HAGIWARA Solutions

マルウェア(ウィルス含む)対策 USB ソリューション

Windows ソフトウェア取扱説明書

この度はワクチン USB3（以下、本製品と表記します。）をご購入いただき、誠にありがとうございます。この取扱説明書では、本製品の導入、使用方法について説明しています。本製品を正しくご利用いただくために、取扱説明書を必ずお読みください。

Linux 版ソフトウェアについてはこちらをご確認ください。

CE FC VCCI

目次

1 ご使用になる前に

本製品は、Trellix 社（旧：McAfee 社）製エンジンを搭載したマルウェア(ウイルス含む)対策用アプリケーションプログラム及びウイルス定義ファイル等のコンテンツ更新版（以下、Trellix プログラムと言います）が格納されたライセンス製品です。本製品をご使用になる前に、本製品に別途同梱している弊社とお客様との本製品の Trellix プログラムに関する取り決めを規定したソフトウェア使用許諾約款（本製品の定義、ライセンスの許諾、禁止制限事項、免責、保証等）を必ずご確認、ご了承いただきますようお願い申し上げます。お客様が本製品を使用開始された場合は、約款に御同意いただいたものといたします。
※Trellix は、2022 年に McAfee Enterprise と FireEye の統合により誕生した新しいブランドです

使用上の注意事項

本製品を正しくお使いいただくために、必ず下記に示す注意事項をお読みになり、内容をよく理解された上でお使いください。本製品を接続して使用する対象機器の故障、トラブルやデータの消失・破損、または誤った取り扱いのために生じた本製品の故障、トラブルは、保証対象外となりますので、あらかじめご了承ください。

警告表示の意味

⚠ 警告	この表示は、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示は、人が傷害を負う可能性が想定される内容や物的損害の発生が想定される内容を示しています

⚠ 警告

・本製品を取り付けて使用する際は、取り付ける対象機器のメーカーが提示する警告、注意事項に従ってください。
・指定以外の電源電圧では使用しないでください。発火、火災、発熱、感電などの原因となります。
・本製品の分解や改造、修理等は絶対に行わないでください。火災、感電、故障の恐れがあります。
・本製品でウイルススキャン、ウイルス削除・隔離を行う対象機器の作動中に本製品は使用しないでください。対象機器のパフォーマンスに影響が出る可能性があります。
・濡れた手で本製品を使用しないでください。感電の恐れや故障の原因となります。
・小さなお子様や乳幼児の手の届くところに置かないでください。キャップ等を誤って飲み込むと窒息の恐れがあります。万一飲み込んだ時は、すぐに医師にご相談ください。
・歩行時や運転中などの使用はしないでください。事故の原因となる恐れがあります。
・本製品は水を使う場所や湿気の多い場所で使用しないでください。感電の恐れや、火災故障の原因となります。
・本製品や本製品を接続した機器に液体や異物が入った場合、または本製品や機器から煙が出たり、悪臭がした場合は、すぐに機器の電源を切り、電源ケーブルをコンセントから抜いてください。そのまま使用を続けると、感電の恐れや火災の原因となります。
・本製品に触れる前に、金属等に手を触れて身体の静電気を取り除いてください。静電気により破損、データ消失の恐れがあります。
・無理に曲げたり、落としたり、傷つけたり、上に重いものを乗せたりしないでください。故障の原因となります。
・本製品のコネクタに汚れ、ほこりなどが付着している場合、乾いたきれいな布で取り除いてください。汚れたまま使用すると故障の原因となります。
・本製品にデータの書き込み・読み出し中に、本製品を機器から取り外したり、機器の電源を切ったりしないでください。データが破壊、または消去される可能性があり、製品の故障の原因となります。

⚠ 注意

・本製品を取り付けて使用する際は、取り付ける対象機器の取扱説明書の使用方法、注意事項に従ってご使用ください。
・本製品に保存するデータ、または保存されるデータは、必ずデータのバックアップを取ってください。本製品内に記録したプログラムやデータの消失、破損等の責任は負いかねますので予めご了承ください。
・本製品はフラッシュメモリを使用している関係上寿命があります（製品保証期間はライセンス期間に準じます。製品保証期間最長５年間です）。長期間ご使用になると、データの書き込み・読み込みができなくなります。
・本製品の初期化をする場合は、本製品内に必要なデータがないことを確かめた後に行ってください。
・弊社は、お客様が、日本国内において、Trellix プログラムを格納した本製品を使用する非独占的且つ移転不能な権利を認めます。本製品は、あくまで、お客様若しくはお客様が使用許諾約款に規定される監査を弊社又は販売代理店に許可可能な国内関連会社での自己使用に限定されます。国内外を問わず、如何なる場合も、本製品の第三者へのレンタル、譲渡はできません。万一お客様が、本件製品を海外の関連会社で使用することを御希望のときは、事前に必ず弊社の書面による承諾を得てください。本製品を海外に輸出するときは、国内外の、関連するすべての輸出法規並びに手続きに完全に従ってください。
・本製品は、国内輸送を想定した梱包にてお届けしています。海外輸送される場合は、お客様にて海外輸送用に梱包いただきますようお願いします。
・お客様でウイルススキャンを実行する際は必ず最新のウイルス定義ファイルをダウンロードしてください。
・本製品に組み込まれた Trellix プログラムは、発見したコンピュータウイルスそのものを除去するのではなく、ウイルスに感染したファイルを削除・隔離するものです。（スキャンのみの設定の場合は感染したファイルの削除を行いません。）ＯＳが感染していた場合は、ＯＳの感染したファイル自体を削除・隔離しますので、感染していないＯＳを新たにインストールするまでホスト機を使用できなくなる可能性があります。

・システムファイルに感染したウイルスは削除・隔離できない場合があります。
・システムメモリに感染したウイルスは削除・隔離ができません。
・ウイルスは日々、新種が見つかっています。検知や削除・隔離ができない場合がありますので最新のウイルス定義ファイルでウイルススキャンを実行してください。
・ウイルスによってレジストリが書き換えられた場合、本製品はレジストリを修復する機能を持っていないためウイルスを削除・隔離後、正常にシステムが起動できない場合があります。
・本件製品のライセンス期間が終了すると、最新のウイルス定義ファイルは取得できなくなります。ライセンス終了後は、Trellix プログラムによる如何なる保護も提供されず、又保証されません。ライセンスが終了したにも拘わらず、お客様が本件製品を継続使用し、これにより損害を生じたとしても、弊社、販売代理店は、一切その責任を負いません。
・本製品では削除・隔離できないウイルスがございます。
・本製品は、最新のウイルスパターンファイルに更新することで、Trellix 社が対応しているウイルスの検知が可能であり、すべてのウイルスを検知することを保証しているものではありません。なお、暗号化されているファイルやパスワード付きの圧縮ファイルなど、ウイルスを検出できない場合もあります。
・お客様は、弊社が本製品の利用状況に関わる技術情報（お客様のご利用の端末情報を除く）を含み、これらに限定されませんが、技術および関連情報を収集および使用する場合があること、これらの情報は、弊社製品に関連するソフトウェアアップデート、製品サポート、およびその他サービスをお客様に円滑に提供するために定期的に収集されることについて、お客様は同意されたものとします。
弊社は、商品の改善またはお客様に対するサービスもしくは技術の提供を行うために、お客様を個人的に識別しない方法に限り、これらの情報を使用することができるものとします。

保管上のご注意

下記の場所では本製品を保管しないでください。製品に悪影響を及ぼしたり、感電、火災の原因になったりする場合があります。
・直射日光があたるところ
・水濡れの可能性のあるところ
・暖房器具の周辺、火気のある周辺
・高温（50℃以上）、多湿（85%以上）で結露を起こすようなところ、急激に温度の変化があるところ
・平坦でないところ、土台が安定していないところ、振動の発生するところ
・強い磁界や静電気の発生するところ
・ほこりの多いところ

製品保証規定

製品保証期間内に発見された不具合につきましては、本製品に起因する不具合と判断されたものに限り、無償修理又は代替品を納入させていただきます。また、輸送途中における製品の破損、故障に関しては、あきらかに弊社の責に帰すべき事由に基づく破損、故障と判断されたものに限り、無償修理又は代替品を納入させていただきます。
また、アプリケーションプログラムの、お客様の特定目的の適合性については、これを保証できかねます。
なお、下記の場合においては、弊社は一切の責任を負いませんので予めご了承ください。
・納入後の輸送（移動）時の落下衝撃等、お客様の取り扱い不具合により生じた故障、損傷の場合
・地震・雷・風水害などの天災および弊社の責任以外の火災災害による故障、損傷の場合
・弊社以外で修理、改造された場合
・本書に記載された使用方法及び注意事項に反する取扱から生じた故障、損傷の場合
・本製品を接続する対象機器の故障、トラブルに起因する場合
・本製品内に記録されたプログラムやデータの消失、破損（本製品の不具合により、メモリ内に記録されたプログラムや各種データが破損または消去された場合といえども、当該プログラムまたはデータに対し、弊社は一切の責任を負いません。）
・本製品の紛失、盗難などにより第三者の手に製品が渡った場合に、記録データが漏洩する可能性があります。その場合に発生しうる損害に対する補償は、一切責任を負いかねますので、製品の管理には十分にご注意ください。

補償の制限

如何なる場合であっても、弊社、販売代理店は、お客様に対して、本件製品に関連して生じた、利益の損失、使用の損失、データの損失、信用の損失、信頼の損失、ビジネスの中断若しくは他の一切の類似の損害を含む如何なる付随的な、間接的な、特別な、また派生的な損害、及び逸失利益の喪失に係る賠償の責任を負いません。

2 使用許諾

本契約は、お客様（以下「お客様」とします）とハギワラソリューションズ株式会社（以下「弊社」とします）との間で弊社がお客様へ提供するソフトウェア（以下「許諾ソフトウェア」とします）の使用権許諾に関して次のように条件を定めます。
弊社は、お客様に対して、以下の条件に従って許諾ソフトウェアの使用を許諾いたします。お客様は、本契約書の内容をしっかりとお読みになり、本契約書の内容に同意できる場合に限り、お客様の責任で許諾ソフトウェアを使用してください。許諾ソフトウェアを使用することによって、お客様は本契約の各条項に同意したものとみなされます。本契約の各条項に同意されない場合、弊社はお客様に対し、許諾ソフトウェアのご使用を許諾できません。

第１条（総則）
　許諾ソフトウェアは、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約によって保護されています。許諾ソフトウェアは、本契約の条件に従い弊社からお客様に対して使用許諾されるもので、許諾ソフトウェアの著作権等の知的財産権は弊社に帰属し、お客様に移転いたしません。

第２条（使用権）
1. 弊社は、許諾ソフトウェアの非独占的な使用権をお客様に許諾します。
2. 本契約によって生ずる許諾ソフトウェアの使用権とは、お客様が取得または購入された許諾ソフトウェアがインストールされている電子機器上において、許諾ソフトウェアをお客様の機器等に対して使用する権利をいいます。
3. お客様は、許諾ソフトウェアの全部又は一部を複製、複写、並びに、これに対する修正、追加等の改変をすることができません。

第３条（権利の制限）
1. お客様は、許諾ソフトウェアを再使用許諾、譲渡、貸与又はリースその他の方法で第三者に使用させてはならないものとします。
2. お客様は、許諾ソフトウェアを用いて、弊社又は第三者の著作権等の権利を侵害する行為を行ってはならないものとします。
3. お客様は、許諾ソフトウェアに関しリバースエンジニアリング、逆アセンブル、逆コンパイル等のソースコード解析作業を行ってはならないものとします。
4. お客様は、本契約に基づいて、許諾ソフトウェアがインストールされている電子機器と一体としてのみお客様の許諾ソフトウェアに関する権利の全てを、譲受人が本契約の条項に同意することを条件に譲渡することができます。但しその場合、お客様は許諾ソフトウェアの複製物を保有することはできず、許諾ソフトウェアの一切（全ての構成部分、媒体、電子文書及び本契約書を含みます）を譲渡しなければなりません。

第４条（許諾ソフトウェアの権利）
　許諾ソフトウェアに関する著作権等一切の権利は、弊社または、本契約に基づきお客様に対して使用許諾を行うための権利を弊社に認めた原権利者（以下原権利者とします）に帰属するものとし、お客様は許諾ソフトウェアに関して本契約に基づき許諾された使用権以外の権利を有しないものとします。

第５条（責任の範囲）
1. 弊社及び原権利者は、第６条２項に定義するアップデートデータが正常にインストールできることを保証いたしません。また、弊社及び原権利者は、当該アップデートデータのインストールによってお客様に損害が発生しないことを保証いたしません。
2. 弊社及び原権利者は、許諾ソフトウェアにエラー、バグ等の不具合がないこと、若しくは許諾ソフトウェアが中断なく稼動すること又は許諾ソフトウェアの使用がお客様及び第三者に損害を与えないことを保証しません。また、弊社及び原権利者は、許諾ソフトウェアが第三者の知的財産権を侵害していないことを保証いたしません。
3. 許諾ソフトウェアの稼動が依存する、許諾ソフトウェア以外の製品、ソフトウェア又はネットワークサービス（第三者が提供する場合に限られず、弊社又は原権利者が提供する場合も含みます）は、当該ソフトウェア又はネットワークサービスの提供者の判断で中止又は中断する場合があります。弊社及び原権利者は、許諾ソフトウェアの稼動が依存するこれらの製品、ソフトウェア又はネットワークサービスが中断なく正常に作動すること及び将来に亘って正常に稼動することを保証いたしません。
4. お客様に対する弊社及び原権利者の損害賠償責任は、当該損害が弊社又は原権利者の故意又は重過失による場合を除きいかなる場合にも、お客様に直接且つ現実に生じた通常の損害に限定され且つお客様が証明することのできる許諾ソフトウェアの購入代金を上限とします。
5. 弊社又は原権利者は、債務不履行及び不法行為等の理由の如何にかかわらず、如何なる場合においても、お客様に生じた逸失利益、結果的損害、間接損害、若しくは、データ消失及び破損における損害については、一切賠償する責を負わないものとする。
6. 弊社は、弊社ウェブページにて定めるお問合わせ窓口（許諾ソフトウェア購入ページからリンクしてご確認ください。）に限り、お客様が弊社から使用許諾を受けた許諾ソフトウェアに関する技術的サポートを提供します。但し、弊

社は、お客様の同意を得ることなく、当該窓口の受付時間及び当該サポートの提供の有無について随時変更することができるものとします。なお、弊社は、お客様との間で、別途契約を締結しないかぎり、当該サポートをお客様に提供及び継続する義務を一切負うことはありません。

第６条（著作権保護及び自動アップデート）
1. お客様は、許諾ソフトウェアの使用に際し、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約に従うものとします。
2. お客様は、弊社又は弊社の指定する第三者がウェブ上に、許諾ソフトウェアのセキュリティ機能の向上、エラーの修正、アップデート機能の向上等の目的で許諾ソフトウェアが適宜にアップデートデータ（以下「アップデートデータ」とします）を公開する場合は、アップデートデータ公開後 90 日以内に許諾ソフトウェアをアップデートしなければなりません。また、お客様は、アップデートデータ公開後 90 日を経過した場合は、旧許諾ソフトウェアを、アップデートをする目的以外で使用することができません。お客様は、(ⅰ)当該許諾ソフトウェアのアップデートに伴い、許諾ソフトウェアの機能が追加、変更又は削除されることがあること、及び(ⅱ)アップデートされた許諾ソフトウェアについても本契約が適用されることに同意するものとします。

第７条（契約の解約）
1. 弊社は、お客様が本契約に定める条項に違反した場合、直ちに本契約を解約することができるものとします。
2. 前項の規定により本契約が終了した場合、お客様は契約の終了した日から ２週間以内に許諾ソフトウェアの全てを廃棄するか、弊社に対して返還するものとします。お客様が許諾ソフトウェアを廃棄した場合、直ちにその旨を証明する文書を弊社に差し入れるものとします。
3. 本条 1 項の規定により本契約が終了した場合といえども、第 4 条、第 5 条、第 7 条第 2 項及び第 3 項並びに第 8 条第 1 項及び第 3 項乃至第 5 項の規定は有効に存続するものとします。

第８条（データ使用に対する同意）
お客様は、弊社が本製品の利用状況に関わる技術情報（お客様のご利用の端末情報を除く）を含み、これらに限定されませんが、技術および関連情報を収集および使用する場合があること、これらの情報は、弊社製品に関連するソフトウェアアップデート、製品サポート、およびその他サービスをお客様に円滑に提供するために定期的に収集されることについて、お客様は同意されたものとします。
弊社は、商品の改善またはお客様に対するサービスもしくは技術の提供を行うために、お客様を個人的に識別しない方法に限り、これらの情報を使用することができるものとします。

第９条（その他）
1. 本契約は、日本国法に準拠するものとします。
2. お客様は、許諾ソフトウェアを国外に持ち出して使用する場合、適用ある条例、法律、輸出管理規制、命令に従うものとします。
3. 本契約に関連する一切の紛争については、弊社本店所在地の地方裁判所または簡易裁判所を第一審の専属管轄裁判所とします。
4. 本契約の一部条項が法令によって無効となった場合でも、当該条項は法令で有効と認められる範囲で依然として有効に存続するものとします。
5. 本契約に定めなき事項又は本契約の解釈に疑義を生じた場合は、お客様及び弊社は誠意をもって協議し、解決するものとしま

3 同梱品の確認

本製品のパッケージには次のものが含まれています。はじめに、すべてのものが揃っているかご確認ください。万一、不足品がありましたら、お買い求めの販売店までご連絡ください。

ワクチン USB3 （製品本体）.....1 個

4 本製品について

本製品は、Trellix 社製アンチマルウェアエンジン、ウイルス定義ファイル及び弊社のアプリケーションプログラム（以下、ウイルススキャンソフト）を搭載し、本製品を接続する機器（以下、対象機器と言います）に感染しているマルウェア(ウイルス含む)の検出および削除・隔離をする機能を搭載した製品です。
本マニュアル上ではウイルススキャンはマルウェア(ウィルスを含む)を検知(削除・隔離含む)する処理としています。

※**マルウェア**とは有害なソフトウェア全般を指す総称です。ウイルス、ワーム、トロイの木馬、スパイウェアなどコンピュータやネットワークに悪影響を及ぼす全ての悪意のあるソフトウェアがマルウェアに該当します。

ウイルススキャンソフトのライセンス

ウイルススキャンソフトウェアは、ライセンス期間内のみご利用いただけます。ライセンス期間終了後も継続してご利用する場合は、ライセンスの更新（購入）が必要となります。 詳しくは販売代理店までお問い合わせください。
※ライセンスには定義ファイル更新、技術サポートとウイルススキャンソフトウェアのマイナーバージョンアップのサポートが含まれます。

本製品の特長

✓ *マルウェア(ウイルス含む)ファイルのスキャン・削除・隔離機能*

対象機器に本製品を接続すると、自動的にウイルススキャンソフトを起動し、対象機器に保存されているファイルへウイルススキャン・削除・隔離を実行します。スキャン結果は画面、搭載 LED で表示します。

- ❑ ウイルススキャン実行中 ・・・ 本体の赤色●LED と青色●LED が交互に点滅します
- ❑ ウイルスを検知した場合 ・・・ 本体の赤色●LED が点灯します
- ❑ ウイルスが検知されなかった場合 ・・・ 本体の青色●LED が点灯します。
- ❑ ウイルスが検知し、削除/隔離成功した場合 ・・本体の青色●LED が点灯します。
- ❑ エラーが発生した場合 ・・・ 本体の赤色●LED が点滅します。

✓ *スキャンモード(スキャンのみ・削除・隔離)の選択機能*

メニュー画面から 3 種類のスキャンモードを選択することが可能です。

❑スキャンのみ：
マルウェア(ウイルス含む)検知のみを実行します。マルウェア(ウイルス含む)を削除・隔離しません。

❑スキャン＋即削除：
マルウェア(ウイルス含む)検知を実行しながら、マルウェア(ウイルス含む)を検知すると即削除処理を行います。

❑スキャン＋即隔離：
マルウェア(ウイルス含む)検知を実行しながら、マルウェア(ウイルス含む)を検知すると隔離処理を行います。

✓ *メモリ上で動作しているプロセススキャン機能*

ファイルだけではなく、メモリ上で動作しているプロセスに対してもウイルススキャンする機能をもっています。
プロセススキャンはファイルスキャンの前に実施されます。

✓ *Windows/Linux のマルチプラットフォーム対応* *New!*

長年 Windows 専用製品としてご愛顧いただいてきたワクチン USB3 が、クロスプラットフォーム対応へと進化。
Linux プラットフォームのお客様にも、ワクチン USB をご利用いただけます。
Linux 版ソフトウェアのマニュアルはこちらからご確認ください。

✓ *ログ保存機能*

ウイルススキャンの結果、発見したウイルス情報、実行した PC 情報をログファイルとして本製品に保存します。
（対象機器の OS/ユーザー権限によってはログを本製品に保存できない場合があります。）

✓ *ウイルス定義ファイル更新機能*

本製品に搭載されているウイルス定義ファイルは、インターネットに接続可能な PC に本製品を接続することで手動での更新が可能です。

✓ *ウイルススキャンソフトのアップデート機能*

本製品をインターネットに接続されたPC に接続し、ウイルス定義ファイルの更新を行うと、インターネット経由で自動的にウイルススキャンソフトの更新情報を取得します。ウイルススキャンソフトの更新情報が確認されると通知され、ソフトウェアの更新を行うことができます。

✓ *本製品へのウイルス感染防止機能*

本製品では、リムーバブルディスク領域への一切書き込みはできないようになっています。ウイルス感染している PC に接続しても未知のウイルスを含め、本製品へのウイルス感染を防止するための機能を持っています。

