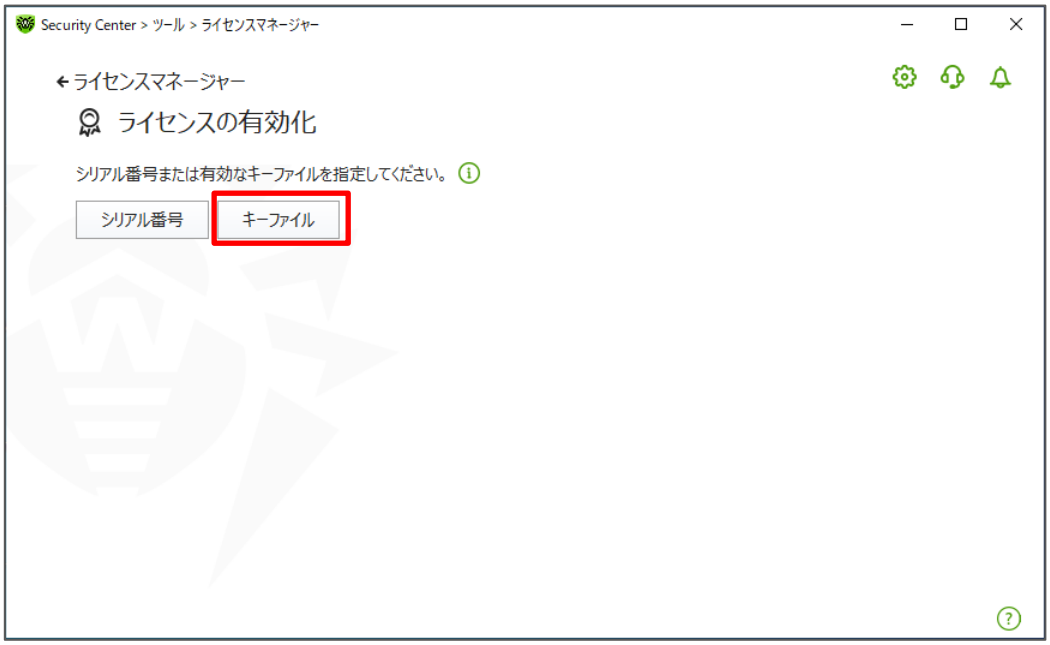

図 39. ライセンスの有効化

6) 「キーファイル」画面で「参照」ボタンをクリックし、更新されたライセンスキーファイルを指定します。

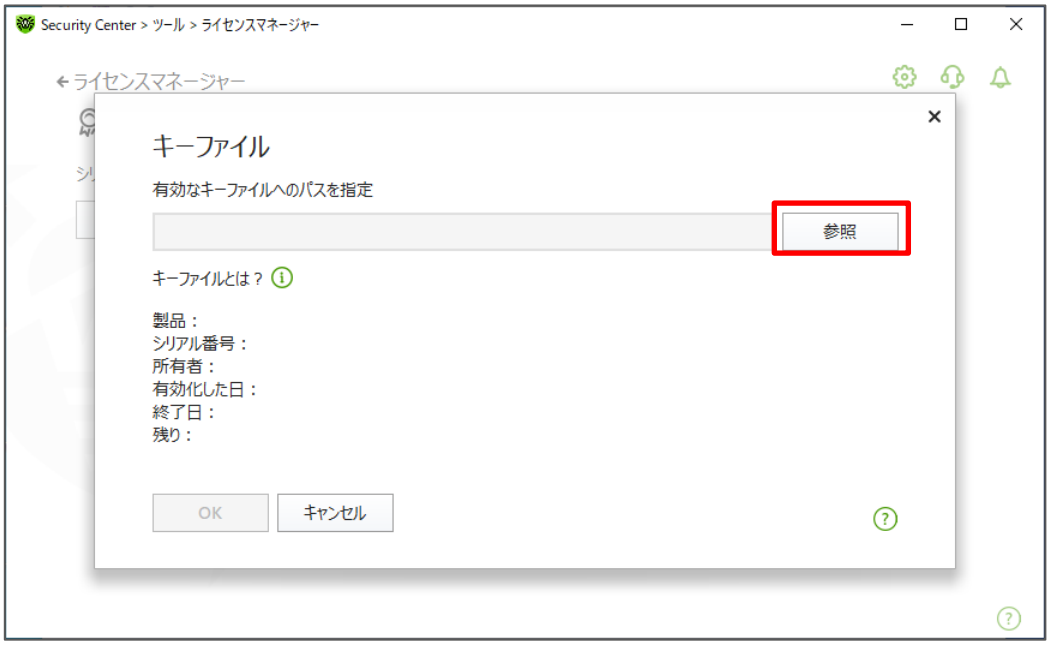

図 40. キーファイル

7) キーファイルを指定し、表示された所有者情報、終了日等の情報に誤りがないことを確認し、「OK」ボタンをクリックします。

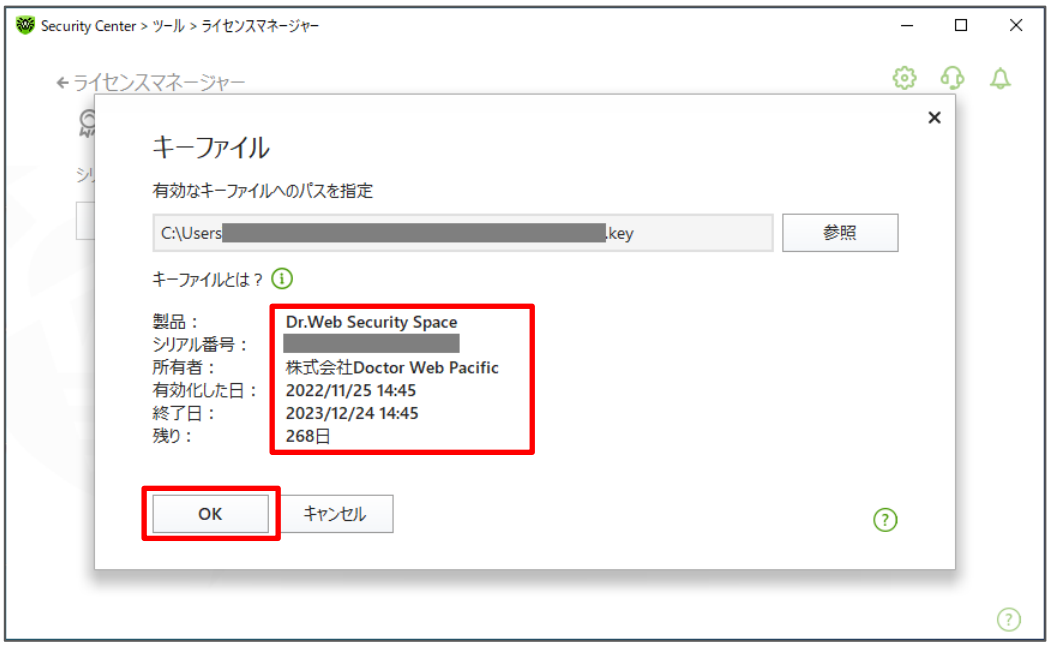

図 41. キーファイル

8) 「ライセンスマネージャー」画面が表示されたら、新しいライセンスが登録されたことを確認します。

図 42. ライセンスマネージャー

※ 以降は、以前のライセンスの削除の手順になります。誤って、更新されたライセンスを削除しないよう、注意してください。

9) 「詳細」ボタンをクリックします。

10) 表示された画面にて「選択されたライセンス」をクリックし、リストから以前のライセンスを選択します。

11) 「ごみ箱」アイコンをクリックします。

図 43. ライセンスマネージャー

12) 「確認」画面が表示されたら、「OK」ボタンをクリックします。

図 44. 確認(ライセンスマネージャー)

13) 「ライセンスマネージャー」画面が表示されたら、表示されている内容を再度確認し閉じます。

※　ライセンスの終了日が更新されたライセンスのものか確認してください。

※　ライセンスが一つのみ登録されている状態では、ごみ箱アイコンはグレーになっております。

図 45. ライセンスマネージャー

6.10 アンチウイルスネットワーク

この機能を用いると、Dr.Web がインストールされた端末から、他の Dr.Web がインストールされた端末の設定を変更することができます。

※　同一のバージョンを使用してください。

設定を行なう前に、Windows ファイアウォール(もしくは同等の機能を有するソフトウェア)の設定で、udp の 55566 と tcp の 135(RPC)、プライベートポート番号の通信が許可されているかご確認ください。