✓ *ログ表示、出力、ログ削除機能*

本製品内のログ情報を閲覧、任意のフォルダに出力、一括削除を行うことができます。

✓ *スキャンターゲットの設定機能*

スキャンしたい場所（ドライブやフォルダ）を任意で設定することができます。

動作環境／製品仕様

USB インターフェース	USB 2.0（High Speed/Full Speed）/　USB3.0(Super Speed)	
動作環境（*1*2*3）	USB インターフェースを標準搭載した DOS/V 機器 物理空きメモリ-容量 1GB 以上(*6) ページキャッシュが ON であること(推奨) CD-ROM ドライブが認識されること(推奨) CD-ROM ドライブによるオートラン実行がされること(推奨)	
対応 OS（*2*3*5*7） [日本語 OS/英語 OS]	Windows 7 (*4) Windows 8/8.1 Windows10 Windows11 Windows Server 2008 SP2(*8) Windows Server 2008 R2(*8) Windows Server 2012,2012R2(*8) Windows Server 2016(*8) Windows Server 2019(*8) Windows Server 2022 *64bit のみ(*8) Windows Embedded Standard 7(*10) Windows Embedded POSReady 7(*10) Windows10 Enterprise LTSB/LTSC Windows10 IoT Enterprise LTSB/LTSC Windows11 Enterprise LTSC Windows11 IoT Enterprise LTSC LinuxOS ※対応 LinuxOS についてはこちらをご確認ください ※日本語 OS 以外の OS では自動的に英語表示に切り替わります。 ※対応 OS は Trellix 社ウイルススキャンエンジンによって変わります。 今後アップデートがあった場合、弊社製品の対応 OS が変わる可能性がございます。	
対応アカウント*9	コンピュータの管理者（Administrator） 制限ユーザー アカウント種類(管理者・標準ユーザー)	
対応画面サイズ	640 x480 以上 ※800 x 600 以下のサイズの場合、一部画面がタッチパネルに適した画面へ切り替わります。	
動作電圧	5V±5%	
消費電流	スキャン時	最大 220mA
	待機時	最大 140mA
動作温度	0～50℃	
動作湿度	30～80%（結露なきこと）	
取得規格	CE、FCC、VCCI、RoHS	
重量	11g	
外形寸法（キャップ含む）	全長 79.0mm×幅 18.0mm×高さ 9.4mm	

*1　拡張ボードで増設した USB インターフェースには対応していません。
*2　USB Mass Storage Class ドライバ、CD-ROM ドライバがあらかじめ組み込まれている必要があります。
*3　オートランによるアプリケーション起動を行うには、OS 側でオートラン実行が有効となっている必要があります。
*4　権限昇格ダイアログ画面が表示されます。無効にした場合、システムフォルダ内で検知したウイルスを削除・隔離できなくなります。
*5　64bitOS の対応について・Vista 以降の OS では、Windows¥Sytem32 へのアクセスは、Windows¥SysWOW64 にリダイレクトされます。
*6　推奨の物理空きメモリ容量は 1.5GB 以上です
*7　英語版 OS で英語表記するためには OS に Multi Language Pack がインストールされている必要があります。
*8　制限ユーザで動作しない場合があります。
*9　ワクチン USB ソフトウェアに付与されている権限が許可されているファイルのみウイルススキャン・削除・隔離が可能です。
　　またウイルススキャン・削除・隔離の可否は個々のフォルダ・ファイルに設定されているアクセス許可(設定)にもよります。
*10 フルコンポーネント状態で動作確認を取っております。コンポーネントが削られている環境ではお客様がご確認をお願いいたします。

NOTE	ウイルス定義のファイルサイズは、ウイルスの増加に対応するため、日々増加しています。 それに伴い動作に必要なメモリ容量も増加しています。 ページングファイル(仮想メモリ)を作成することにより、 物理メモリ以上のデータ処理が可能になる場合があります。 ※通常は、OS によって自動的に作成される設定となっています

5 制限事項について

●セキュリティソフトがインストールされている PC での動作について

セキュリティソフトがインストールされている PC では本ソフトウェアが正常に動作しない場合があります。セキュリティソフトが弊社のソフトウェアの動作制限、デバイスへのアクセス制限を行っている場合があるためです。
セキュリティソフトに誤検知された場合、ワクチン USB ソフトウェアの除外を行ってください。

●OS やソフトウェアによって対応デバイスへのアクセスが制限されている場合の動作について

OS やソフトウェアによってデバイスへのアクセスが制限(デバイスコントロール等)されている場合、ワクチン USB に動作制限がかかる場合があります。その場合、ワクチン USB の除外を行ってください。

●インターネット接続について

本ソフトウェアを実行するためにインターネット接続は必要ではありません。ただし本ソフトウェアの定義ファイル更新・アップデート取得の際にはインターネット接続が必要となります。インターネットへアクセス制限が掛かっている場合、以下のアクセス許可を行ってください。

■定義ファイル更新
・http://update.nai.com/へのアクセスが許可されていること(ポート：80/8080)

■ソフトウェア更新
・http://dl.hscjpn.co.jp/へのアクセスが許可されていること(ポート：80/8080)
・http://www.hagisol.co.jp/へのアクセスが許可されていること(ポート：80/8080)
・https://www.hagisol.co.jp/へのアクセスが許可されていること(ポート：443)

■ライセンス更新
・http://www.udrw.com/へのアクセスが許可されていること(ポート：80/8080)
・http://dl.hscjpn.co.jp/へのアクセスが許可されていること(ポート：80/8080)

●ウイルススキャン範囲について

ワクチン USB がウイルススキャンできる範囲はワクチン USB ソフトウェアに付与されている権限が許可されているファイルのみウイルススキャン(削除・隔離)が可能です。
OS へのユーザーログイン権限とソフトウェアが持っている権限は同じではありません。
そのような場合、ワクチン USB ソフトウェア(startup.exe)を右クリックし「管理者として実行」やワクチン USB の設定で権限昇格する設定を行ってください。

[ワクチン USB の設定方法]
１：ワクチン USB のメイン画面の上部のツール→設定を選択。
２：設定画面のタブ：画面表示を選択し、権限昇格制御設定を[有効]にして、保存する。

この設定により、毎回起動する度にワクチン USB の権限昇格画面が表示されますので、
お客様で管理者のユーザー名を選択、必要に応じてパスワードを入力してください。

6 使用の流れ・使用方法についての動画

本製品のセットアップからご使用までの流れを以下に記載します。

■ライセンス開始(アクティベーション)

ライセンス開始 (アクティベーション)	インターネットがつながった PC で定義ファイルを更新してください。 アクティベーションが行われ、ライセンスが開始されます。

■製品のご使用

ウイルススキャン実行	対象機器に接続し、ウイルススキャンを実施してください。
ウイルススキャン 結果(ログ)の確認	ウイルススキャンが終了すると、ウイルス検出結果が画面に表示されます。 また本製品に搭載された 2 つの LED(青・赤)でも結果を表します。 ログを確認すればウイルス感染の状況を確認することができます。
(ウイルスが見つかった場合) ウイルス削除・隔離の実行	ウイルスが発見された場合、ウイルススキャン結果より、削除しても問題が無いウイルスファイルであることを確認してください。 問題無いことを確認後、「スキャン＋即駆除」、「スキャン＋即隔離」を選択し、ウイルスの削除・隔離を行なってください。

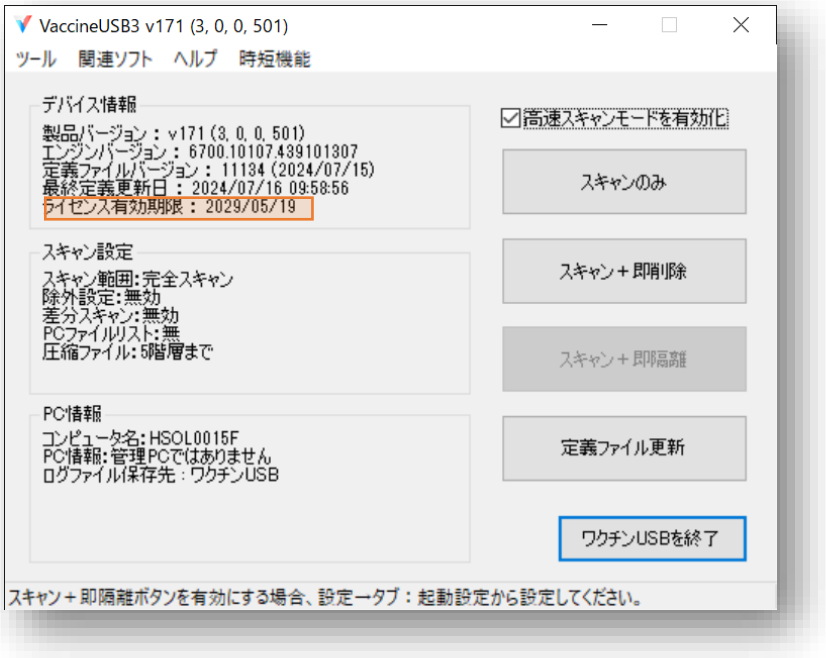
ワクチン USB の使用方法に関する動画を用意しております。※要インターネット接続
ワクチン USB の起動画面の[使用方法 動画を見る]を押してください。ワクチン USB3 の WEB ページが開きますので動画を御覧ください。

7 アクティベーション・定義ファイル更新

ウイルススキャンする際は必ずウイルス定義ファイルを更新し、最新のウイルス定義ファイルをご使用ください。

ライセンス開始方法(アクティベーション)

初めて定義ファイル更新を行うと、自動的にライセンスが開始されます(アクティベーション)。
ライセンス有効期限はメイン画面で確認してください。※定義ファイル更新方法は次項をご確認ください。

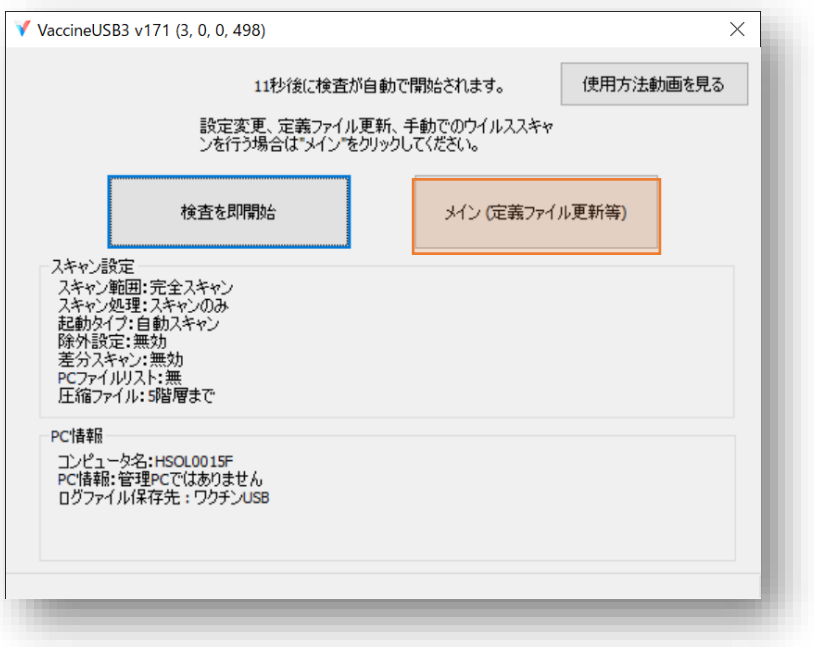


定義ファイル更新方法

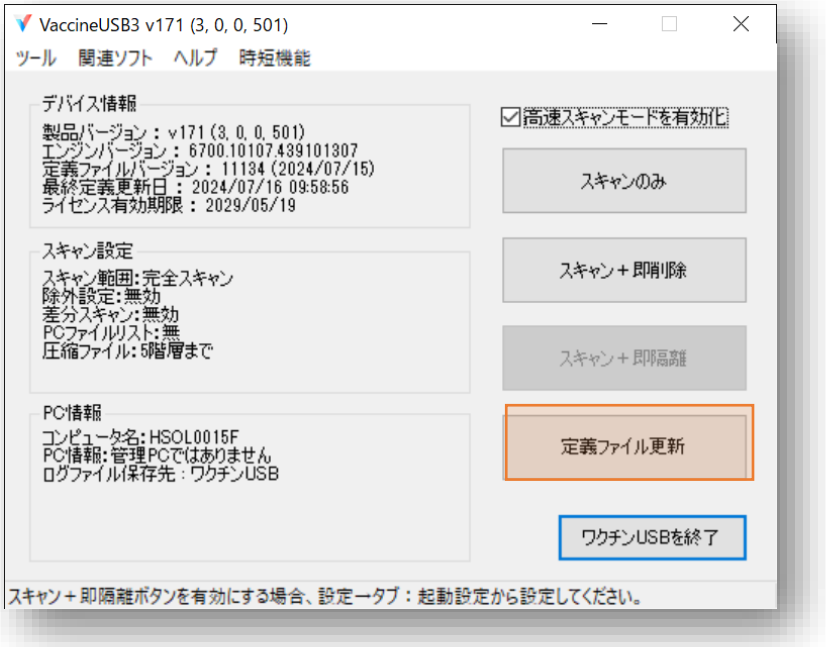
1：インターネットに接続している PC に、本製品を接続し、本製品を対象機器し、OS のコンピュータの[CD-ROM]アイコンを開き、[StartUp.exe]アイコンをダブルクリックしてください。
初回は使用許諾が表示されますので、内容を確認し、問題がなければ[OK]ボタンを押してください。

NOTE	• 再起動を促すメッセージが表示されることがありますが、再起動する必要はありません。表示された場合は、[いいえ]ボタンをクリックしてください。
	• 定義ファイル更新に失敗する場合、http://update.nai.com/へのアクセスが許可されていることをお客様の管理者様へ確認してください。

２：以下の画面で[メイン]ボタンをクリックしてください。
※本起動画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますのでそれまでに操作を行なってください。



３：メイン画面の[定義ファイル更新]ボタンをクリックし、画面の表示に従って、操作してください。



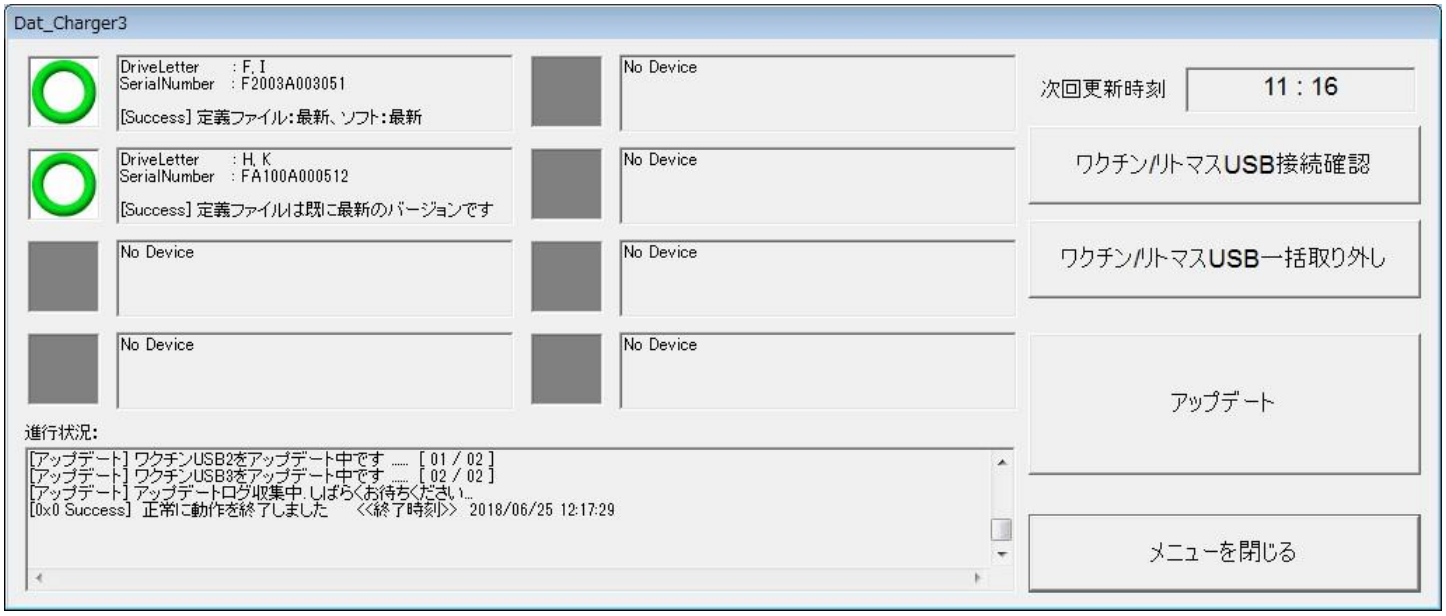
ウイルス定義ファイル更新処理後、ソフトウェアアップデート確認を行います。現在のバージョンより高いバージョンが確認できると、ソフトウェア更新アナウンス画面が表示されます。

通信環境により、ウイルス定義ファイルのダウンロードには時間がかかる場合があります。
ウイルス定義ファイルのダウンロード中は、対象機器や PC から本製品を抜かないでください。
アクセス LED（緑色）が点滅していないことを確認から取り外してください。
無理やり抜くと、データが壊れて本製品が故障する原因となります。

ワクチン USB を複数台同時にウイルス定義ファイル更新する

複数台同時にワクチン USB のウイルス定義ファイル更新するソフトウェア DatCharger3 をご用意しております。
DatCharger3 はワクチン USB3 の定義ファイル更新作業支援ソフトウェアです。
最大 8 台一括でワクチン USB3 の定義ファイル更新ができ、お客様の作業時間短縮と工数を減らします。
※注意：ソフトウェア・アップデートはできません。

■画面イメージ



■ダウンロード

Dat Charger3 はこちらからダウンロードしてください

8 ウイルススキャンする

ウイルススキャンの種類

本製品のウイルススキャンは以下の３種類あります。

スキャンモード	内容
スキャンのみ	PC 内のファイルをウイルススキャンし、ウイルスを発見します。 ウイルスは発見しても削除は行いません。 まずこのモードでご使用頂き、削除しても問題無いウイルスであることを確認した後に、スキャン＋即削除・即隔離モードでウイルスの削除・隔離を行う事を推奨致します。
スキャン＋即削除	PC 内のファイルをウイルススキャンし、ウイルスを発見次第削除します。 ※PC にとって重要なファイルでもウイルスであれば削除しますので、十分注意ください。
スキャン＋即隔離	PC 内のファイルをウイルススキャンし、ウイルスを発見次第隔離します。 ※PC にとって重要なファイルでもウイルスであれば隔離しますので、十分注意ください。 隔離したファイルは PC の特定フォルダに保存されます。

・SD や USB メモリは標準でウイルススキャンの対象となります。

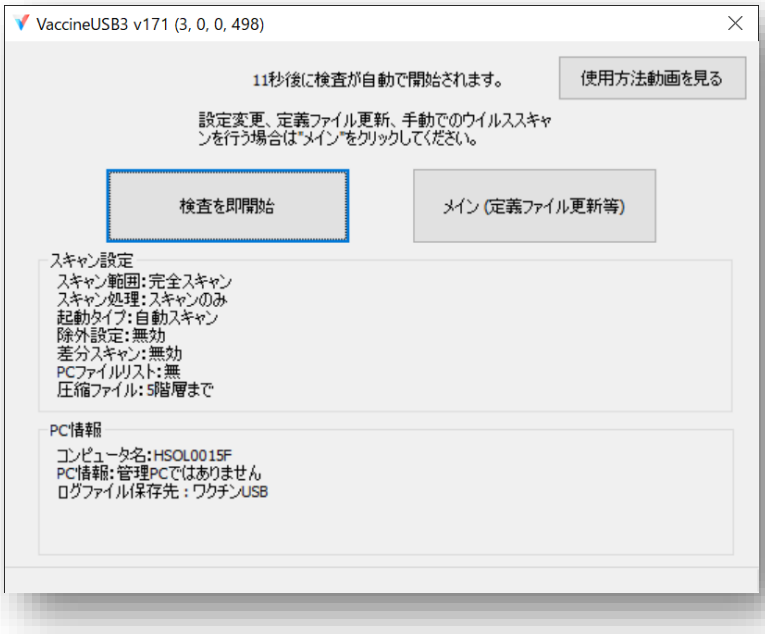
・ネットワークドライブは標準でウイルススキャンの対象外となります。対象とする場合、設定のカスタムスキャンを使用してください。

PC をウイルススキャンする

１：本製品を対象機器し、OS のコンピュータの[CD-ROM]アイコンを開き、[StartUp.exe]アイコンをダブルクリックしてください。

NOTE	• 再起動を促すメッセージが表示されることがありますが、再起動する必要はありません。表示された場合は、[いいえ]ボタンをクリックしてください。

２：起動画面が表示されます。



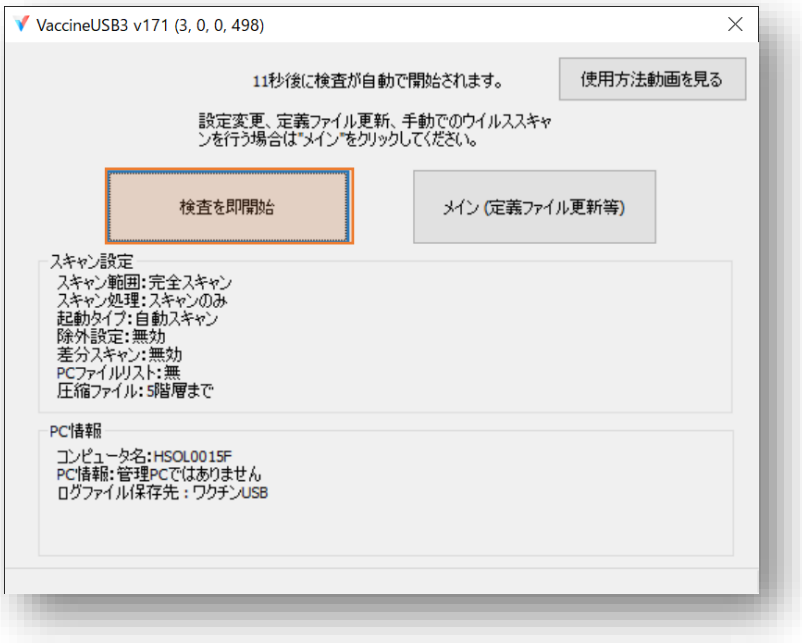
ウイルススキャンを開始する方法は３つあります。

①	起動画面で[検査開始]ボタンをクリックして、設定されているウイルススキャンを行う
②	起動画面で 15 秒待ち、自動的にウイルススキャンを行う。
③	メイン画面へ移動し、[スキャンのみ]、[スキャン＋即削除・隔離]を選択しウイルススキャンを行う。

各ウイルススキャン方法

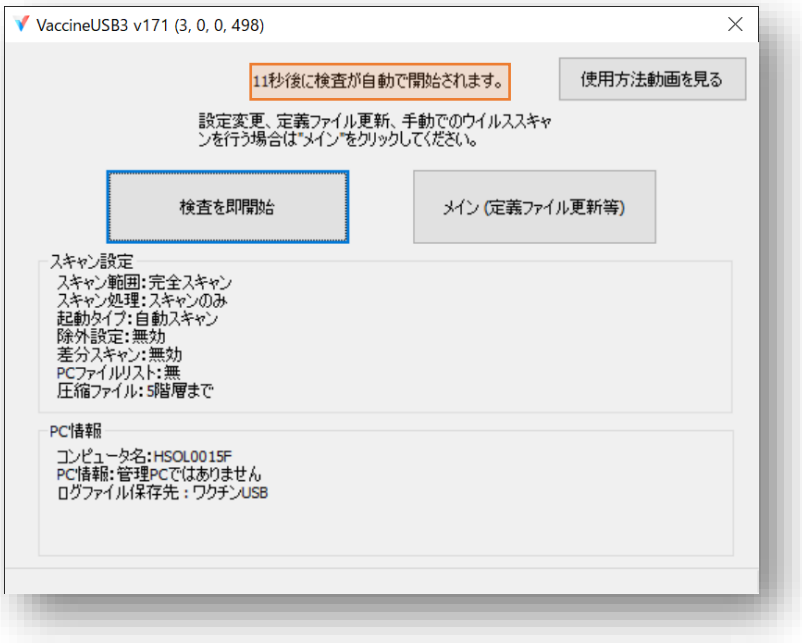
①	起動画面で[検査開始]ボタンをクリックして、設定されているウイルススキャンを行う