尚、アクセス元端末には、”Dr.Web Security Space”をインストールしてください。”Dr.Web Anti-Virus”では、アクセス元となれません。

6.10.1　接続先の設定

1)　設定変更可能モードに切り替えます。

2)　Security Center の画面右上にある「歯車」アイコンをクリックします。

3)　「設定」画面が表示されたら、「アンチウイルスネットワーク」をクリックします。

4)　以下の項目を設定します。

- 「リモート管理を有効にする」を「オン」に変更
- コード

  他の端末から接続時のパスワードとなります。

図 46.　アンチウイルスネットワーク

5)　画面を閉じます。

6.10.2　リモートからの管理

1) 設定変更可能モードに切り替えます。
2) Security Center から「ツール」をクリックします。
3) 「アンチウイルスネットワーク」をクリックします。

図 47.　ツール

4) 「アンチウイルスネットワーク」の画面が表示されます。

図 48.　アンチウイルスネットワーク

5) 接続したい PC をクリックし、展開された画面の「接続」ボタンをクリックします。

図 49. アンチウイルスネットワーク

6) パスワードを入力し、「OK」をクリックします。

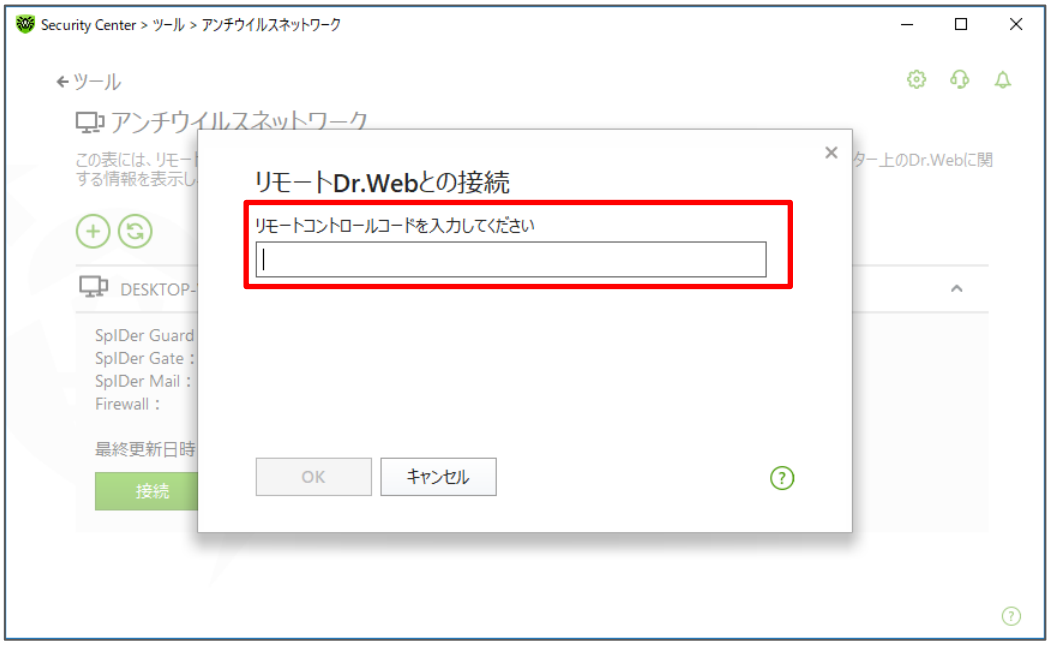

図 50. リモート Dr.Web との接続

7)　接続すると右下に「リモート接続が確立されました」と表示されます。

※　接続先の PC 名と IP アドレスも表示されます。

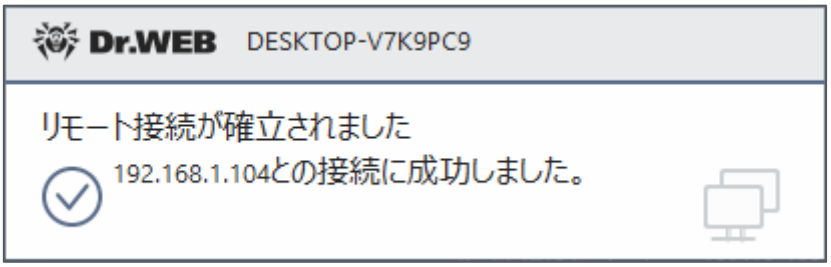

図 51.　接続確立

8)　タスクトレイ内の水色の Dr.Web アイコンをクリックすると、アンチウイルスネットワークで接続した端末のメニューが表示されます。