起動画面で[検査開始]ボタンをクリックしてください。スキャンが開始されます。



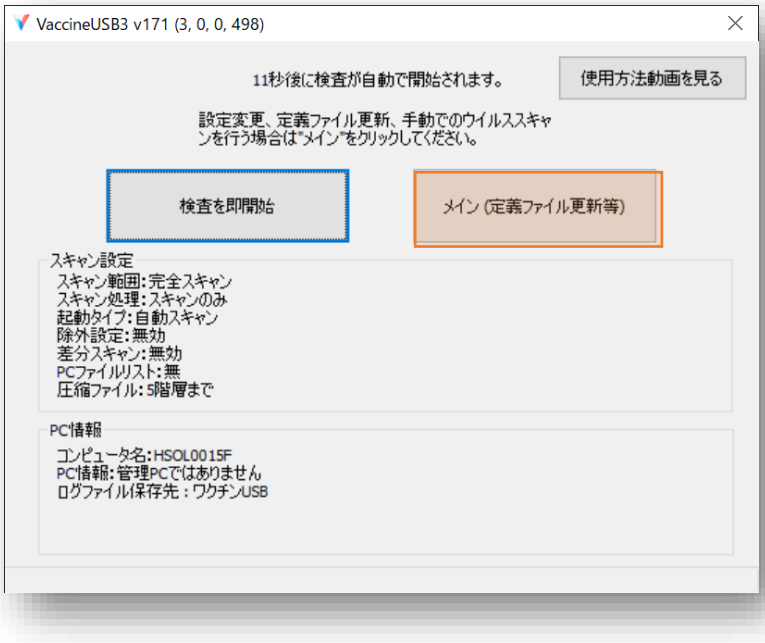
②	起動画面で 15 秒待ち、自動的にウイルススキャンを行う。

起動画面で 15 秒待つとウイルススキャンが開始されます。

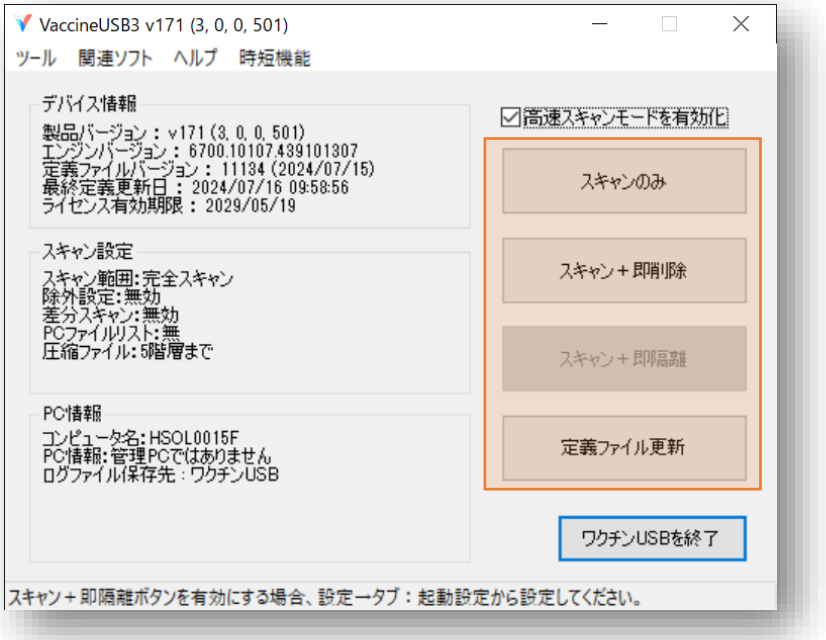


③	メイン画面へ移動し、[スキャンのみ]、[スキャン＋即削除・隔離]を選択しウイルススキャンを行う。

１：起動画面で[メイン]ボタンを押し、メイン画面へ移動してください。

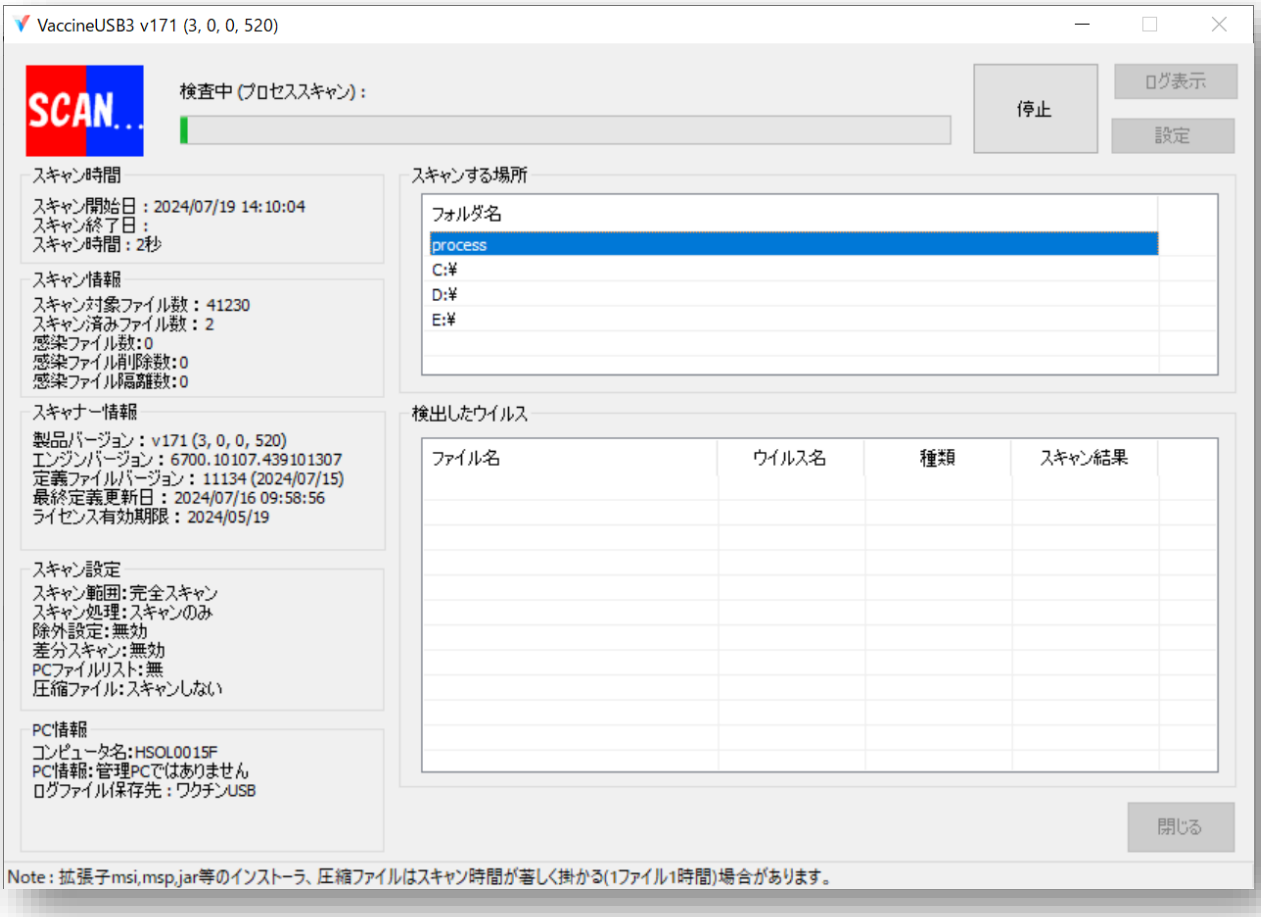


２：メイン画面で[スキャンのみ]、[スキャン＋即削除]、[スキャン＋即隔離]を選択し、ボタンをクリックしてください。選択したモードでウイルススキャンが開始されます。



※[スキャン＋即隔離]を切り替える(有効化)するには設定画面から行ってください。

３：ウイルススキャン画面に移り、ウイルススキャンが行われます。



４：ウイルススキャンが完了すると、検査結果画面が表示されます。結果を確認してください。

ウイルススキャン結果

■検査結果内容

検査結果画像	コメント	内容
	検査が正常に終了しました。ウイルスは見つかりませんでした。	ウイルスがみつからなかった場合に表示されます。
	検査が正常に終了しました。ウイルスが見つかりましたが、全て削除しました。	ウイルスが見つかったが、全てのウイルスの削除した場合に表示されます。
	検査が正常に終了しました。ウイルスが見つかりましたが、全て隔離しました。	ウイルスが見つかったが、全てのウイルスの隔離した場合に表示されます。
	ウイルスが見つかりました。	ウイルスが見つかった場合に表示されます。 ※スキャンタイプが[スキャンのみ]の場合に表示されます。
	全てのウイルスを削除できませんでした。	ウイルスが見つかったが、全てのウイルスを削除できなかった場合に表示されます。 ※スキャンタイプが[スキャン＋即削除]の場合に表示されます。
	全てのウイルスを隔離できませんでした。	ウイルスが見つかったが、全てのウイルスを隔離できなかった場合に表示されます。 ※スキャンタイプが[スキャン＋即隔離]の場合に表示されます。
	ワクチン USB にエラーが発生しました。	ワクチン USB にエラーが発生した場合に表示されます。※エラーが発生するまでの結果を検査情報に表示します。
	ワクチンUSBをユーザーによって途中で中断しました。	ユーザーによってワクチン USB を中断した場合に表示されます。 ※中断するまでの結果を検査情報に表示します。

項目	内容
コンピュータ名	PC のコンピュータ名を表示します。
スキャン終了日	ウイルススキャンを終了した日時を表示します。
スキャン時間	ウイルススキャンの実行時間を表示します。
スキャン対象ファイル数	PC 内のウイルススキャンを行った総ファイル数です。
スキャン済みファイル数	ウイルススキャンが終了したファイル数です。
感染ファイル数	検査によって見つかったウイルス感染ファイル数です。
感染ファイル削除数	検査によって見つかったウイルス感染ファイルを削除した数です。
感染ファイル隔離数	検査によって見つかったウイルス感染ファイルを隔離した数です。
差分ファイル コメント	差分スキャンの結果が表示されます。 ・差分スキャンは無効になっています。 ・差分スキャンを実施しました。 ・ＰＣファイルリストが未作成なため、差分スキャンを実施しませんでした。 次回以降差分スキャンが実施されます。 ・ＰＣファイルリストが未作成なため、差分スキャンを実施しませんでした。 ＰＣファイルリストの作成に失敗しました。

■検査結果内容(LED)

ワクチン USB 搭載 LED でも検査結果を表示します。モニターが無い端末実施にご確認ください。

青色 LED	赤色 LED	動作ステータス
交互点滅		スキャン実行中。
●	-	スキャン終了。感染はありませんでした。 または感染ファイルの削除/隔離に成功しました。
-	●	スキャン終了。感染ファイルを発見しました。
-	✿	プログラムエラーが発生しました。

✿ は点滅を示します。
● は点灯を示します。
— 消灯を示しています。

LED 位置

■ウイルスを発見した場合

ウイルスが発見された場合、ウイルススキャン結果より、削除しても問題が無いウイルスファイルであることを確認してください。問題無いことを確認後、「スキャン＋即駆除」、「スキャン＋即隔離」を選択し、ウイルスの削除/隔離を行なってください。ワクチン USB を取り外す場合は、[閉じる]ボタンを押し、メイン画面から[ワクチン USB を終了]ボタンを押してください。

※弊社ではウイルス情報についての問い合わせには対応できませんのでご了承ください。

ウイルスが削除できない場合

ウイルススキャン＋即削除・即隔離を繰り返し行ってもウイルスを削除できない場合は、システムファイルがウイルスに感染している、システムメモリにウイルスが存在している場合があります。その場合はウイルスの種類によって適切に処置する必要があります。
次の方法で削除できる場合もあります。

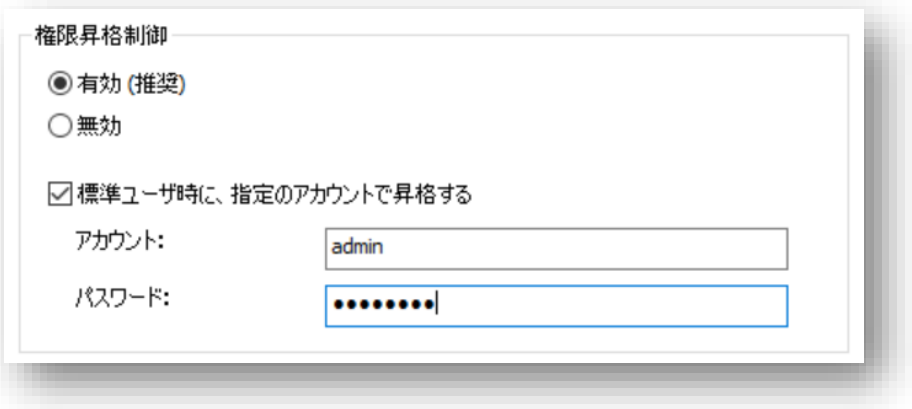
■権限昇格して実施

ワクチン USB を権限昇格させて実行することによって削除できる場合があります。権限昇格(設定)は設定画面から行うことができます。設定内容は以下を参照ください。

権限昇格制御

ワクチン USB ソフトウェアを権限昇格して使用する際に使用します。
本機能を有効にした場合、ワクチン USB3 起動時に管理者権限昇格画面が表示されますので、必要に応じてアカウント ID とパスワードを入力してください。

また指定のアカウントとパスワードを登録することができ、登録時は管理者権限昇格画面に自動的にアカウント ID とパスワードが入力されます。
すでに OS にログインしているアカウントが管理者権限の場合、そのログインしているアカウントを使用し、
ワクチン USB ソフトウェアの権限昇格を行います。



項目	内容
有効	ワクチン USB 起動時にワクチン USB ソフトウェアの権限昇格を行います。 そのため起動時に権限昇格画面が表示されます。 権限昇格時に自動的にアカウント・パスワードを入力する場合、アカウントとパスワードを登録してください。
無効	ワクチン USB 起動時にワクチン USB ソフトウェアの権限昇格を行いません。

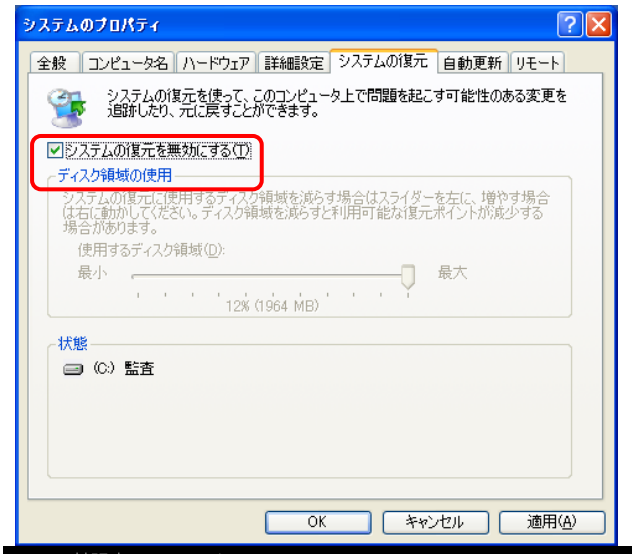
■セーフモードでの削除方法

Windows をセーフモードで起動して、ウイルススキャンを実行します。

システムレストア機能を無効にする方法

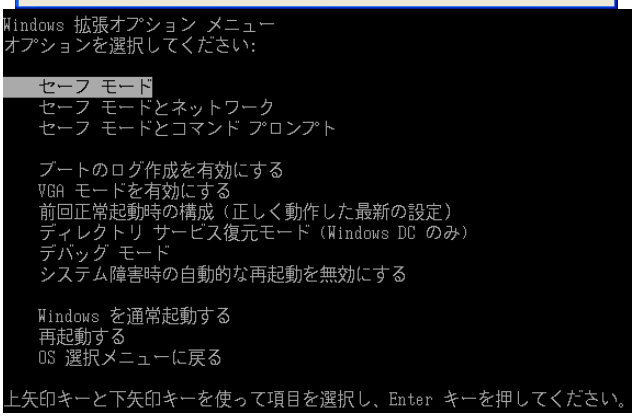
1. デスクトップ上のマイコンピュータアイコンを右クリックし、プロパティを選択します。
2. システムの復元タブをクリックします。
3. システムの復元を無効にする」をチェックします。
4. [OK]ボタンをクリックします。
5. 再起動を促されるので、「はい」を選択します。

※ レストアユーティリティを再度有効にするには、上記③で、「システムの復元を無効にする」のチェックを外します。

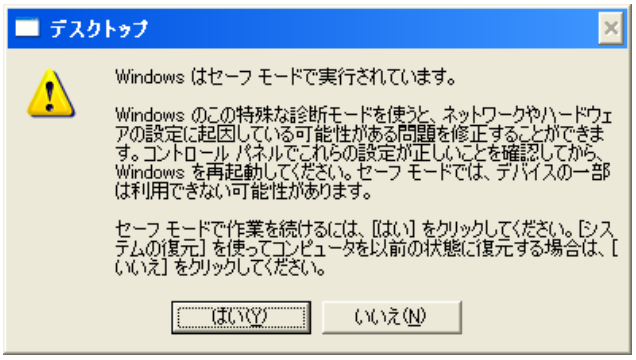


Windows をセーフモードで起動する方法

1. 電源が OFF になっていることを確認します。
   Windows が起動している場合は、Windows を終了します。
2. 電源を入れ、F8 キーを右図の画面が表示されるまで連打します。
3. 「セーフモード」を選択して、Enter キーを押します。



4. セーフモードで起動が始まります。右の画面が表示された場合は、[はい]をクリックします。

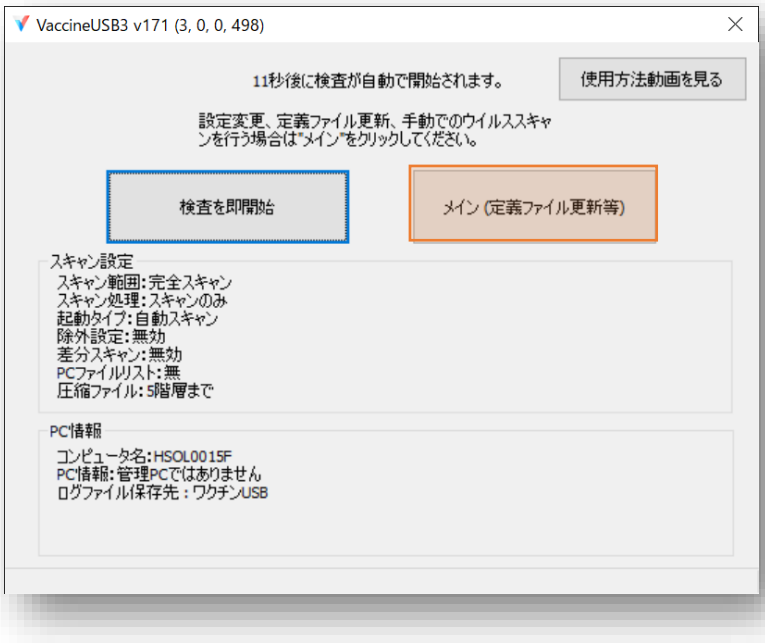


9 ログを確認する

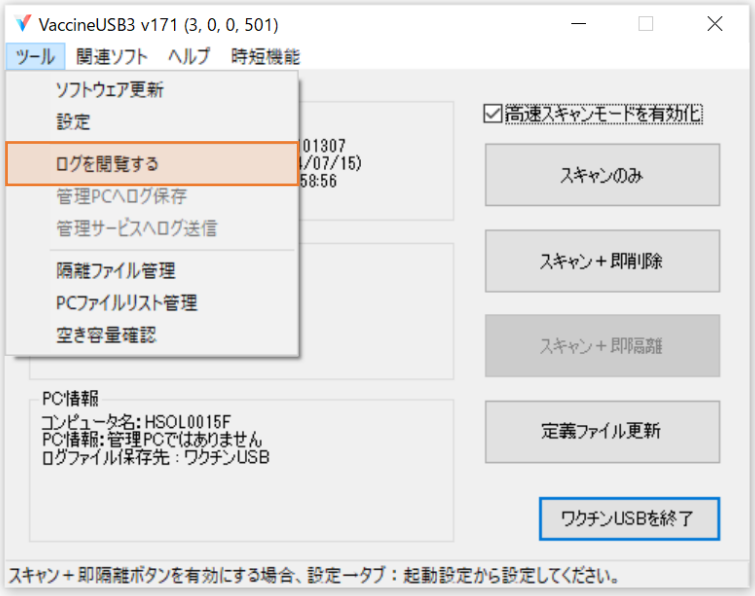
スキャンした結果は、ログファイルとしてワクチン USB 内に保存します。ログファイルは、スキャンするたびに生成します。ロゴの確認方法は以下をご確認ください。