※　グレー(灰色)の Dr.Web アイコンは、接続している端末自身のものです。

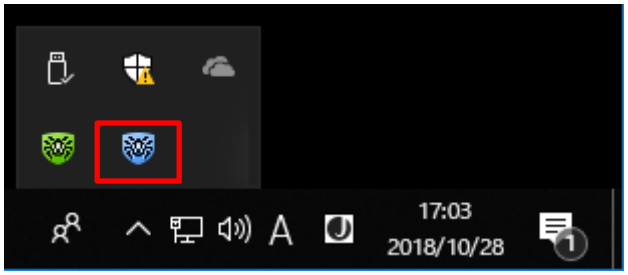

図 52.　タスクトレイアイコン

9)　終了する際は、下図の赤枠の箇所をクリックします。

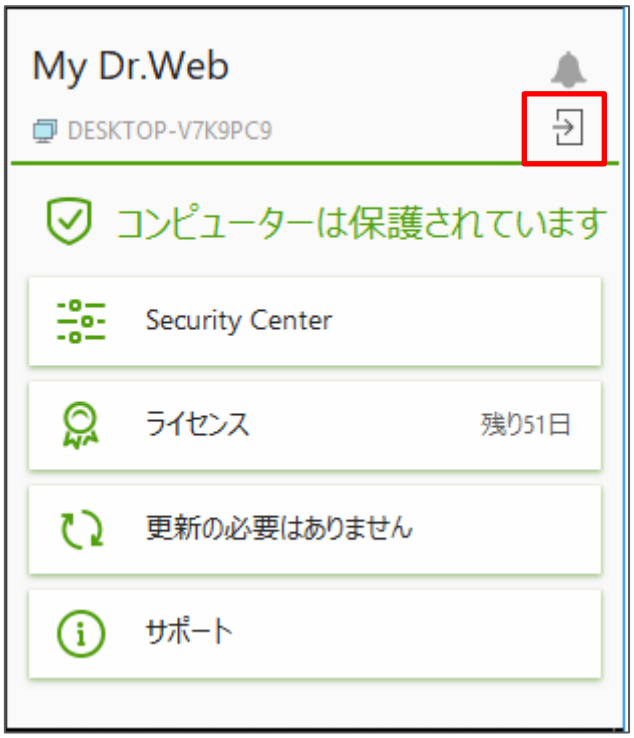

図 53.　メニュー（アンチウイルスネットワーク接続時）

6.11 インターネットに接続されていない端末の定義ファイル等の更新

インターネットに接続されていない端末に Dr.Web をインストールした場合、以下の方法で定義ファイル等の更新を行なうことが可能です。

※　本機能を利用する場合、インターネットに接続された端末に同一の Dr.Web のインストールが必要です。

※　インターネットに接続されていないクローズドネットワーク内の複数の端末で利用されている場合は、Dr.Web Enterprise Security Suite(ESS)の利用もご検討ください。

1) **インターネットに接続されている端末上**に定義ファイル等を保存するフォルダを作成します。
   例　：　C:¥repo

※　以降は、C:¥repo を定義ファイル等が保存されるフォルダとして記載しております。

2) **インターネットに接続されている端末上**の Dr.Web を設定変更可能モードに切り替えます。
3) Security Center の画面右上にある「歯車」アイコンをクリックします。
4) 「設定」画面が表示されたら、「更新」をクリックします。
5) 「アドバンス設定」をクリックします。

図 54.　[設定]-[更新]

6) 「ミラーサイトからの更新」を「オン」に変更します。

図 55. [設定]-[更新](アドバンス設定)

7) 「ミラーサイトからの更新」画面で「参照」をクリックし、1)で作成した定義ファイル等を保存するフォルダ(C:¥repo)を指定します。

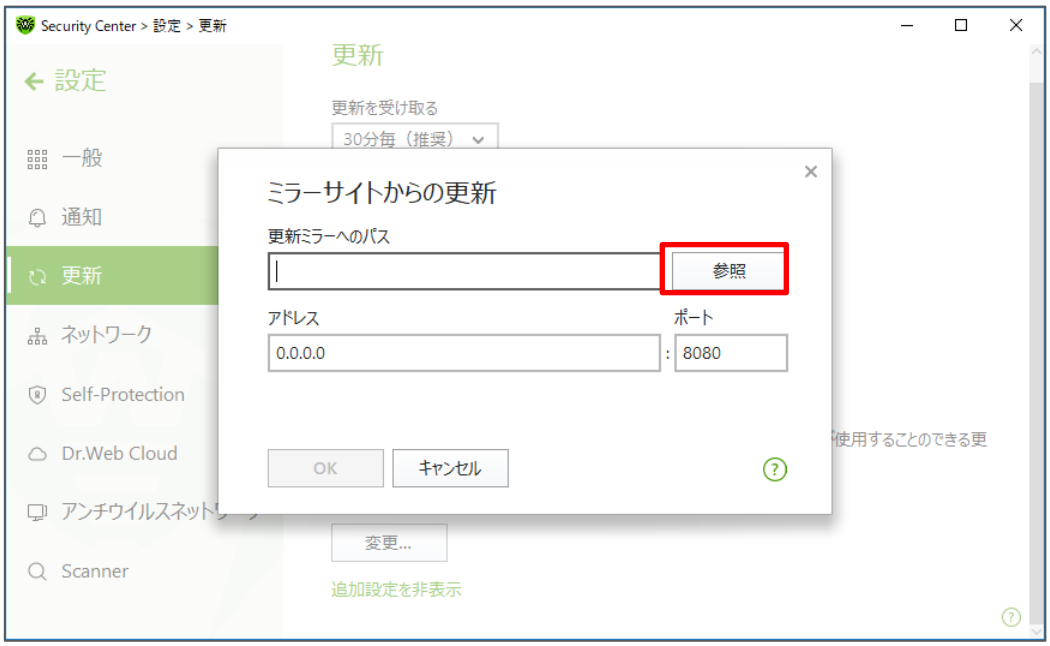

図 56. ミラーサイトからの更新

8) 「ミラーサイトからの更新」画面で「OK」をクリックします。

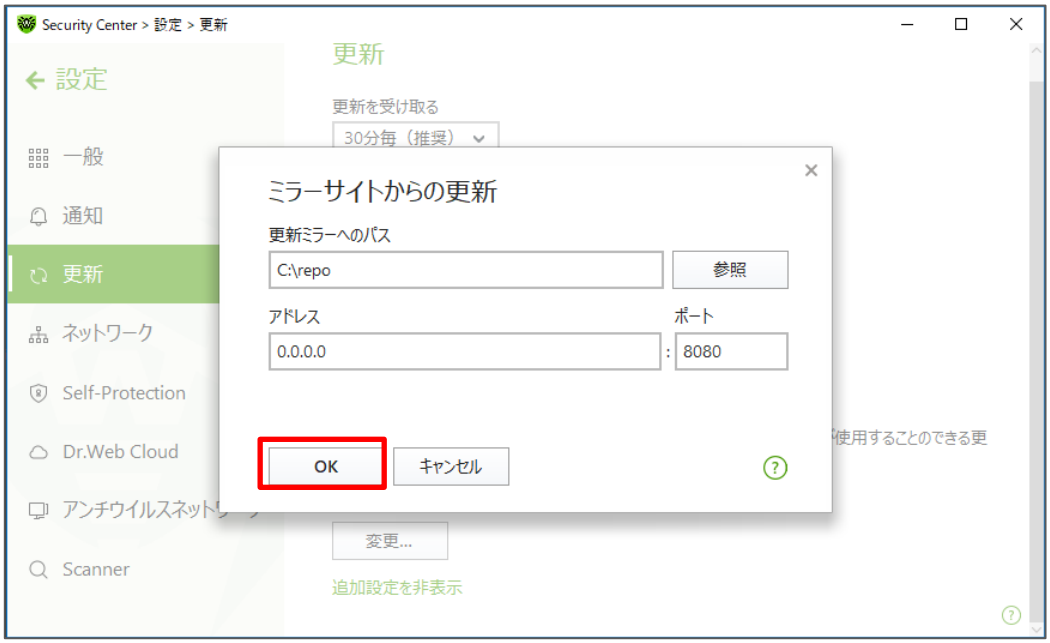

図 57. ミラーサイトからの更新

9) 「ミラーサイトからの更新」が「オン」に変更されたことを確認し、画面を閉じます。

図 58. [設定]-[更新](アドバンス設定)