1.PC へ本製品を接続し、起動画面で[メイン]ボタンをクリックしてください。

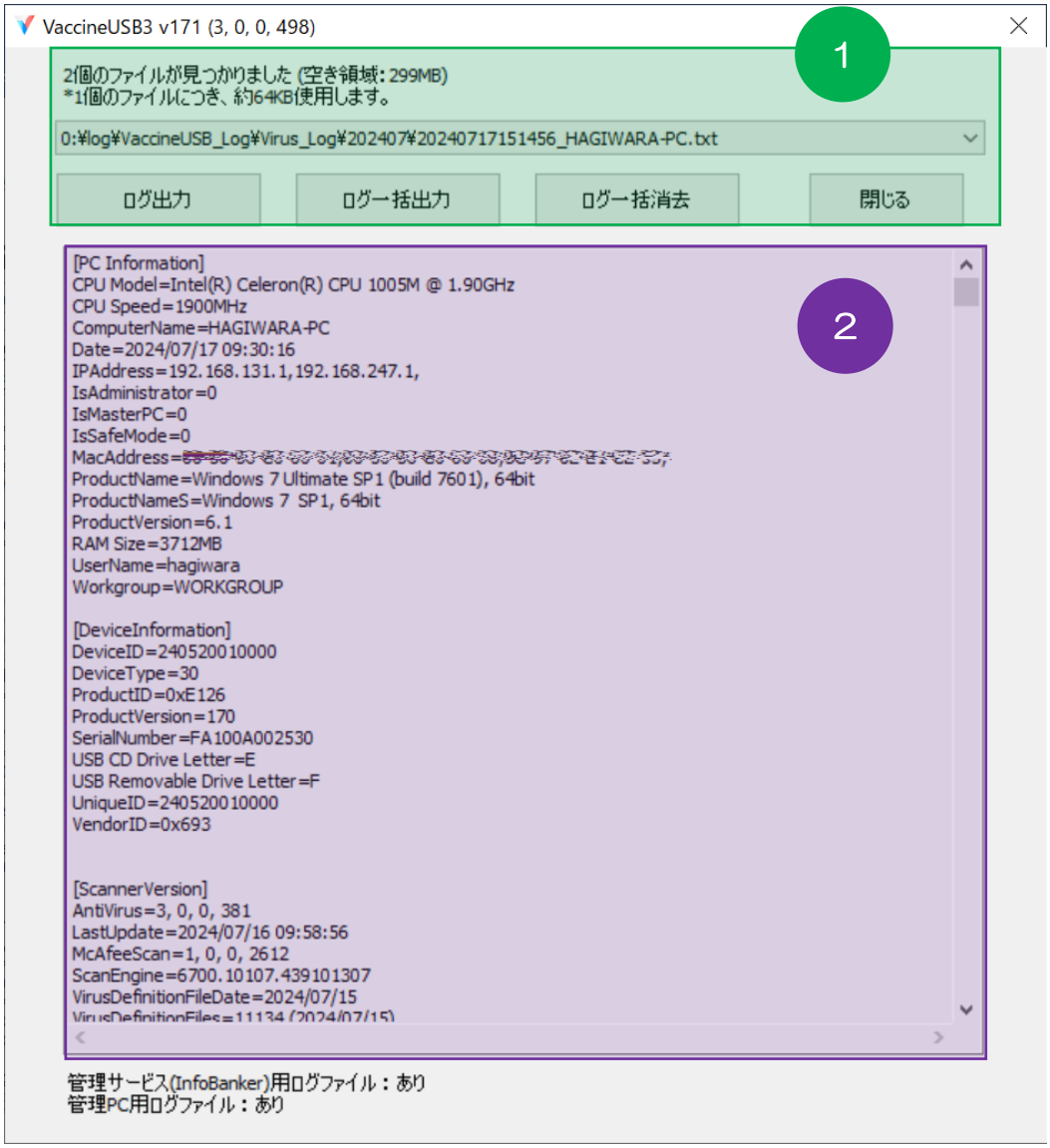
※この画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますので、それまでに操作を行なってください。



2.ツールバーの[ツール]を選択し、[ログを閲覧する]をクリックしてください。



3.ログ画面が表示されます。



1

・ログファイル数と、ログファイル格納領域の空き容量を表示
・ログファイル保存場所 / ログ・ファイル名を表示

項目	内容
ログファイル名	YYYYMMDDHHMMSS_スキャンしたコンピュータ名.txt
ログ格納フォルダ	YYYYMM フォルダの下にウイルス有り/ウイルス無しで分けられ保存されます。 ウイルス有り：Virus_Log フォルダに格納 ウイルス無し：NoVirus_Log フォルダに格納 例：2012 年 9 月にウイルススキャンを行い、ウイルス有りの場合の格納フォルダ フォルダ：VaccineUSB¥Virus_Log¥201209

・各種ログ制御ボタン

ボタン	内容
ログ出力	表示中のログを任意の場所へファイルとして出力します
ログ一括出力	保存しているすべてのログを任意の場所へファイルとして出力します。
ログ一括消去	保存しているすべてのログを削除します。 管理サービス用ログ、管理 PC 用ログファイルも削除されます。
閉じる	ログ画面を閉じ、メイン画面へ戻ります。

2 選択されたログファイルの内容を表示

ログ内容

項目（Key）	内容
セクション[PC_Information］ＰＣ情報	
CPU Model	CPU モデル
CPU Speed	CPU のクロック数
ComputerName	コンピュータ名
Date	ログファイル作成日時
IPAddress	IP アドレス（複数ある場合は、「、(カンマ)」区切りで表示）
IsAdministrator	0：制限ユーザー（標準ユーザー）、１：アドミン権限
IsMasterPC	0：管理 PC 1:管理 PC 以外の PC
IsSafeMode	0：セーフモード以外、１：セーフモード起動
MacAddress	MAC アドレス（複数ある場合は、「、(カンマ)」区切りで表示）
ProductName	OS バージョン（サービスパック/build 情報含む）
ProductNameS	OS バージョン（サービスパック含む）
ProductVersion	OS カーネルバージョン
RAM Size	メモリ容量
UserName	ログインユーザー名（アカウント名）
Workgroup	ワークグループ名
セクション[DeviceInformation］デバイス情報	
DeviceID	デバイスのケースに貼り付けられている番号(USB シリアルと同じ番号になります)
DeviceType	デバイスのタイプ（ワクチン：30 固定）
ProductID	デバイスの ProductID
ProductVersion	製品バージョン
SerialNumber	デバイスの USB シリアルナンバー
USB CD Drive Letter	ワクチン USB の CD ドライブのドライブレター　例：E
USB Removable Drive Letter	ワクチン USB のリムーディスクディスクドライブのドライブレター　例：G
UniqueID	弊社の管理番号
VendorID	デバイスの VendorID
セクション[ScannerVersion］スキャンアプリ情報	
AntiVirus	アンチウイルスソフトウェアバージョン
LastUpdate	定義ファイル更新日時
McAfeeScan	アンチウイルスソフトウェアライブラリバージョン
ScanEngine	スキャンエンジンバージョン
VirusDefinitionFileDate	ウイルス定義ファイル日時
VirusDefinitionFiles	ウイルス定義ファイルバージョン
セクション[ScanSetting］スキャンの設定	
IsEnableAccessControl	ワクチン USB への動作制限 0:動作制限をかけない

	1:動作制限をかける
IsEnableMasterPCLog	管理 PC ログファイル設定 0:管理 PC 用ログを作成しない 1:管理 PC 用ログを作成する
IsEnableRunas	権限昇格制御（0:無効設定 1:有効設定）
LogSaveType	2:ログを PC へ保存する場合、強制的にログを保存する
ScanMode	スキャンモード（0：完全スキャン、1：簡易スキャン、2：カスタムスキャン）
ScanType	スキャンタイプ （0：スキャンのみ、1：スキャン＋即削除　3:スキャン＋即隔離）
StartMode	スタートアップモード(0:カウントダウン　1:メイン画面表示　2:即スキャン)
IsEnableIncrementalScan	差分スキャン設定 0:差分スキャン無効 1:差分スキャン有効
CompareFileListName	差分スキャン時に使用した PC ファイルリスト名。 ※対象 PC の PC ファイルリストがワクチン USB 内に無い場合、表示されません
SaveFileListName	ワクチン USB 内に保存した PC ファイルリスト。 差分スキャン機能が有効な場合のみ、PC ファイルリストは保存されます。
セクション[TargetList] スキャンターゲットリスト	
TargetO	スキャンする場所のパス （Oには数字） ※複数ある場合は複数表示されます。
セクション[IgnoreList] 除外(フォルダ/拡張子)リスト	
TargerO	除外するフォルダ、拡張子を表示されます。
セクション[License] ライセンス情報	
LicenseAlert	弊社管理番号
LicenseLast	ライセンス終了日
LicenseStart	ライセンス開始日
LicenseTerm	ライセンス日数
セクション[Virus***] 検出したウイルスの情報（***：ウイルスナンバー（001～））	
Path	ウイルスのフルパス
Infectype	Trellix 社(旧マカフィ社)が規定しているウイルスの種類
VirusName	Trellix 社(旧マカフィ社)が規定しているウイルス名
Hash	ウイルスファイルのハッシュ
CleanAction	弊社の管理項目
Result	ウイルススキャンの結果 ・CleanActionNoAction：ウイルス発見しました（削除/隔離処理行なっていません） ・CleanActionVirusDeleteSuccess：ウイルス削除成功しました ・CleanActionVirusQuarantineSuccess：ウイルス隔離成功しました ・CleanActionDeleteFail：ウイルスの削除に失敗しました。 ・CleanActionQuarantineFail：ウイルスの隔離に失敗しました。
ウイルス検知時のログ例	[Virus001] Path=C:¥ABCDE.exe InfectType=AVT_TROJAN

	VirusName=GenericRXWK-DZ!6D2FA557E8D0 Hash=561E094A718485EFD453B0947A92B7E5C0F57910 CleanAction=0x29aa0024:CleanActionNoAction, Result=0x710f0003:KEY_AV_SUMMARY_INFECTED,
セクション[Error***] ウイルス処理の失敗した結果（***：ウイルスナンバー（001～））	
Path	ウイルスのフルパス
Result	ウイルススキャン結果
セクション[Result] スキャン終了時の結果	
StartTime	スキャンの開始日時
EndTime	スキャン終了時間
TotalTime	スキャンにかかった時間（秒）
TotalScanFiles	スキャンファイルトータル数
VirusFiles	ウイルス検知数
DeleteVirusFiles	ウイルス削除成功数
IsolateVirusFiles	ウイルス隔離成功数
NotDeleteOrNotIsolateVirusFiles	ウイルス削除/隔離 失敗数
ScanErrorFiles	スキャンエラーの数
ScanResult	最終的なスキャン結果 ・ウイルスなし：No Virus ・ウイルスあり：Virus Found
セクション[PC Infomation in detail] PC の詳細情報（****：（0001～））	
BIOSVersion	BIOS バージョン
CPUTotal	CPU の数
CPUTotalCore	CPU コア数
DiskTotal	ドライブ数
IEVersion	IE バージョン(複数ある場合は最新のものが表示)
NetAdapter***	ネットワークカード名
NetDate***	IP アドレスリース有効期限
NetGateway***	デフォルトゲートウェイ
NetIPAddress***	IP アドレスリース及び IPv6 アドレス
NetIPSubnet***	サブネットマスク
NetMACAddress***	MAC アドレス
OSLanguage	OS 言語
OSProductID	Windows プロダクト ID
SystemHostName	ホスト名
SystemManufacturer	コンピュータの製造元
SystemModel	コンピュータの型名
SystemProductIdentifyingNumber	コンピュータのシリアル
SystemProductUUID	マザーボードの UUID
セクション[PC Drive] PC のドライブ情報（**：（01～））	
DriveLetter**	ドライブレター

DriveCapacity**	ドライブ全容量(GB)
DriveFreeCapacity**	ドライブ空き容量(GB)
セクション[software] PC にインストールされているアプリケーション情報（****：(0001～)） ※設定->タブ；ログ内の資産情報管理で有効時のみ表示	
Name****	インストールされているアプリケーション名が入ります。 例：Hagiwara Security Scan Plus
Publisher****	インストールされているアプリケーションの会社名が入ります。 例：Hagiwara Solutions
Version****	インストールされているアプリケーションのバージョン 例：2.50.25
セクション[Hotfix] PC にインストールされている WindowsOS の更新プログラム情報（****：(0001～)） ※設定->タブ；ログ内の資産情報管理で有効時のみ表示	
KBName****	インストールされている更新プログラム名が入ります。 例：KB3035131
KBDate****	インストールされている更新プログラム名のインストール日が入ります。 例：2015/4/14

10 高速スキャンする(時短方法 1)

高速スキャンモードはウイルススキャンを高速化し、スキャン時間を短縮することができるモードです。
高速スキャンモードは PC の CPU スペック(コア数)が高い、メモリ(RAM)空き容量が多いほど、高速化されます。
CPU、メモリを最大限使用するため、本モード使用時は大変 PC が重くなりますので、ご注意ください。

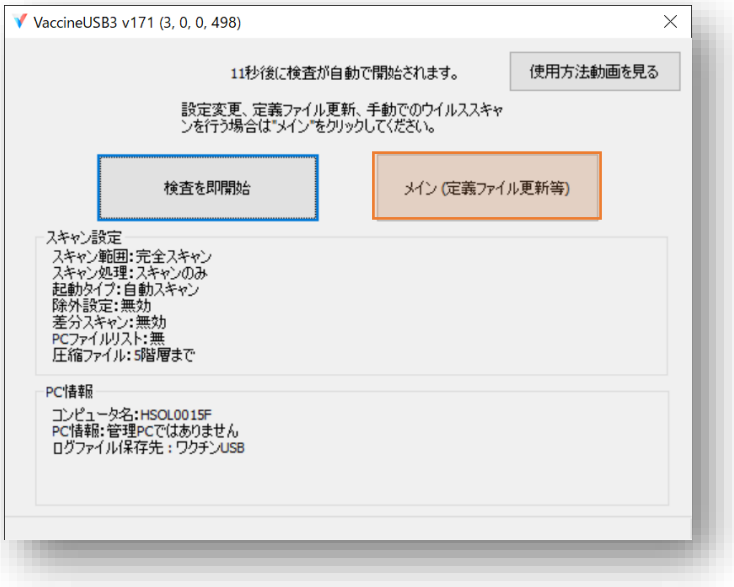
- 著しく古い PC 以外は高速スキャンモードを使用することを推奨いたします。
- スキャンするファイル数や各種設定は通常モードと変わりません。

項目	高速スキャンモード	通常スキャンモード
スキャン時間	短い	標準
PC の CPU 使用率	高い	標準
PC のメモリ使用量	多い	標準
スキャンするファイル	スキャンするファイルに変わりはありません	
設定の反映	設定の反映に変わりはありません	

■設定方法

本製品を接続し、以下の画面で[メイン]ボタンをクリックしてください。

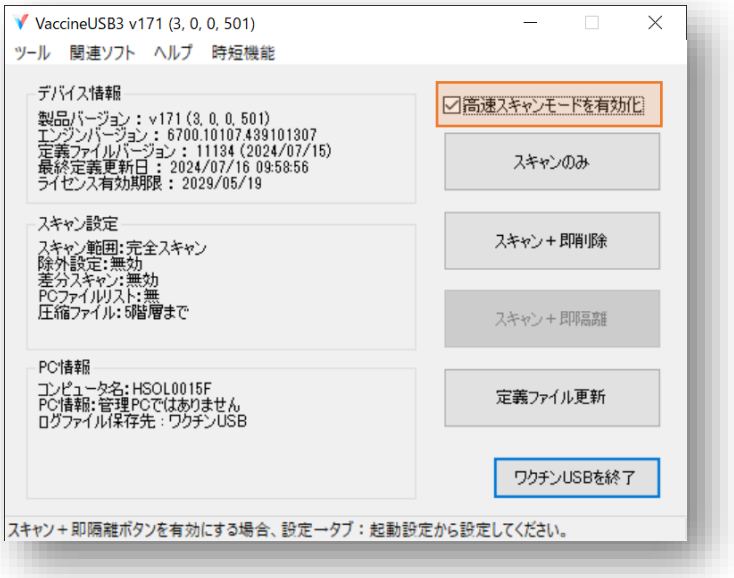
※この画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますので、それまでに操作を行なってください。



メイン画面の[高速スキャンモードを有効化]へチェックを入れてください。以上で設定は終了です。

このチェックが入った状態でスキャンを実施してください。

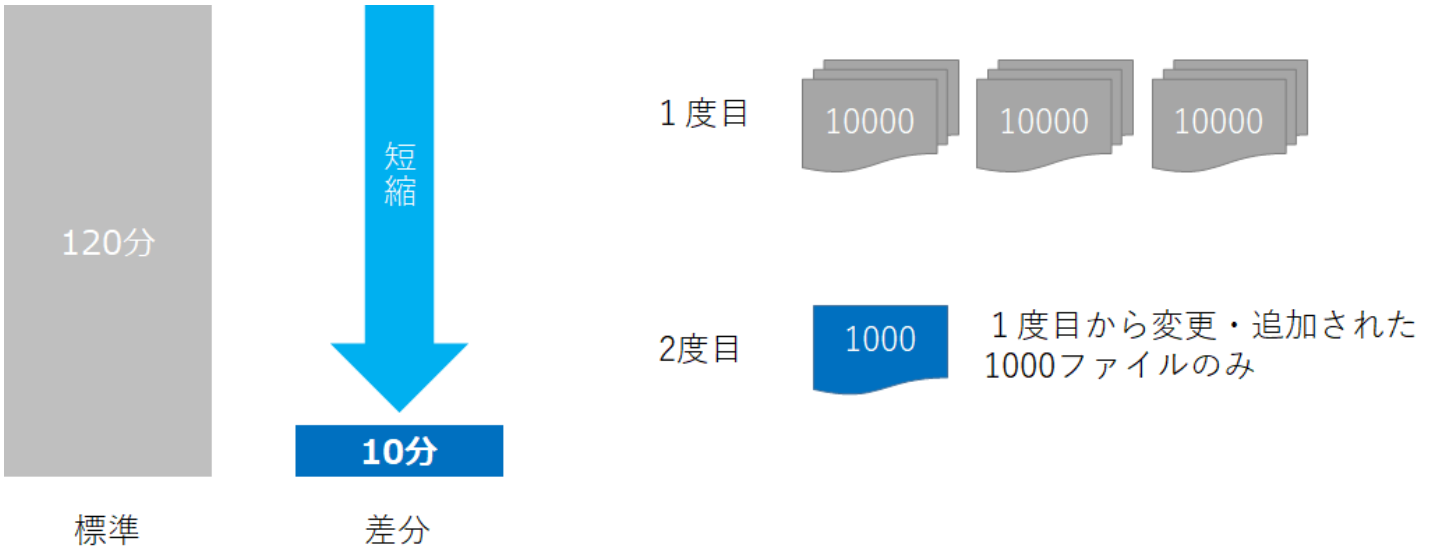
※起動画面から自動スキャンする場合、このチェックを事前に行ってください。



11 前回からの差分のみスキャンする(時短方法 2)

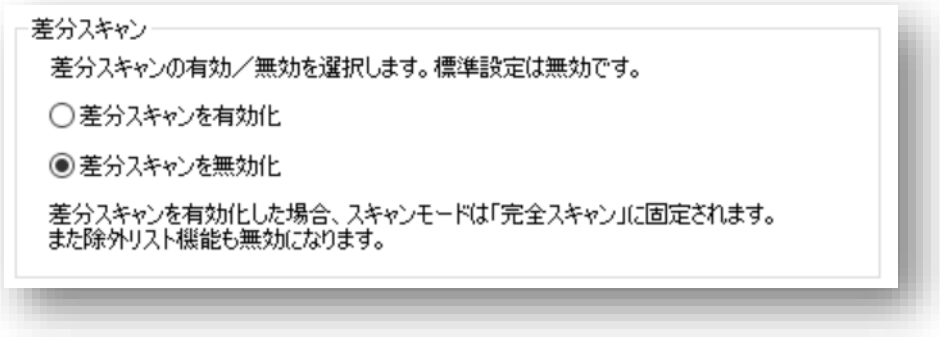
■差分スキャン機能とは
差分スキャン機能とは、前回のウイルススキャンから変更があったファイル、増えたファイルのみウイルススキャンを行う機能になります。この機能を使うことにより、２回目からのウイルススキャン時間の大幅な短縮を行うことができます。

例：PC に 30,000 ファイルあった場合、1 度目のウイルススキャンには 120 分掛かりました。
　　２度目には 31,000 ファイルあった場合、対象は 1,000 ファイルになり、10 分以下でウイルススキャンは終了。



上記例での差分のファイル(1,000 ファイル)を抽出するために 1 度目に行った３万ファイルのファイル情報(PC ファイルリスト)を 1 度目のスキャン時にワクチン USB 内に保存します。その PC ファイルリストとスキャン実行時の PC のファイルを比較※し、その差分があったファイルのみウイルススキャンを行います。
※作成日時、サイズに変更があったファイル、PC ファイルリストに含まれていないファイル(増えたファイル)

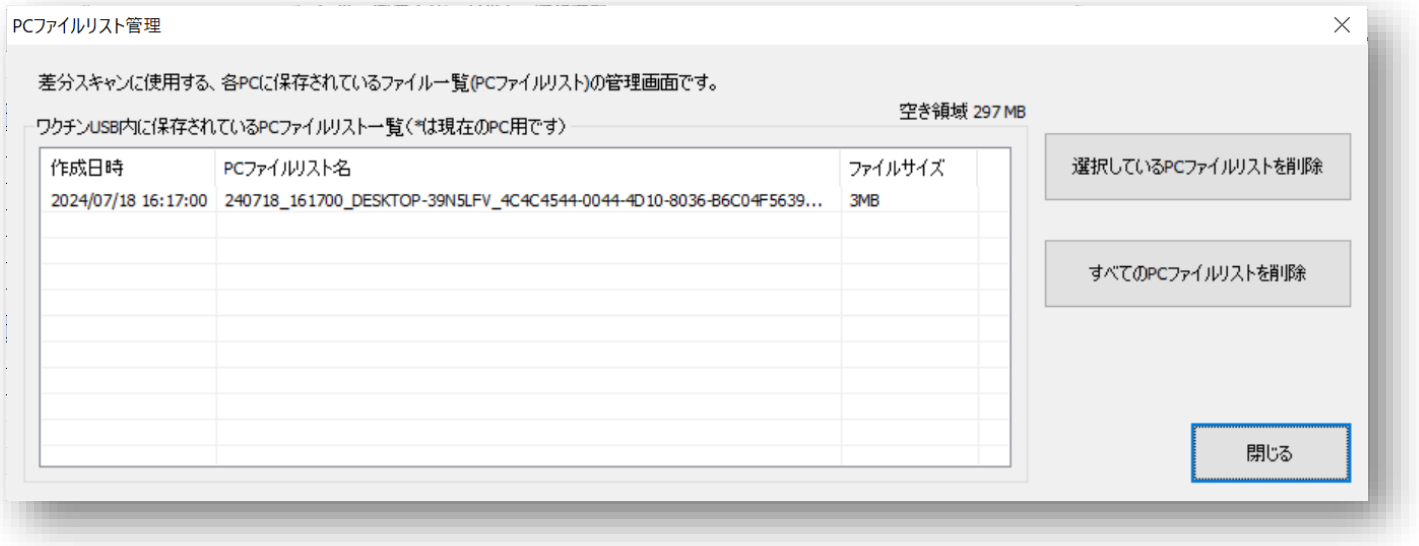
■差分スキャン設定方法
設定画面から差分スキャン機能を設定することができます。[差分スキャン]内の[差分スキャンを有効化]を選択・保存してください。



差分スキャンを有効にした場合、スキャンモードは「完全スキャン」に固定され、除外リスト機能も無効になります。

■PC ファイルリスト管理

PC のファイルリスト一覧はワクチン USB に保存されますが、その PC ファイルリストを確認、削除することができます。メイン画面→ツール→PC ファイルリスト管理を選択してください。管理画面に移動することができます。