10) 定義ファイル等の更新がされるまで待ちます。

※ 手動で更新を実行しても構いません。

11) 更新が完了した後、C:¥repo 内にファイルやフォルダが作成されていることを確認し、C:¥repo フォルダを USB メモリ等にコピーします。

12) **インターネットに接続されていない端末**上の Dr.Web を設定変更可能モードに切り替えます。

13) Security Center の画面右上にある「歯車」アイコンをクリックします。

14) 「設定」画面が表示されたら、「更新」をクリックします。

15) 「変更」をクリックします。

図 59. [設定]-[更新]

16) 「更新元」画面で、「適切な更新ソースを指定」を「Dr.Web の Server(推奨)」から「ローカルフォルダ・ネットワークフォルダ」に変更します。

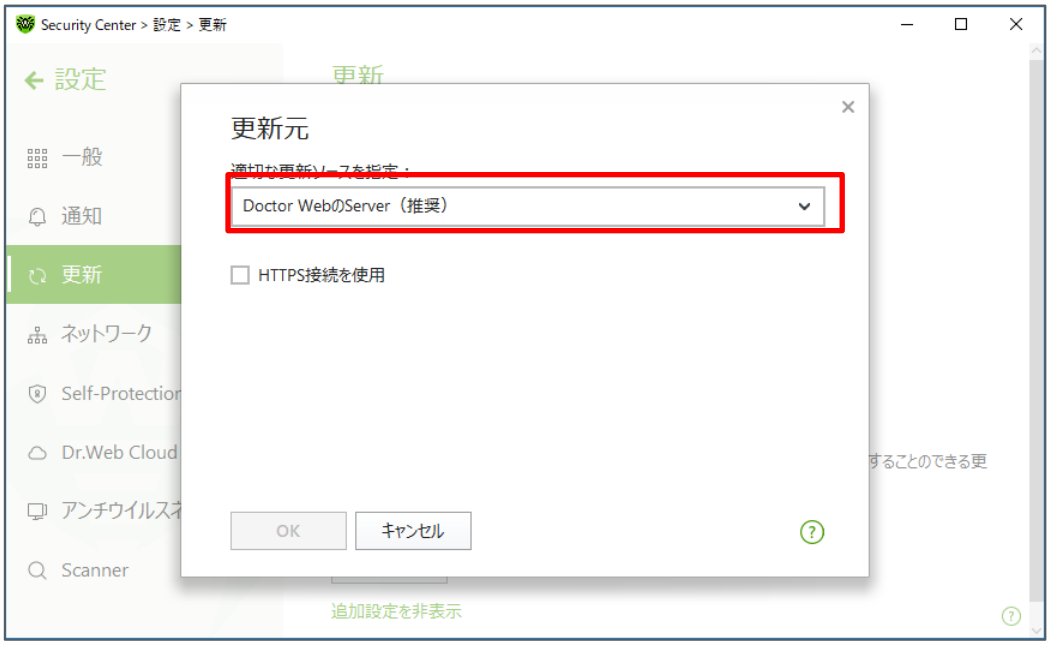

図 60. 更新元

17) 「参照」ボタンをクリックし、USB メモリ内の「repo」フォルダを指定し、「OK」ボタンをクリックます。

図 61. 更新元

18) 「更新元」が「ローカルフォルダ・ネットワークフォルダ」に変更されたことを確認し、画面を閉じます。

図 62. [設定]-[更新]

19) 手動で更新を実行し、定義ファイルが更新されたことを確認します。

お使いの製品の詳細な機能の説明や、利用方法は、各製品マニュアルをご参照ください。
また、製品のご利用について、ご質問やトラブル等がありましたら、下記 URL よりお気軽にお問い合わせください。

https://support.drweb.co.jp/

株式会社 Doctor Web Pacific
〒105-0003 東京都港区西新橋 1-14-10 西新橋スタービル 2F
URL：www.drweb.co.jp