[選択している PC ファイルリストを削除]、[すべての PC ファイルリストを削除]でワクチン USB 内に保存されている PC ファイルリストを削除することができます。

■PC ファイルリスト仕様

項目	内容
PC ファイルリストサイズ	PC 内にあるファイル/フォルダ数、ファイル/フォルダ名長によって可変。 ※PC のファイル数によっては 5MB を超える場合もあります。
保存先	ワクチン USB
最大保存容量	300MB ※PC ファイルリストの合計サイズが 300MB を超える場合は、PC ファイルリストを保存することができません。エラーが表示されます。 そういった場合は PC ファイルリスト管理から削除、空き領域を確保してください。
取得タイミング	ウイルススキャン終了時
PC ファイルリスト名 ルール	ウイルススキャン実施日時_コンピュータ名_PC 固有キー 例：170329_175408_WINSEV3E_40279CD-C4FE-DC11-BDEE-8E13CDB985
その他ルール	1 台の PC に対して、最新のファイルリストのみ保存されます。 例えば PC(A)に対して 3 度ウイルススキャンをした場合、3 度目終了後には 3 度目にスキャンした時のファイルリストのみが保存されている状態となります。 1 度目と 2 度目のファイルは順次削除されます。

■差分スキャンの表示

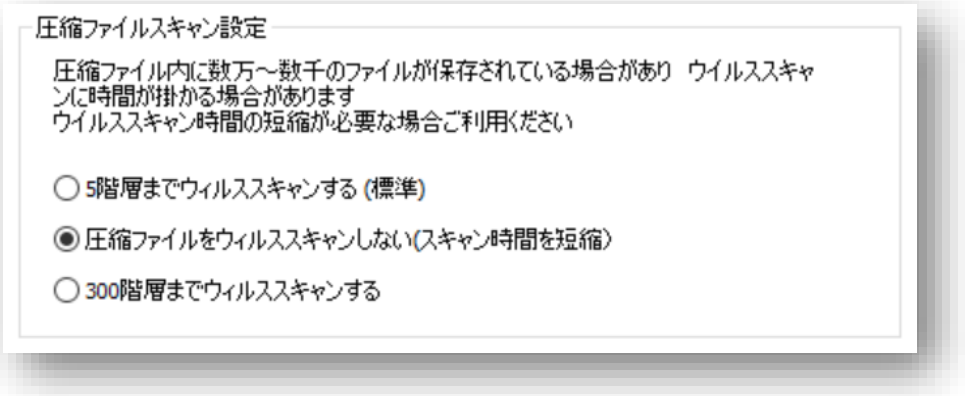
２度目以降の差分スキャン実施時する際にはボタン表示が変わります。

12 圧縮ファイルをスキャンしない(時短方法 3)

多言語用ファイル、Java Archive(拡張子：jar)などは圧縮ファイル内に数万～数千のファイルが保存されている場合があります。これらを安全に解凍しながら、ウイルススキャンを行うため非常に時間が掛かります。
通常圧縮ファイルの５層までのファイルをウイルススキャンしますが、圧縮ファイルをスキップするオプションを用意しております。ウイルススキャン時間の短縮が必要な場合、ご利用ください。

設定方法

設定画面から差分スキャン機能を設定することができます。[圧縮ファイルスキャン設定]内の[圧縮ファイルをウイルススキャンしない]を選択・保存してください。



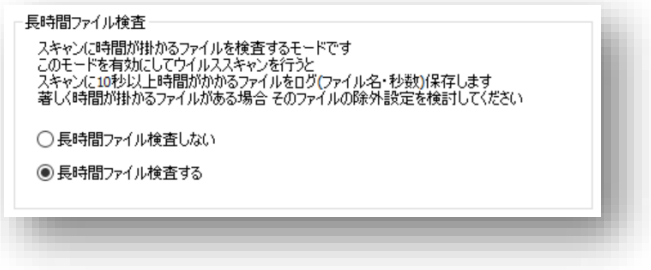
13 スキャンに時間が掛かるファイル検査（時短方法 4）

スキャンに時間が掛かるファイルをお客様で確認できるモード(長時間ファイル検査モード)を用意しております。
このモードを使用しウイルススキャンを行うと、10 秒以上時間がかかるファイルをログ(ファイル名・秒数)保存します
著しく時間が掛かるファイルがある場合 そのファイルの除外設定を検討してください。

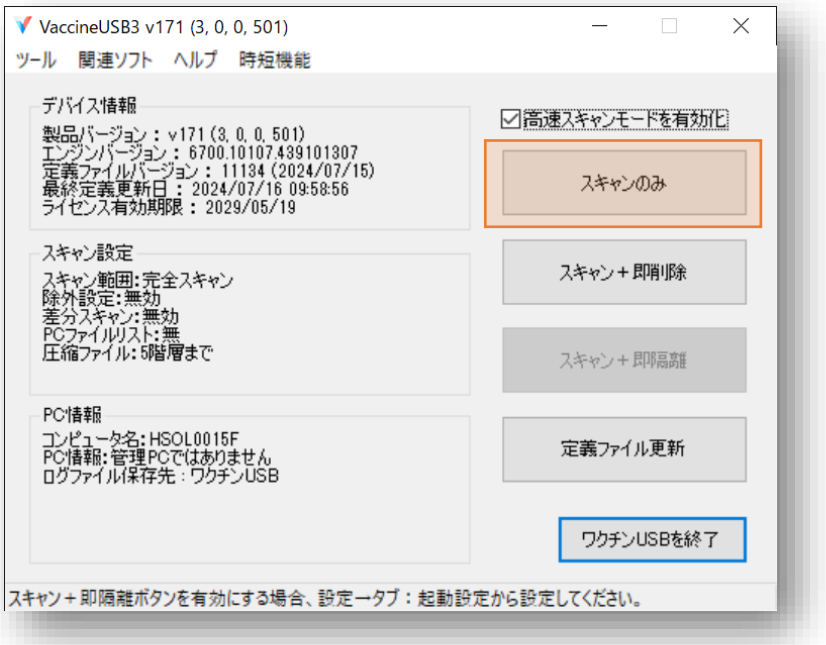
長時間ファイル検査モードを使用しウイルススキャンすると、ログを残すため通常より時間が掛かります。
スキャンに時間が掛かるファイルを確認する場合のみご利用ください。
※長時間ファイル検査する・しないでウイルススキャンするファイル種類・数に違いはございません。

設定方法

設定画面から差分スキャン機能を設定することができます。[長時間ファイル検査]内の[長時間ファイルを検査する]を選択・保存してください。



その後にウイルススキャンを行ってください。



ウイルススキャン完了時にログが保存されます。

ログの保存場所	デスクトップ
ログフォルダ名	VaccineUSB_Log
ログ・ファイル内容	・10 秒以上ウイルススキャンに時間が掛かったファイル名(ファイルパス) ・ウイルススキャンに掛かった秒数

ログ・ファイルを確認し、必要に応じてファイル除外・圧縮ファイル除外などを行ってください

14 隔離したウイルスの管理

ウイルススキャンで[スキャン＋即隔離]を実行し、ウイルスを検知した場合、ウイルスを PC の特定フォルダへ隔離、保存します。ウイルスはパスワード付き圧縮されます。
隔離したウイルスファイルはワクチン USB→安全な PC へ安全に移動でき、検体としてウイルス解析依頼をウイルススキャンメーカへ行うことが容易になります。

隔離ファイル概要

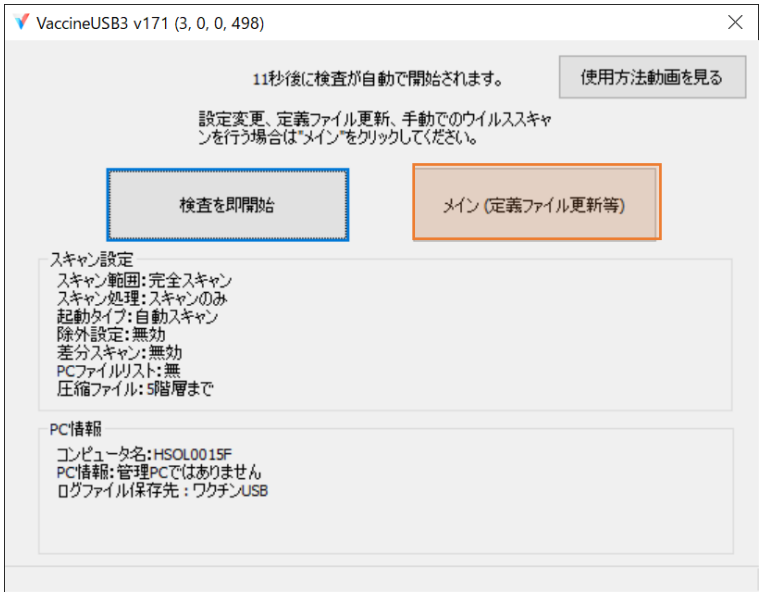
隔離ファイルの仕様は以下になっています。

項目	内容
ファイル圧縮形式	パスワード付圧縮　パスワード：infected
隔離ファイル保存先	%appdata%¥vusb¥isolation¥ ※Windows のエクスプローラのアドレスバーへ入力してください。
隔離ファイル名ルール	隔離した日時_乱数　例：20160211093312_07adf431

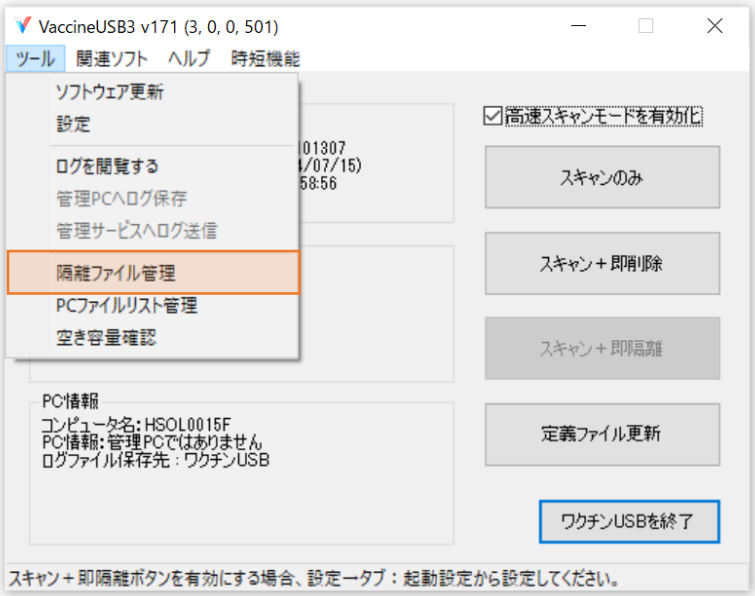
隔離ファイル管理画面への移動

1.PC へ本製品を接続し、以下の画面で[メイン]ボタンをクリックしてください。

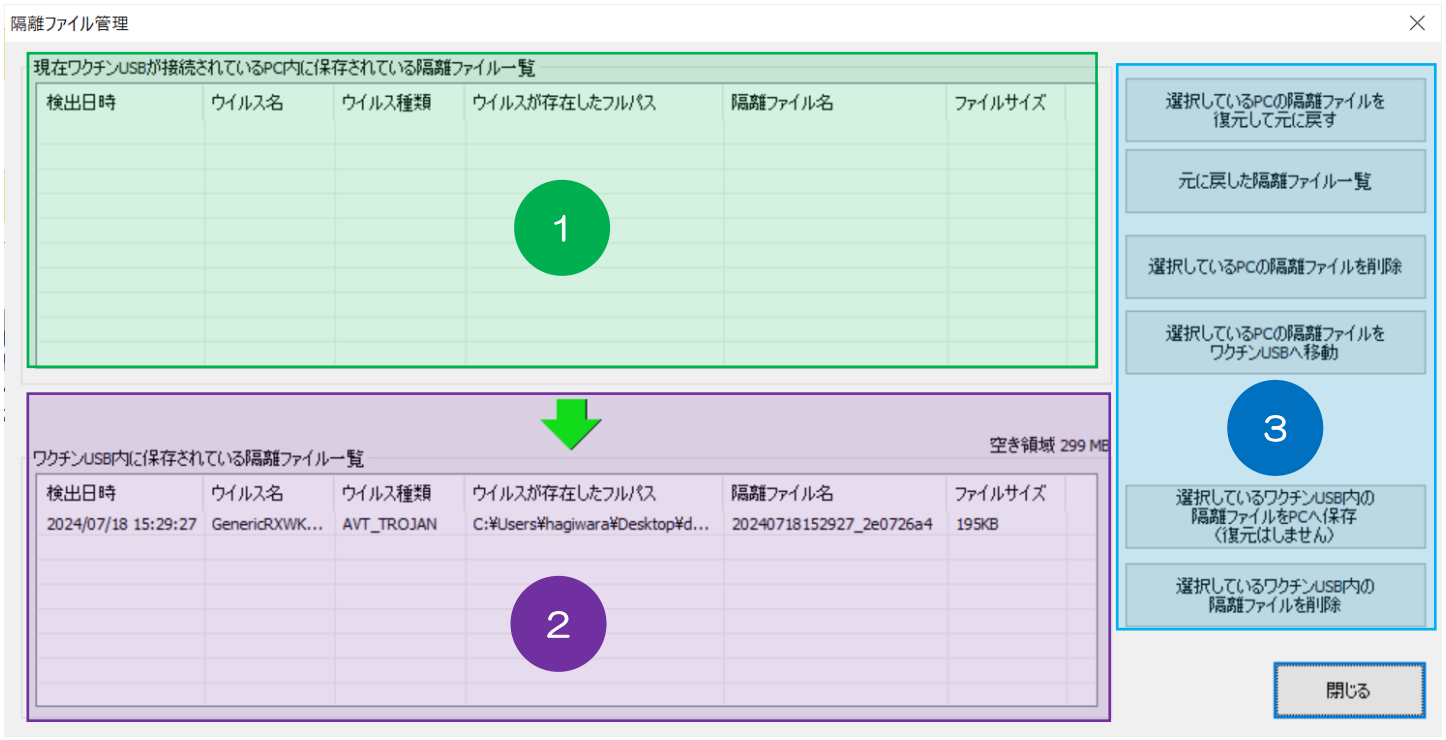
※この画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますので、それまでに操作を行なってください。



2.ツールバーの[ツール]を選択し、[隔離ファイル管理]をクリックしてください。隔離ファイルの管理画面に移動します。



隔離ファイル管理画面 概要



1 現在ワクチン USB が接続されている PC 内に保存されている隔離ファイル一覧

2 ワクチン USB 内に保存されている隔離ファイル一覧

3 PC・ワクチン USB に保存されている隔離ファイルへの処理ボタン

PC に隔離したウイルスを確認する

PC に隔離したウイルスは隔離ファイル管理画面の①で確認することができます。

PC に隔離したウイルスを元に戻す

PC に隔離されいている隔離ファイル(ウイルス)を解凍し、元の場所へ戻すことができます。
元に戻したい隔離ファイル①を選択して、「選択している PC の隔離ファイルを解凍して元に戻す」ボタンを押してください。
注意：解凍後、ウイルスとして動作する可能性がありますのでご注意ください

隔離したウイルスを削除する

PC に隔離されているファイルを削除することができます。削除する隔離ファイル①を選択して
[選択している PC の隔離ファイルを削除]ボタンを押してください。

元に戻した隔離ファイル一覧を確認する

元に戻した隔離ファイル一覧を確認することができます。現在ワクチン USB が接続されている PC の履歴となり、
他の PC の履歴は確認できません。[元に戻した隔離ファイル一覧]ボタンを押してください。リストが表示されます

ワクチン USB へ隔離ファイルを移動する

PC に隔離されている隔離ファイルをワクチン USB へファイルを削除することができます。隔離ファイルを PC へ移動し解析依頼する場合などにご使用ください。ワクチン USB の特殊領域へ保存するので、安全に隔離ファイルを移動することができます。また隔離ファイルはパスワード圧縮されているの安全です。(パスワード：infected)
移動する隔離ファイル①を選択して、[選択している PC の隔離ファイルをワクチン USB へ移動]ボタンを押してください。

ワクチン USB に保存した隔離ファイルを PC へ移動する

ワクチン USB に保存されている隔離ファイルを PC へ保存することができます。ウイルスメーカへウイルス解析する場合などにご使用ください。隔離ファイルはパスワード圧縮されているの安全です。(パスワード：infected)
移動する隔離ファイル②を選択して、[選択しているワクチン USB 内の隔離ファイルを PC へ保存]ボタンを押してください。

ワクチン USB に保存した隔離ファイルを削除する

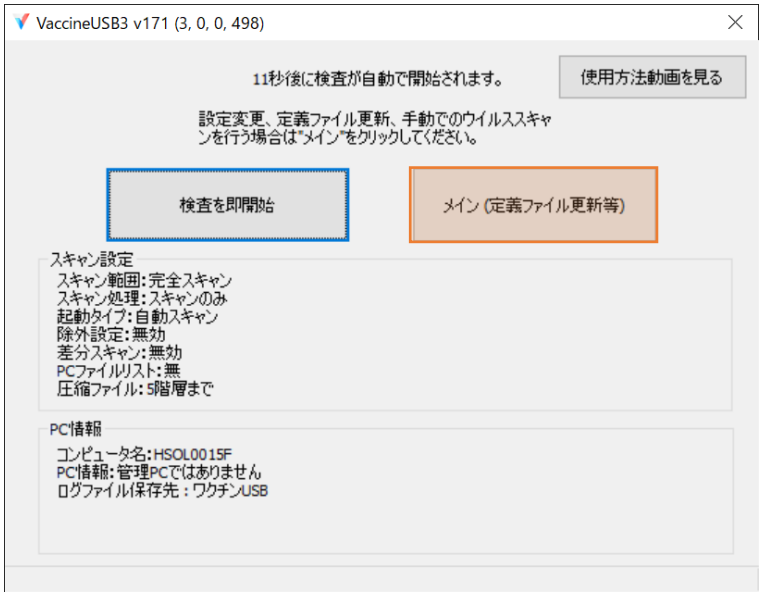
ワクチン USB に保存されている隔離ファイルを削除することができます。
削除する隔離ファイル②を選択して、[選択しているワクチン USB 内の隔離ファイルを削除]ボタンを押してください。

15 設定を変更する

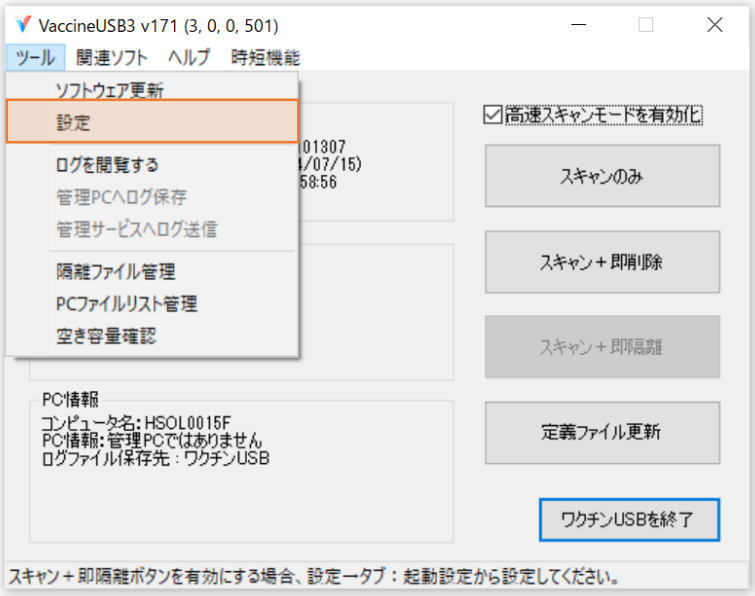
ワクチン USB の機能設定を変更することができます。

PC へ本製品を接続し、以下の画面で[メイン]ボタンをクリックしてください。

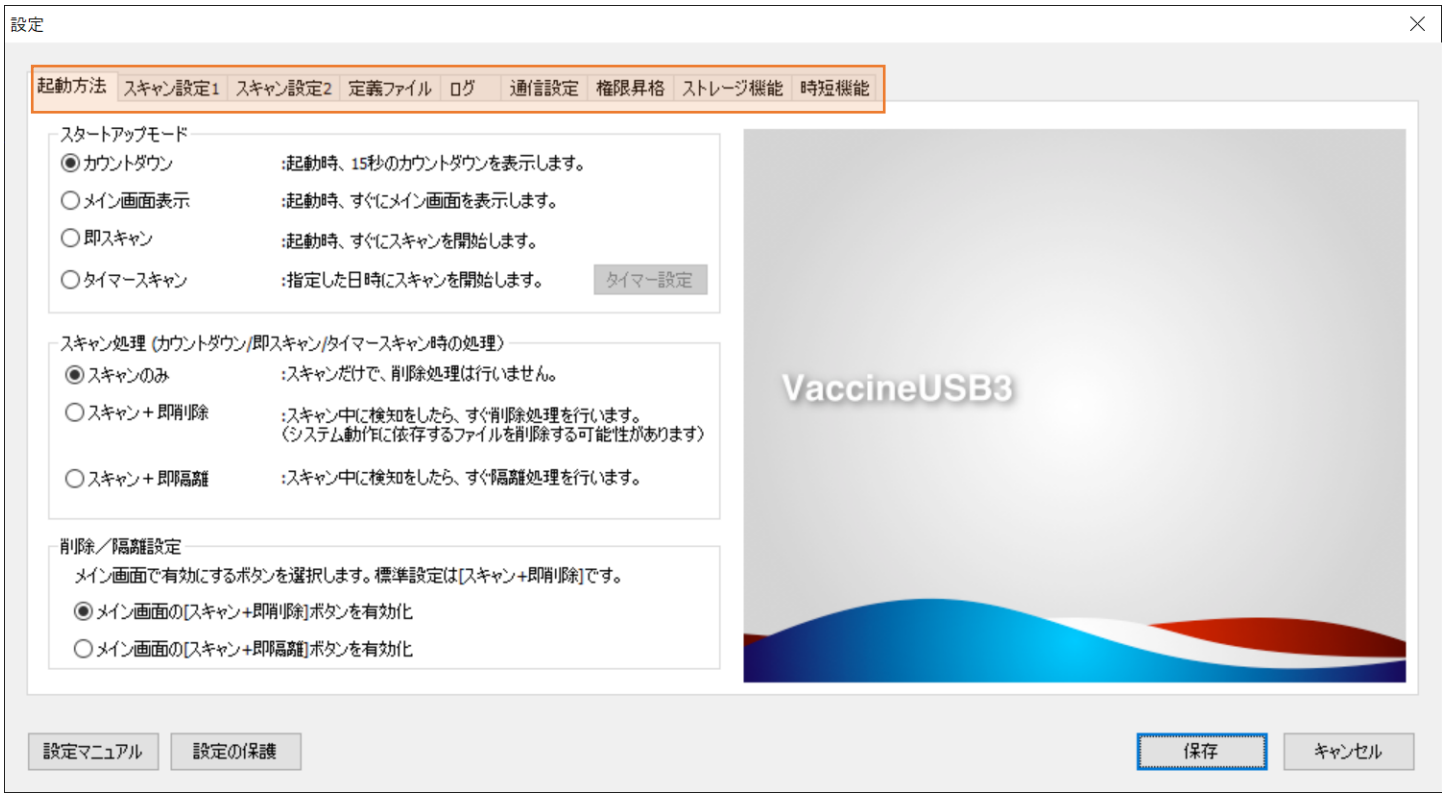
※この画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますので、それまでに操作を行なってください。



ツールバーの[ツール]を選択し、[設定]をクリックしてください。



設定画面が表示されます。設定を変更してください。

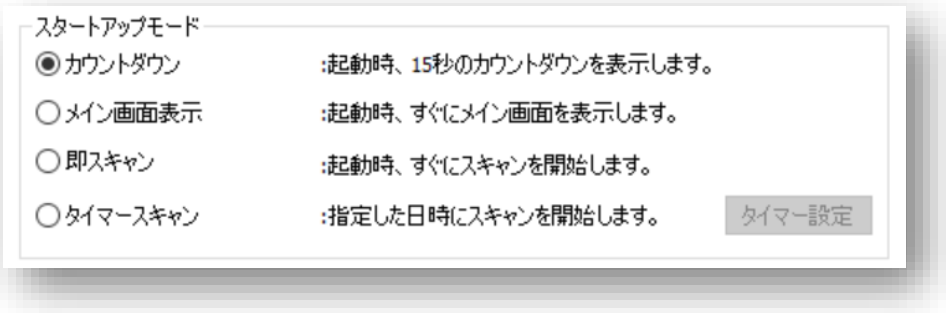


タブの説明（隠れているタブは、右上の  でスクロールすると表示されます）

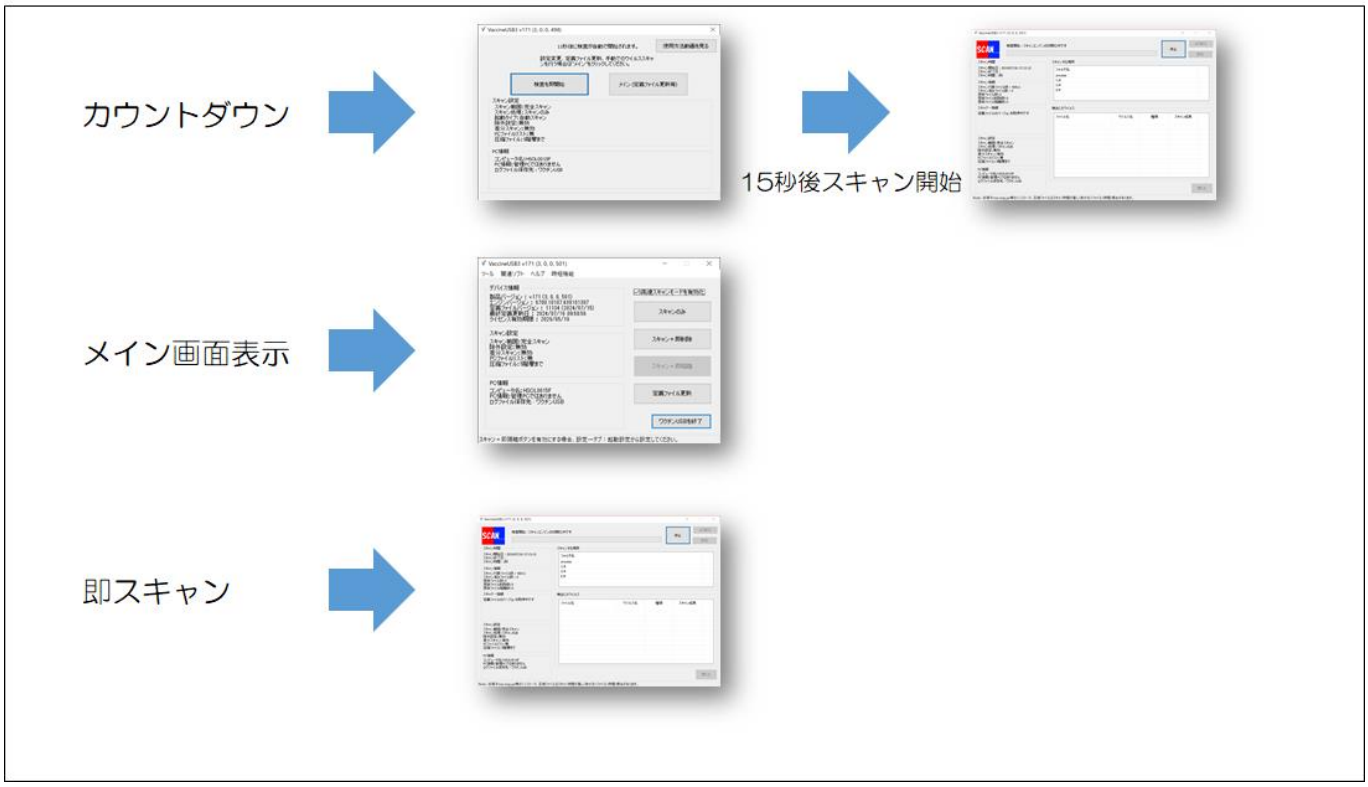
タブ	内容
起動方法	ワクチン USB 起動時の動作を設定することができます。
スキャン設定 1	ワクチン USB のスキャン設定を行うことができます。
スキャン設定 2	
定義ファイル	定義ファイル関連の設定を行うことができます。
ログ	ログ関連の設定を行うことができます。
通信設定	プロキシー設定等の設定を行うことができます。
権限昇格(画面表示から変更)	ワクチン USB の権限昇格設定・画面設定を行うことができます。
ストレージ機能	ワクチン USB のストレージ機能設定を行うことができます。
時短機能	ワクチン USB のスキャン時間を短縮する設定を行うことができます。

設定：起動方法

■スタートアップモード
ワクチン USB 起動時の動作を設定することができます。



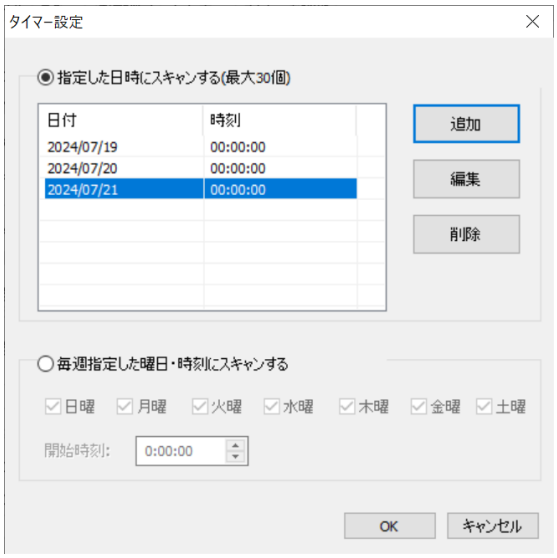
カウントダウン	起動時に約 15 秒のカウントダウン（スキャン開始）画面を表示します
メイン画面表示	起動時にカウントダウン画面を表示せずメイン画面を表示します
即スキャン	起動時にカウントダウン画面は表示しないですぐにスキャンを開始します
タイマースキャン	指定時間にスキャンを開始します　タイマー設定で開始時刻を設定してください



■タイマースキャン　機能

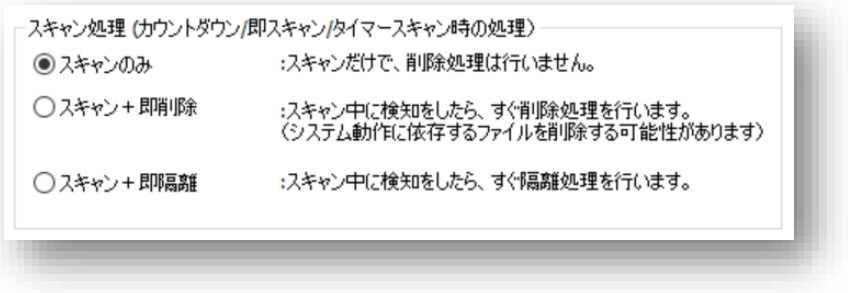
タイマースキャン機能は指定時間にウイルススキャンをする機能です。日時を設定し、ワクチン USB を PC に接続しておくと、指定日時にウイルススキャンを行います。日時の指定としては 「曜日(月～日)＋開始時刻」と最大 30 個の「指定日(YYYY/MM/DD)と開始時刻」があります。本機能を使用すると実施担当がいない時間にスキャンしたり、手間なく複数回ウイルススキャンすることができます。
設定はタイマースキャンを選択し、[タイマー設定]を選択してください。設定は以下の２つ可能です。

・指定した日時にスキャンする（最大３０個まで登録可能）
・毎週指定した曜日・時刻にスキャンする



■スキャン処理

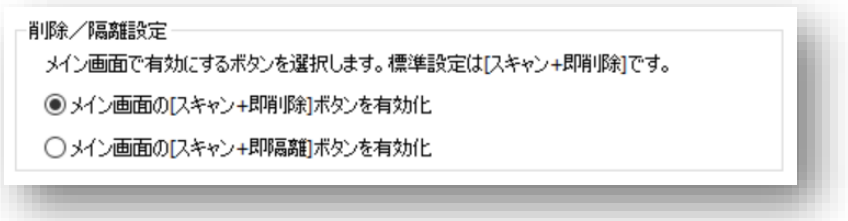
ワクチン USB のウイルススキャンのタイプを選択することができます。



項目	内容
スカキャンのみ	ウイルスを検知しても削除・隔離はしません。
スキャン＋即削除	ウイルスを検知次第、すぐに削除処理を行います。
スキャン＋即隔離	ウイルスを検知次第、すぐに隔離処理を行います。

■削除/隔離設定

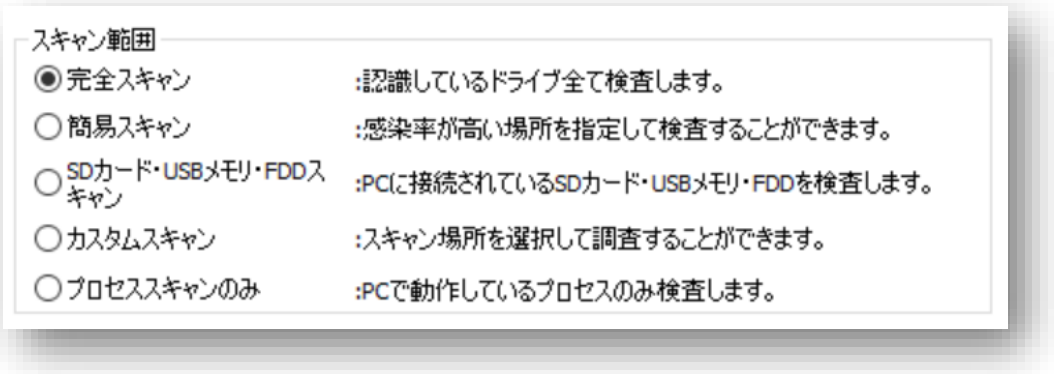
メイン画面で有効にするボタンを設定します。[スキャン＋即削除]、[スキャン+即隔離]のどちらかを選択できます。
同時に両ボタンを有効にすることはできません。



設定：スキャン設定１

■スキャンモード

ウイルススキャンを行う範囲を設定することができます。



項目	内容
完全スキャン	すべてのドライブをスキャンします（ネットワークドライブはスキャンしません）。 ※弊社推奨設定
簡易スキャン	感染率が高い範囲を限定してスキャンします。お時間がない場合ご使用ください。 ※1)、2)、3)、4）は、指定されたパス内の階層フォルダは検索しません)。 1) C:¥ 2) C:¥WINDOWS¥ 3) C:¥WINDOWS¥system¥ 4) C:¥WINDOWS¥system32¥ 5) C:¥Documents and Settings¥（※Vista 以降は C:¥Users¥となります）
SD カード・USB メモリ・FDD スキャン	PC に接続されている、SD カードなどのリムーバブルディスクと認識されるメモリ媒体をウイルススキャンします。
カスタムスキャン	ユーザー様が選択した場所をスキャンします。 スキャンする範囲は⑤スキャンリストで設定してください。
プロセススキャンのみ	PC で動作しているプロセスのみスキャンします。

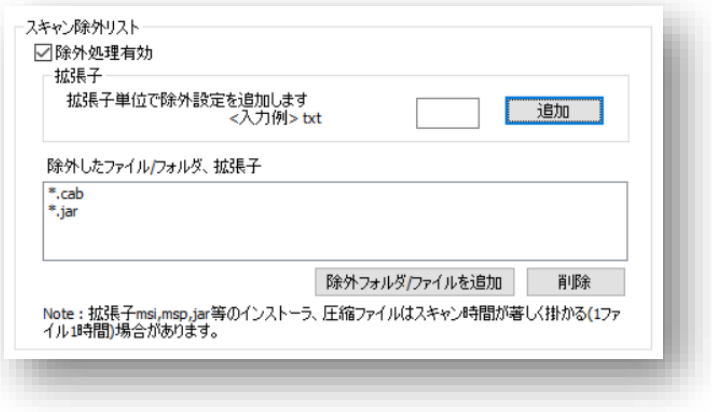
カスタムスキャンを選択した場合、スキャンする場所を設定することができます。

項目	内容
スキャンフォルダを追加	クリックするとフォルダ選択画面を表示します。スキャンするフォルダを選択してください。スキャンリストへ追加します。
削除	スキャンリストに追加したファルダを削除することができます。削除する項目を選択し、削除ボタンを押してください。

設定：スキャン設定２

■スキャン除外リスト

スキャンから外すフォルダ/ファイルとファイル拡張子を設定することができます。大文字小文字の区別は行いません。



項目	内容
除外処理有効ボタン	チェックをつけると、除外項目の追加が可能になります。
除外フォルダ/ファイルを追加ボタン	クリックするとフォルダ選択画面を表示します。スキャンを除外するフォルダ・ファイルを選択してください。除外リストへ追加します。
削除ボタン	スキャンの除外設定をしたファイル・ファルダ・拡張子を削除することができます。除外する項目を選択し、除外ボタンを押してください。
拡張子欄	スキャンを除外するファイル拡張子を追加することができます。 スキャン除外する拡張子を入力し、追加ボタンを押してください。 除外リストへ追加します。

■エンジンの切り替え

ウイルススキャンエンジンを切り替えることができます。

ウイルススキャンエンジンの切り替えは、ワクチン USB の次回起動時に反映されます。

項目	内容
5600 エンジンを使用する	WindowsXP で動作する 5600 エンジンを使用します。 注意事項： 5600 エンジンのサポートはマカフィー社のサポート終了と共に弊社サポートも終了しております。動作不備等一切サポートできませんので、ご了承願います。
**00 エンジンを使用する	**00 エンジン(最新エンジン)を使用します。

設定：定義ファイル

■定義ファイル更新方法

項目	内容
インターネットを使用して定義ファイルを更新します	インターネット経由で定義ファイルをダウンロードします。
インターネットと Local Updater で定義ファイルを更新します	インターネットと Local Updater で定義ファイルをダウンロードします。

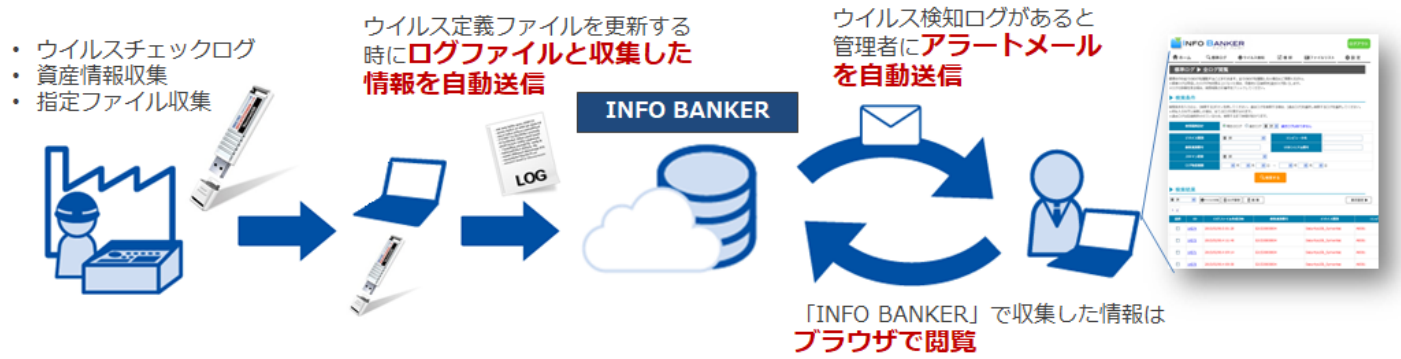
※Local Updater は定義ファイルを社内サーバーに一旦ダウンロードするためのサーバーソフトウェアです。
本ソフトウェアのダウンロードはこちら

設定：ログ

■製品管理サービス設定
InfoBankerCloud(別サービス)/InfoBanker(別売り) サービスへログ送信する機能の設定をすることができます

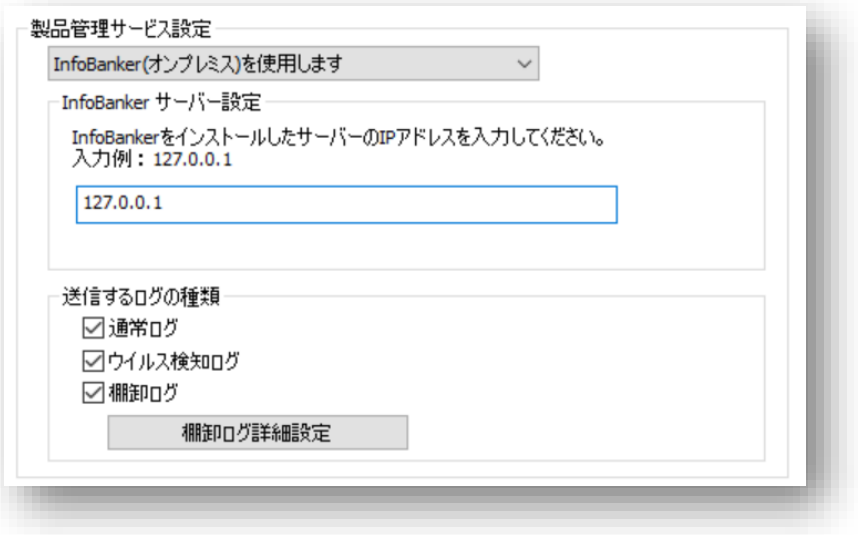
InfoBanker とは？
Info Banker は、ワクチン USB が取得したログをネットワーク経由で収集し、管理するサーバーソフトウェアです。
ログはデータベース化し管理され、ネットワークで接続されたクライアント(PC 等)からブラウザ経由で閲覧することができます。管理者様の負担を減らし、運用管理を容易にします。オンプレミス版とクラウド版をご用意しております。

またウイルス検知ログ(ログ内のスキャン結果：Virus Found)受信時に、指定のメールアドレスへ
通知メールを送ることができます。
管理者はウイルス有無を確認するために毎日 InfoBanker へログインする必要が無くなります。



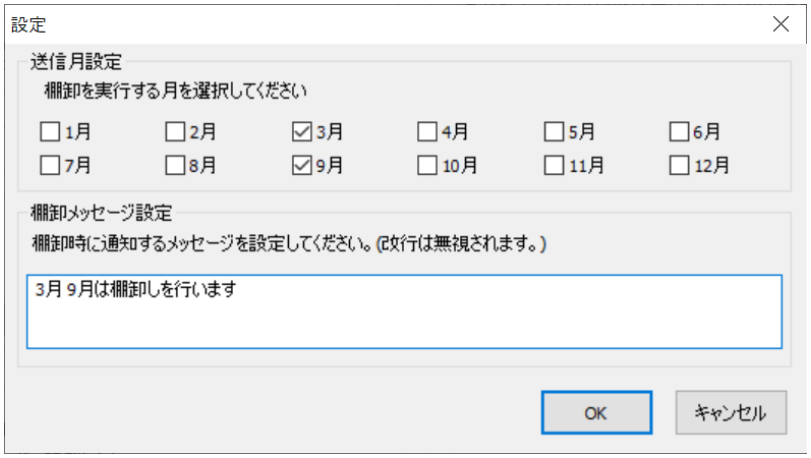
Info Banker オンプレミスについてはこちらをご確認ください
Info Banker クラウドについてはこちらをご確認ください

■InfoBanker(オンプレミス)設定
製品管理サービス設定で InfoBanker(オンプレミス)を選択してください。



項目	内容
InfoBanker サーバー設定	Info Banker をインストールした PC の IP アドレスを入力してください。

Info Banker への送信ログ設定

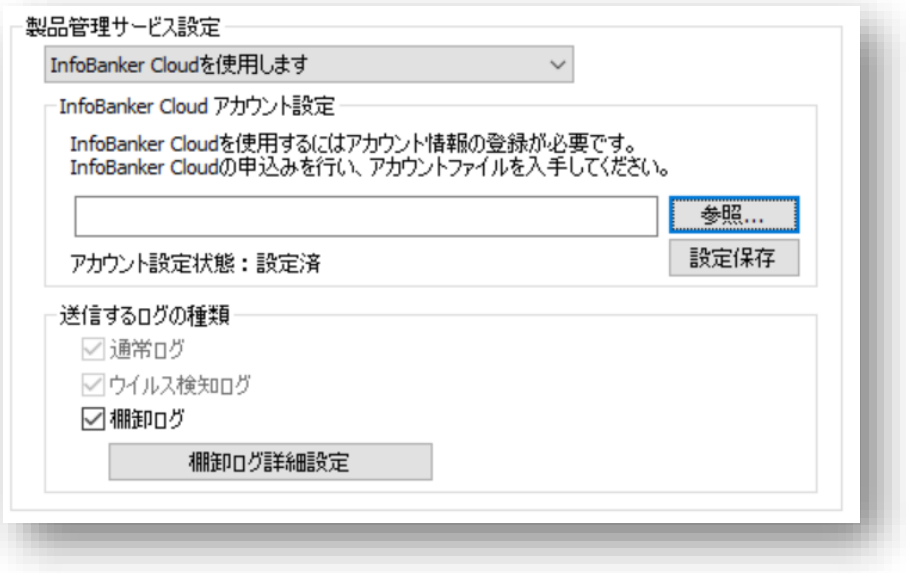
項目	内容
通通常ログ	ワクチン USB が毎回取得するログを送信します。
ウイルス検知ログ	ワクチン USB がウイルスを検知したログのみ送信します。
棚卸ログ	棚卸に使用するログを送信します。棚卸ログ詳細設定ボタンを押すと、棚卸を行う月、対象月にユーザーに表示するメッセージを設定できます。 

その他仕様

項目	内容
ログ送信タイミング	• ウイルス定義ファイル更新直後 • ウイルススキャン処理終了後 • メイン画面のツール→[管理サービスへログ送信]ボタンを押した時
ログの内容	InfoBanker の取扱説明書を御覧ください。
ログを送信した後について	InfoBanker へログファイルを送信後、送信に成功したログは削除されます。
InfoBanker 用ログの閲覧方法	ワクチン USB から閲覧することはできません。
ワクチン USB 内 の InfoBanker 用ログ削除方法	ワクチン USB のログ画面からログ[一括消去]を押してください。 ※通常のログも削除されるのでご注意ください。
ログ有無の確認方法	ワクチン USB のログ画面に下部に表示されます。

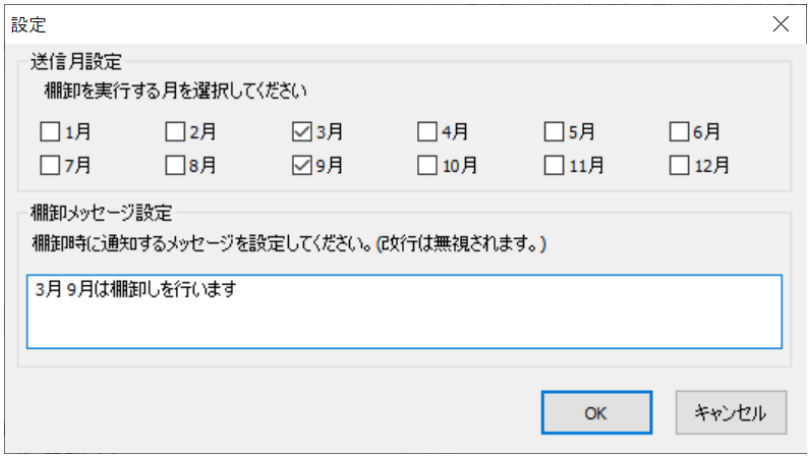
■InfoBanker Cloud 設定

製品管理サービス設定で InfoBanker Cloud を選択してください。



項目	内容
InfoBanker Cloud アカウント設定	InfoBanker Cloud 申込後に弊社から送付するアカウントファイルを[参照]ボタン選択し、インポートしてください。

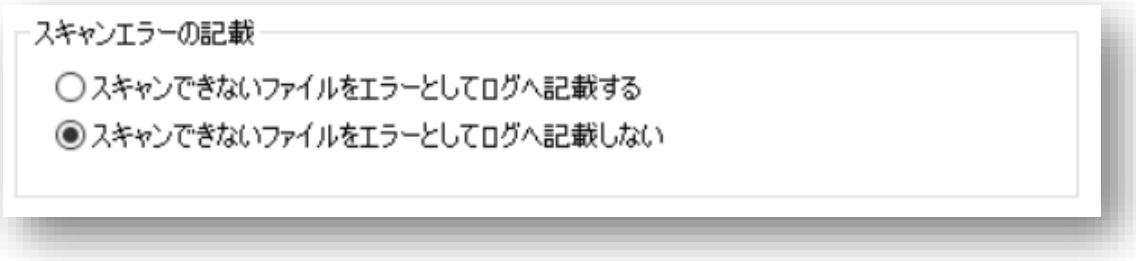
Info Banker への送信ログ設定

項目	内容
通通常ログ	ワクチン USB が毎回取得するログを送信します。標準で有効になっています。
ウイルス検知ログ	ワクチン USB がウイルスを検知したログのみ送信します。標準で有効になっています。
棚卸ログ	棚卸に使用するログを送信します。棚卸ログ詳細設定ボタンを押すと、棚卸を行う月、対象月にユーザーに表示するメッセージを設定できます。 

その他仕様

項目	内容
ログ送信タイミング	• ウイルス定義ファイル更新直後 • ウイルススキャン処理終了後 • メイン画面のツール→[管理サービスへログ送信]ボタンを押した時
ログの内容	InfoBanker の取扱説明書を御覧ください。
ログを送信した後について	InfoBanker へログファイルを送信後、送信に成功したログは削除されます。
InfoBanker 用ログの閲覧方法	ワクチン USB から閲覧することはできません。
ワクチン USB 内 の InfoBanker 用ログ削除方法	ワクチン USB のログ画面からログ[一括消去]を押してください。 ※通常のログも削除されるのでご注意ください。
ログ有無の確認方法	ワクチン USB のログ画面に下部に表示されます。

■スキャンエラーの記載
ワクチン USB3 はスキャンできないファイルがある場合、それをエラーログとして残します。
エラーをログへ記載するかを選択することができます。「記載しない」が推奨となります。



■資産情報管理
PC にインストールされているアプリケーション・WindowsOS の更新プログラムを取得し、ログに残す機能になります。

取得した場合、ログ内のセクション[Software]内に以下の情報が記載されます。

キー名	内容
Name****	アプリケーション名が入ります。例：Hagiwara Security Scan Plus
Publisher****	アプリケーションの会社名が入ります。例：Hagiwara Solutions.
Version****	アプリケーションのバージョン　例：2.50.25

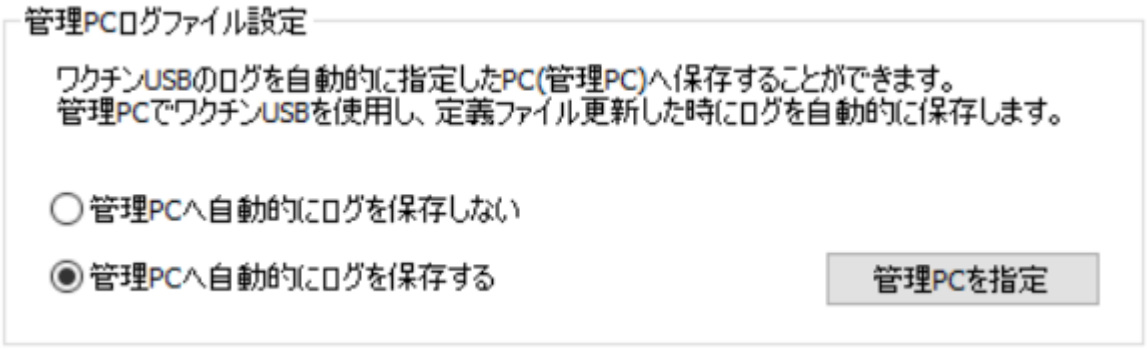
****には 0000-9999 が入ります。

またログ内のセクション[Hotfix]内に以下の情報が記載されます。

キー名	内容
KBName****	インストールされている更新プログラム名が入ります。。例：KB3035131
KBDate****	インストールされている更新プログラム名のインストール日が入ります。例：2015/4/14

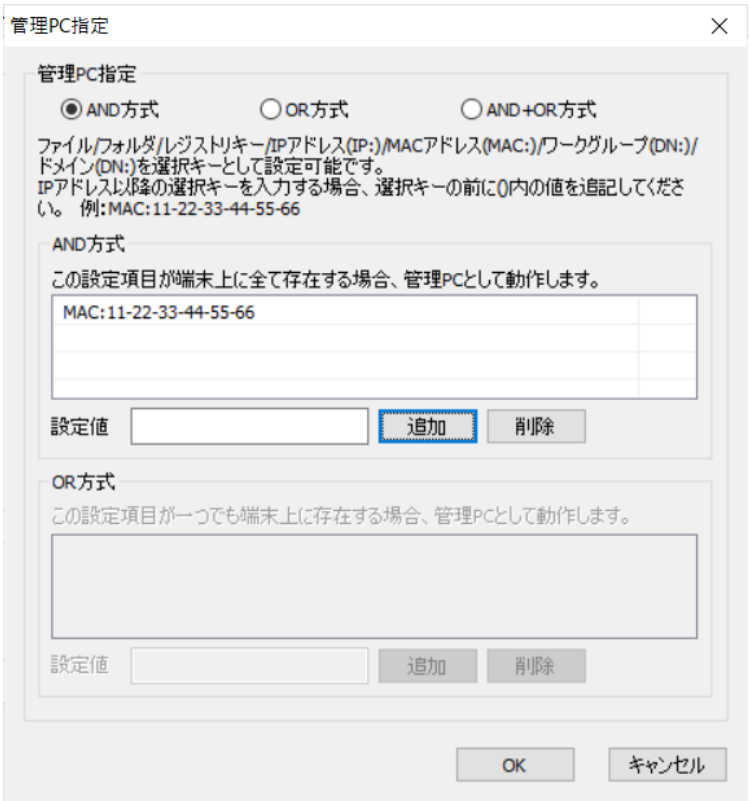
****には 0000-9999 が入ります。

■管理 PC ログファイル設定
お客様が指定した PC（管理 PC）へ自動的ログ保存を設定できます。
管理 PC 用ログ保存を作成すると、管理 PC へ接続した時に自動的に管理 PC へログファイルが保存されるため
ログを容易に管理することが可能になります。



項目	内容
管理 PC へ自動的にログを保存しない	管理 PC へ自動的にログを保存しない
管理 PC へ自動的にログを保存する	管理 PC へ自動的にログを保存します。管理 PC を設定する必要があります。 [管理 PC 指定]ボタンを押して設定してください。

管理 PC 指定 画面

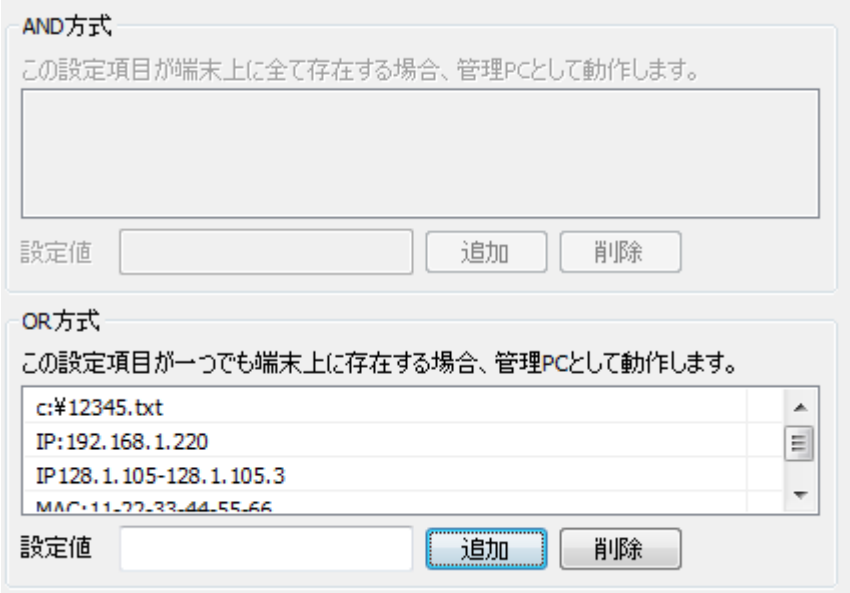


管理 PC 指定画面では管理 PC の条件を決定します。条件と一致した PC を管理 PC として動作します。
指定条件には以下の AND 方式、OR 方式、AND＋OR 方式があります。お客様の都合のよい方法を選択してください。

方式	[1]AND 方式	[2]OR 方式
内容	設定項目が”全て”PC に存在する場合に管理 PC として動作します。 例： 設定１：C:¥file1.bin・・・・ファイル 設定２：C:¥folder1・・・・フォルダ 設定３： HKEY_CURRENT_USER¥Software¥TEST¥TEST1・・・・レジストリキー PC 内に設定１，２，３”全て”存在する場合、セキュリティ USB が実行可能になります。	設定項目の中で１つでも該当設定が存在する場合に管理 PC として動作します。 例： 設定１：C:¥file2.bin・・・・ファイル 設定２：C:¥folder2・・・・フォルダ 設定３： HKEY_CURRENT_USER¥Software¥TEST¥TEST2・・・・レジストリキー PC 内に設定１，２，３の内、“最低一つ”存在する場合、セキュリティ USB が実行可能になります。
設定項目	最大 99 個	最大 99 個
使用用途	特定のファイル、フォルダ、レジストリキーなどを全 PC に設定できる場合。 例：全 PC をアクティブディレクトリで管理している、新規に PC を調達した場合など	PC 内のファイル、フォルダ、レジストリキー構成を変更できない、また共通のファイル等がない場合。 例：PC の回収が難しい場合など

AND＋OR 方式は AND 条件と OR 条件両方を満たす場合、管理 PC として動作する方式です。

方式を決定しましたら、認証キーを登録します。[設定値]欄へ認証キーを入力し、[追加]ボタンを押してください。
認証キーは最大 99 個まで登録可能です。
追加した条件を削除した場合は、項目を選択し、(削除する)ボタンを押してください。



管理 PC を特定する認証キーの設定

管理 PC を特定する認証キーとしては以下を設定することができます。
・ファイル/フォルダの有無
・レジストリキーの有無
・MAC アドレス
・IP アドレス
・ドメイン
・ワークグループ

認証条件(AND/OR)に合わせて、[設定値]枠へ認証値を入力し、[追加する]ボタンを押してください。画面上では最大 99 個まで登録可能です。

■ファイル/フォルダ設定

使用する PC 内に指定したファイル/フォルダが存在するかで判定します。

[設定例]
認証に使用するファイルを設定する場合、ファイル保存場所のフルパスを設定してください。

例；C:¥test¥test フォルダ下の test.bin ファイルを認証ファイルにする場合、設定項目へ
C:¥test¥test¥test.bin

[上級者向け設定]
環境設定を使用し、設定することができます。ユーザ名などフルパス内のフォルダに入っている場合等にご使用ください。

例：C:¥Documents and Settings¥user1¥test¥test.bin を設定する場合
※ PC のログインユーザによって user1 が user2 などに変わります。

設定例：%USERPROFILE%¥test¥test.bin

■レジストリキー設定

使用する PC 内に指定されたレジストリキーが存在するかで判定します。レジストリキーをルートからすべて設定してください。

[設定例]
例：HKEY_CURRENT_USER¥Software¥TEST¥TEST2

■MAC アドレス設定

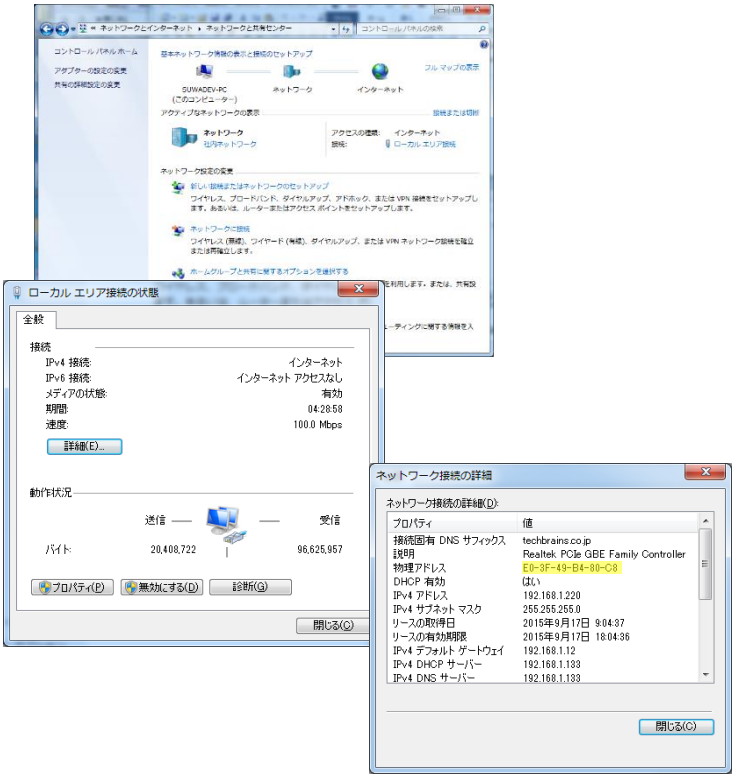
使用する PC の MAC アドレスが指定した MAC アドレスと一致するかで判定します。
MAC アドレスの先頭に ”MAC:”を付けて設定をしてください。

[設定例]

例 MAC:11-22-33-44-55-66

[PC の MAC アドレスの確認方法] ※例：Windows7

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→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン　物理アドレスとして表示されています。



■IP アドレス設定

使用する PC の IP アドレスが指定した IP アドレスと一致するかで判定します。
IP アドレスの先頭に ”IP:”を付けて設定をしてください。
IPv4 のみ対応しております。IPv6 には対応しておりません。

[設定例]

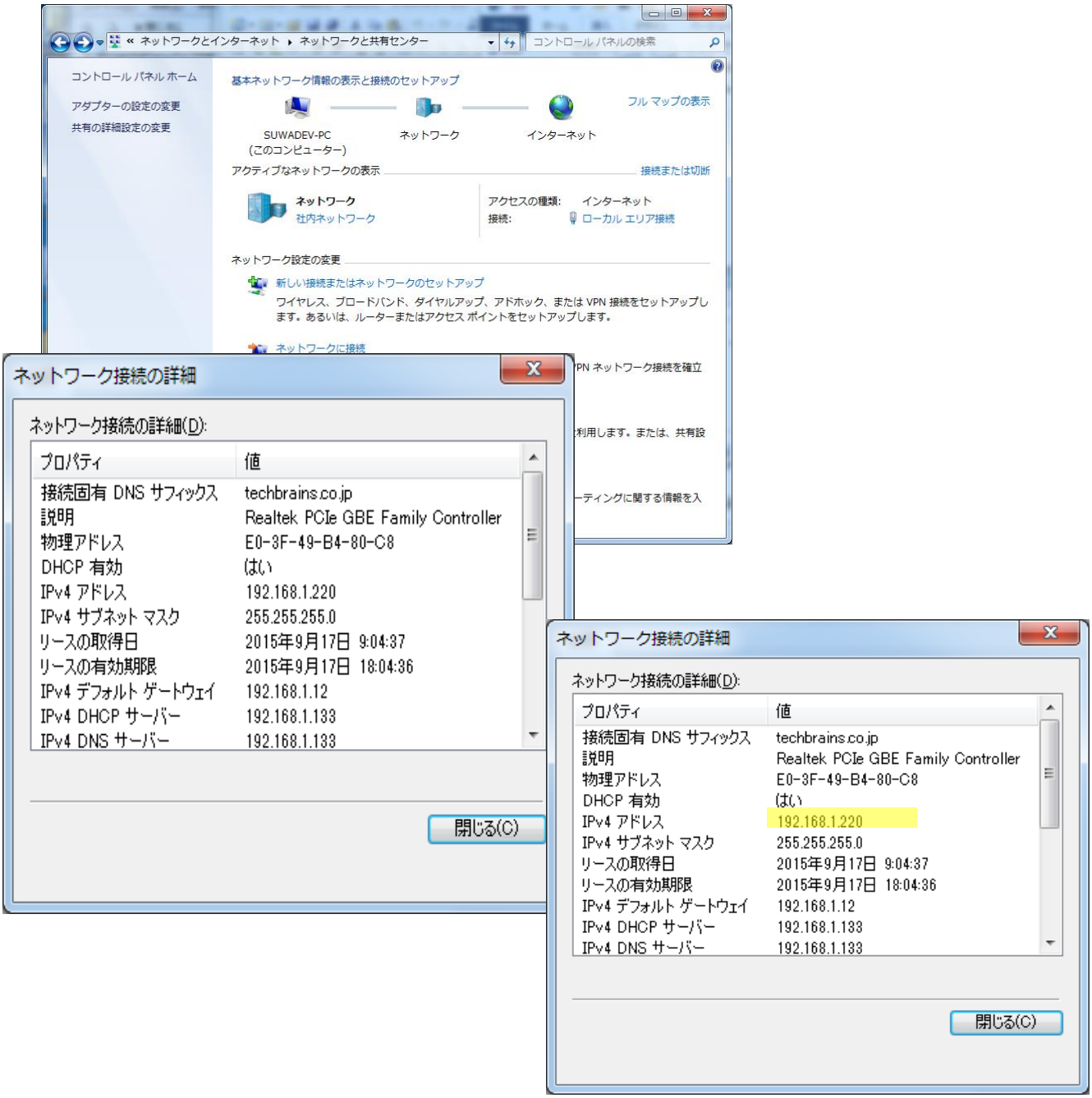
例 IP:192.168.1.220

範囲指定や、サブネットマスクでの設定も可能です。

- 範囲指定例：128.1.105.1-128.1.105.3　や 128.1.121.1-128.1.125.255
- サブネットマスク例：198.51.100.0/24

[PC の IP アドレスの確認方法]　※例：Windows7

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→アクティブなネットワークの表示からローカルエリア接続を選択→詳細ボタン　IPv4 アドレスとして表示されています。



■ドメイン設定

使用する PC のドメインが指定したドメインと一致するかで判定します。
ドメインの先頭に ”DN:”を付けて設定をしてください。

[設定例]

例 DN:hagisol.co.jp

[PC のドメインの確認方法] ※例：Windows7

コマンドプロンプトで、『nbtstat -n』と打ち込んで表示される、NetBIOS ローカルネームテーブルで、種類がグループとして表示されている行の名前の部分が、NetBIOS ドメイン名です。

■ワークグループ設定

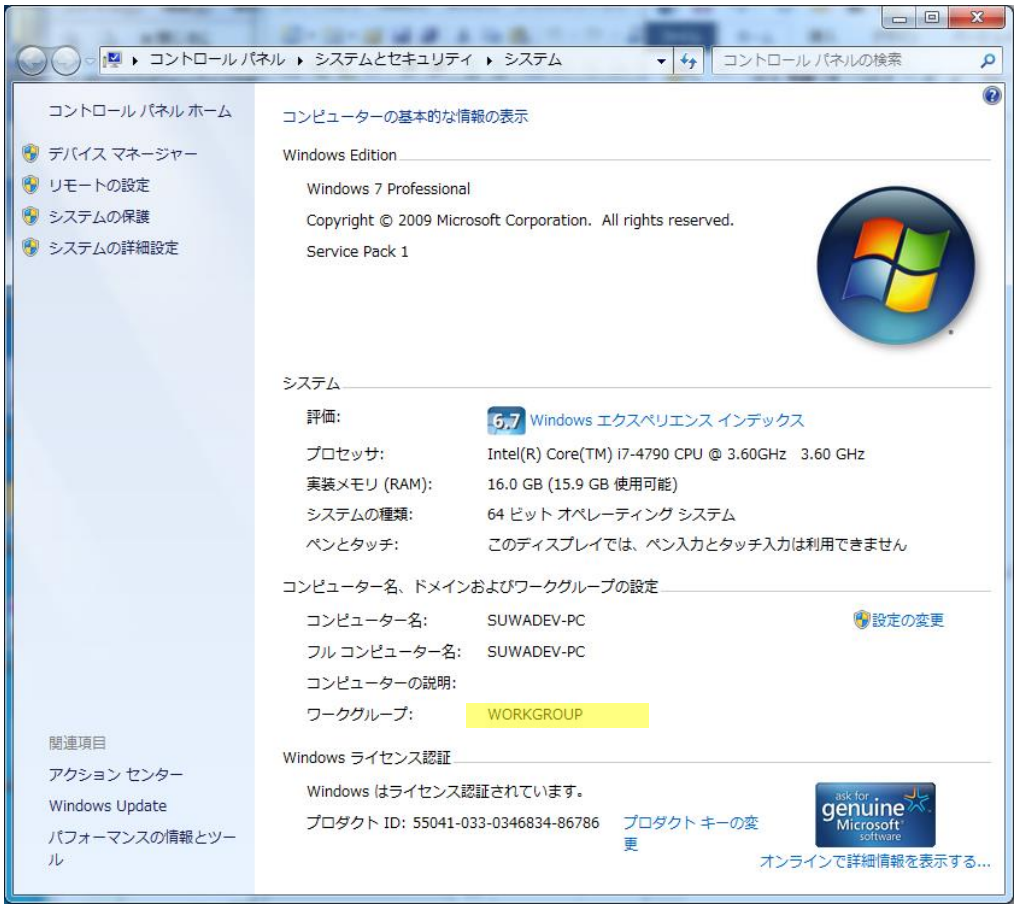
使用する PC のワークグループが指定したワークグループと一致するかで判定します。
ワークグループの先頭に ”DN:”を付けて設定をしてください。

[設定例]

例 DN:WORKGROUP

[PC のワークグループの確認方法] ※例：Windows7

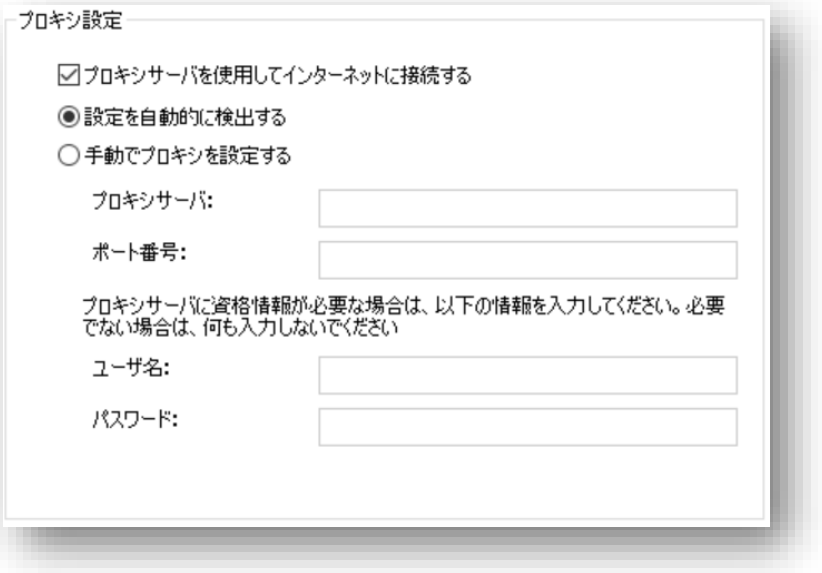
コントロールパネル→システムとセキュリティ→システムで表示されるワークグループ名



管理 PC を特定する認証キーについての説明は以上になります。

設定：通信設定(プロキシサーバー設定)

定義ファイル、ソフトウェア更新をプロキシサーバー経由で行う場合、本項目の設定を行ってください。

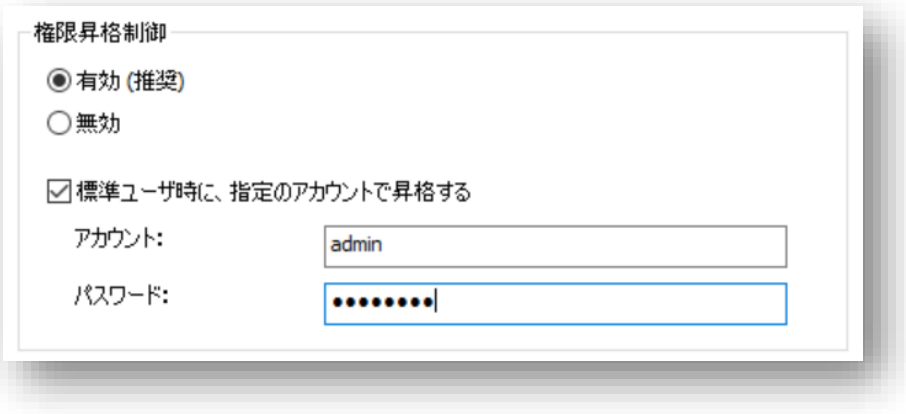


設定：権限昇格(画面表示から変更)

■権限昇格制御

ワクチン USB ソフトウェアを権限昇格して使用する際に使用します。
本機能を有効にした場合、ワクチン USB3 起動時に管理者権限昇格画面が表示されますので、必要に応じてアカウント ID とパスワードを入力してください。

また指定のアカウントとパスワードを登録することができ、登録時は管理者権限昇格画面に自動的にアカウント ID とパスワードが入力されます。
すでに OS にログインしているアカウントが管理者権限の場合、そのログインしているアカウントを使用し、
ワクチン USB ソフトウェアの権限昇格を行います。



項目	内容
有効	ワクチン USB 起動時にワクチン USB ソフトウェアの権限昇格を行います。 そのため起動時に権限昇格画面が表示されます。 権限昇格時に自動的にアカウント・パスワードを入力する場合、アカウントとパスワードを登録してください。
無効	ワクチン USB 起動時にワクチン USB ソフトウェアの権限昇格を行いません。

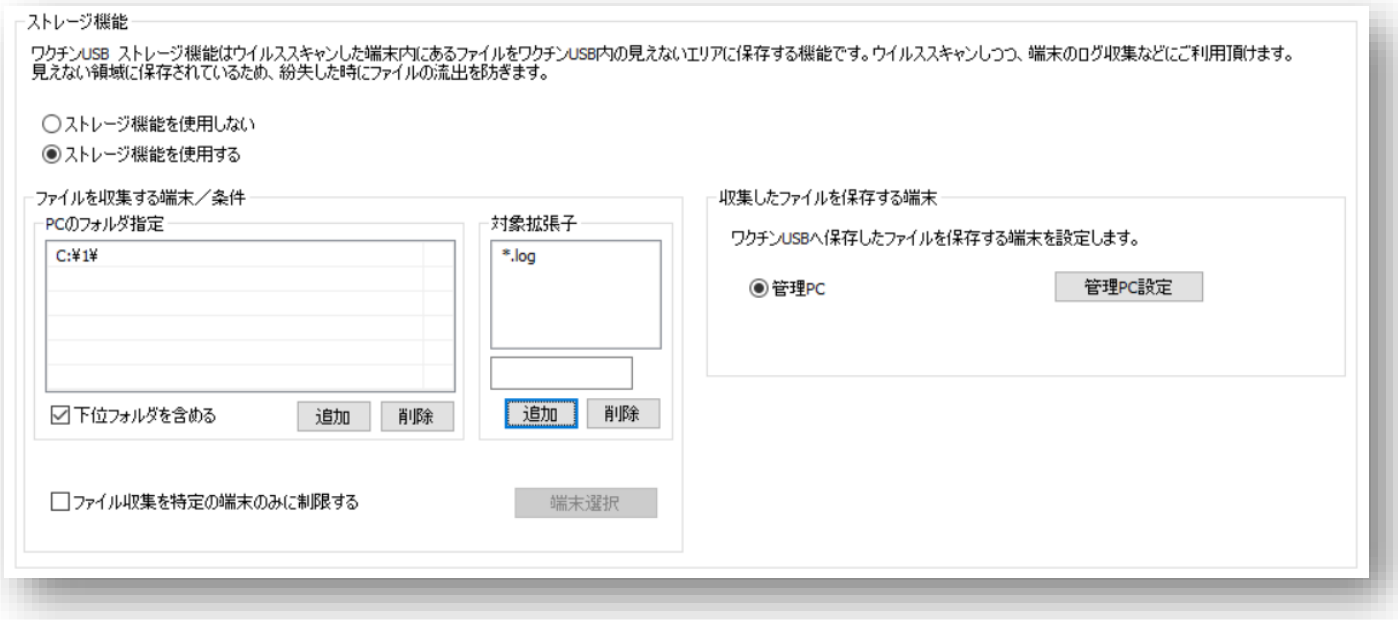
■画面の最前面表示

ワクチン USB のウインドウを最前面にするかどうかを設定できます。

項目	内容
通常表示する	Window 標準画面で表示します。他のソフトウェアをワクチン USB の画面上に被せることが可能です。
ワクチン USB ソフトウェア画面を常に最前面に表示します	常に最前面にワクチン USB の画面を表示します。

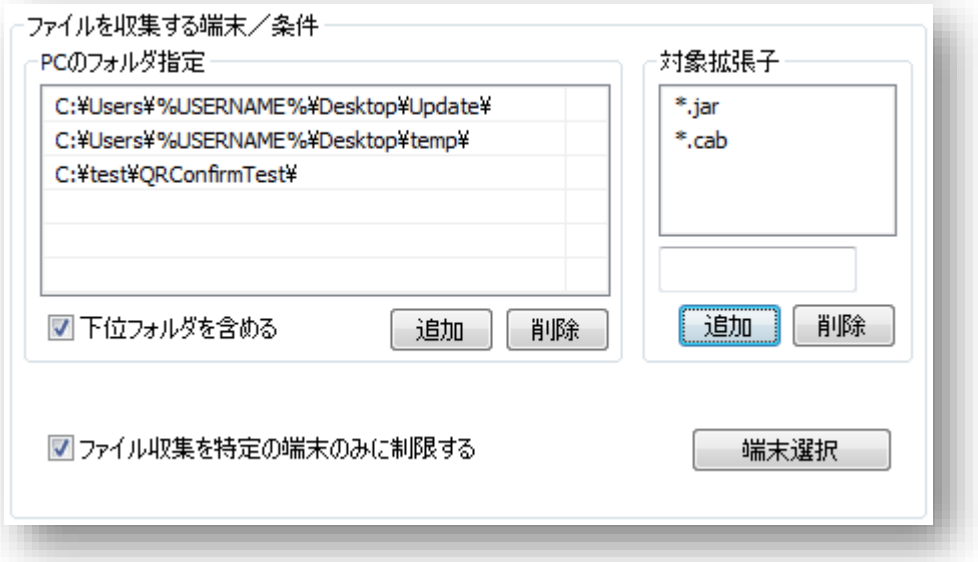
設定：ストレージ機能

ワクチン USB　ストレージ機能はウイルススキャンした端末内にあるファイルをワクチン USB 内の見えないエリアに保存する機能です。ウイルススキャンしつつ、端末のログ収集などにご利用頂けます。見えない領域に保存されているため、紛失した時に ファイルの流出を防ぎます。 最大 1GB までワクチン USB 内に保存することができます。
本機能を使用する場合、セキュリティ上、[設定の保護]をご利用し、設定変更を他者から守ることを推奨します。
設定の保護は設定画面の左下からボタンから行うことができます。



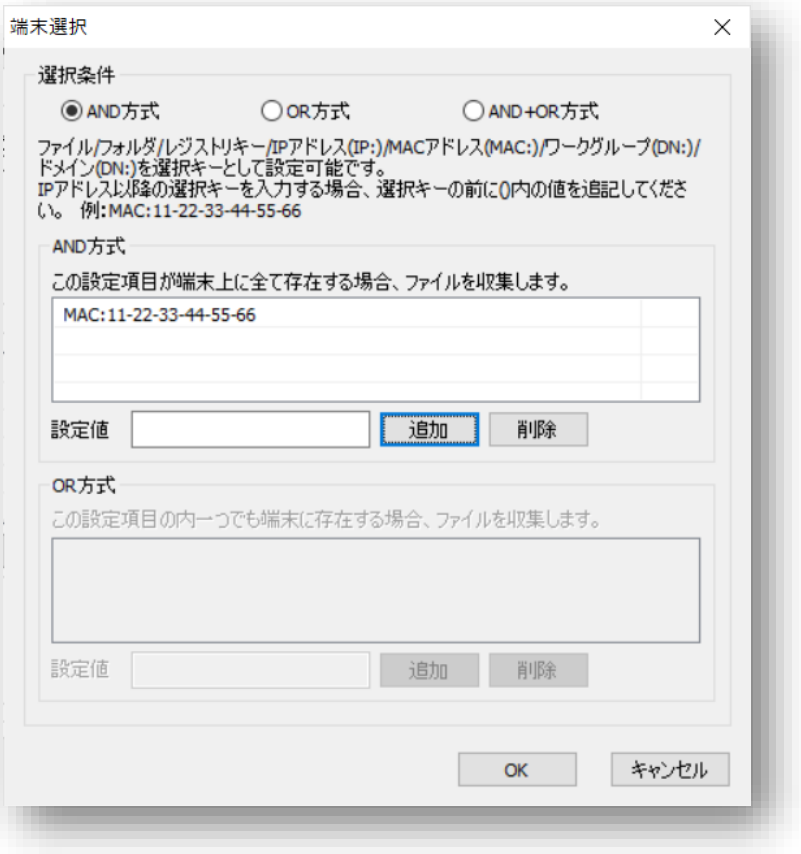
ストレージ機能を使用する場合、以下の２つの設定ができます。
・ファイルを収集する端末・条件
・収集したファイルを保存する端末

■ファイルを収集する端末・条件
ファイルを収集する端末と収集条件を設定できます。



項目	内容
PC のファルダ指定	取得するファイルがあるフォルダを設定できます。 フォルダ以下の下位フォルダも含めるかも選択できます。 また対象拡張子も設定でき、取得するファイルを制限することができます。
ファイル収集を特定の端末のみに制限する	ファイル収集する端末を制限することができます。 [端末選択]を押すと、取得する端末が設定できます。

■ファイルを収集する端末の選択
[端末選択]ボタンを押すと以下の画面が表示されます。条件が合う端末のみからファイルを収集します。
詳細設定は[管理 PC]設定と同一になりますので、詳細は本書の項：管理 PC ログファイル設定をご確認ください。

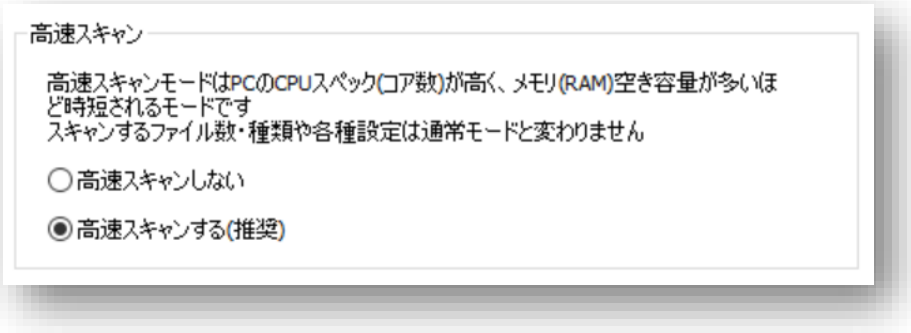


■収集したファイルを保存する端末
収集したファイルは指定した管理 PC 接続時に自動的にワクチン USB から管理 PC へ保存します。
管理 PC の設定方法については[こちら]をご確認ください。

設定：時短機能

■高速スキャン

高速スキャンモードはウイルススキャンを高速化し、スキャン時間を短縮することができるモードです。
詳細はこちらをご確認ください。



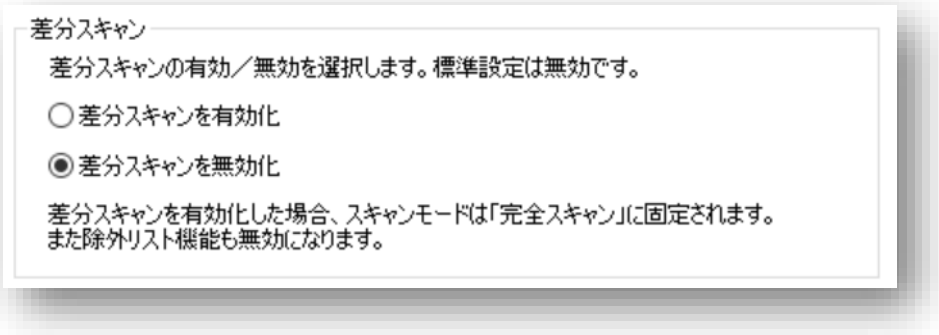
項目	内容
高速スキャンしない	高速スキャンしない
高速スキャンする(推奨)	高速スキャンをする

■圧縮ファイルスキャン設定

圧縮ファイルにたいしてのウイルススキャン設定を行うことができます。圧縮ファイル内のファイルが大量にある場合ウイルススキャンに非常に時間が掛かる場合あります。ウイルススキャンに時間が掛かる場合、本設定の変更を行ってください。

項目	内容
圧縮ファイルをウイルススキャンしない	圧縮ファイルをウイルススキャンしない
5 階層までウイルススキャンする	圧縮ファイルの 5 階層までにあるファイルをウイルススキャンする
300 階層までウイルススキャンする	圧縮ファイルの300 階層までにあるファイルをウイルススキャンする

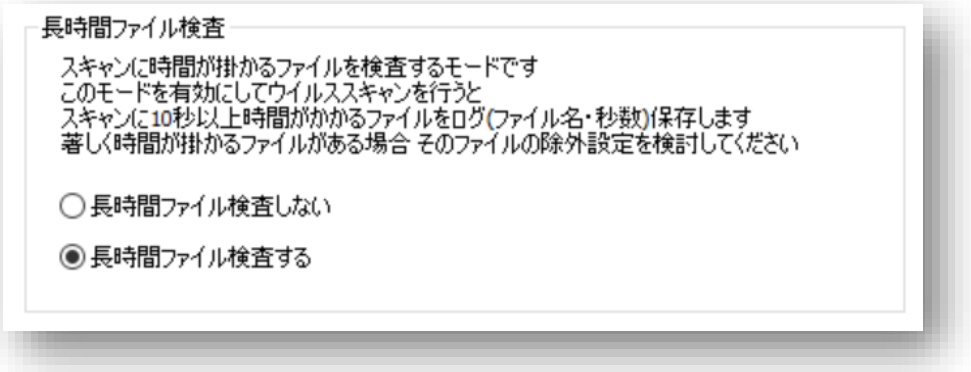
■差分スキャン
差分スキャン機能を設定します。差分スキャン機能については[こちら]をご確認ください。



項目	内容
差分スキャンを有効化	差分スキャン機能を有効にします。
差分スキャンを無効化	差分スキャン機能を無効にします。

■長時間ファイル検査

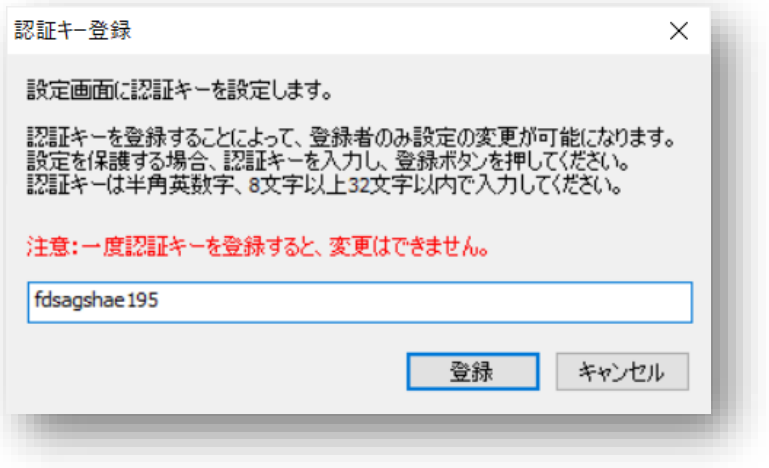
スキャン時に時間が掛かるファイルを見つけるモードです。長時間ファイル検査の詳細は[こちら]をご確認ください。



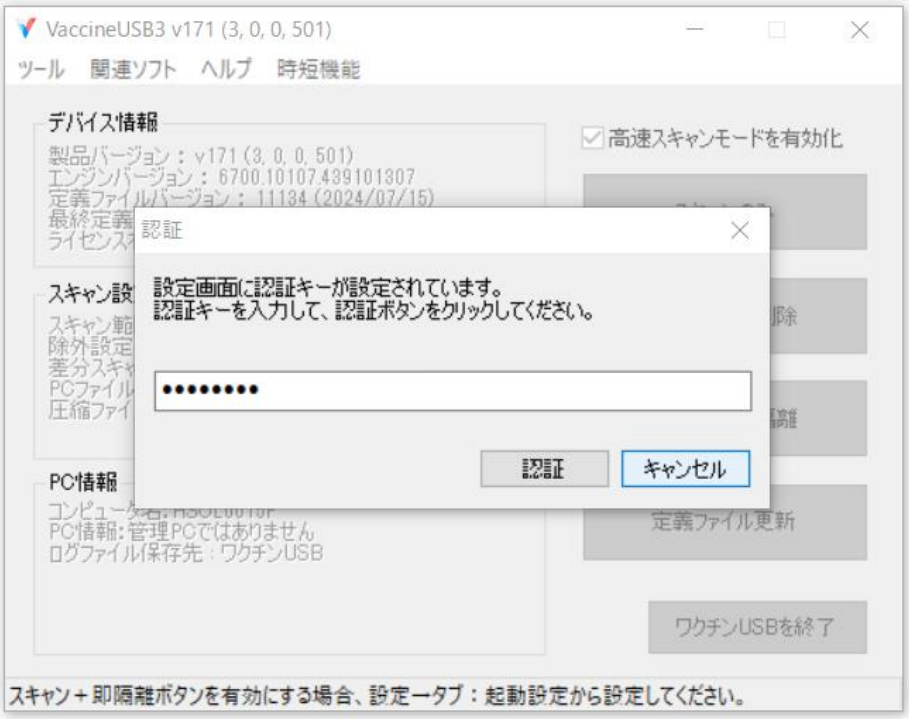
項目	内容
長時間ファイル検査しない	通常のウイルススキャンを行います
長時間ファイル検査する	スキャン時に時間が掛かるファイルを見つけるモードでウイルススキャンをおこないます。 ウイルススキャン終了時に 10 秒以上時間が掛かったファイルをログを保存します。

設定の保護

管理者以外の設定の変更を許可しない場合は、[設定の保護]ボタンを押して、認証キーを登録してください。
[設定の保護]ボタンを押すと、以下画面が表示されるので、認証キーを入力して、[登録]ボタンを押してください。
認証キーは一度登録すると変更できません。



認証キー登録後に設定を変更する際に、以下の画面が表示されます。登録した認証キーを入力してください。

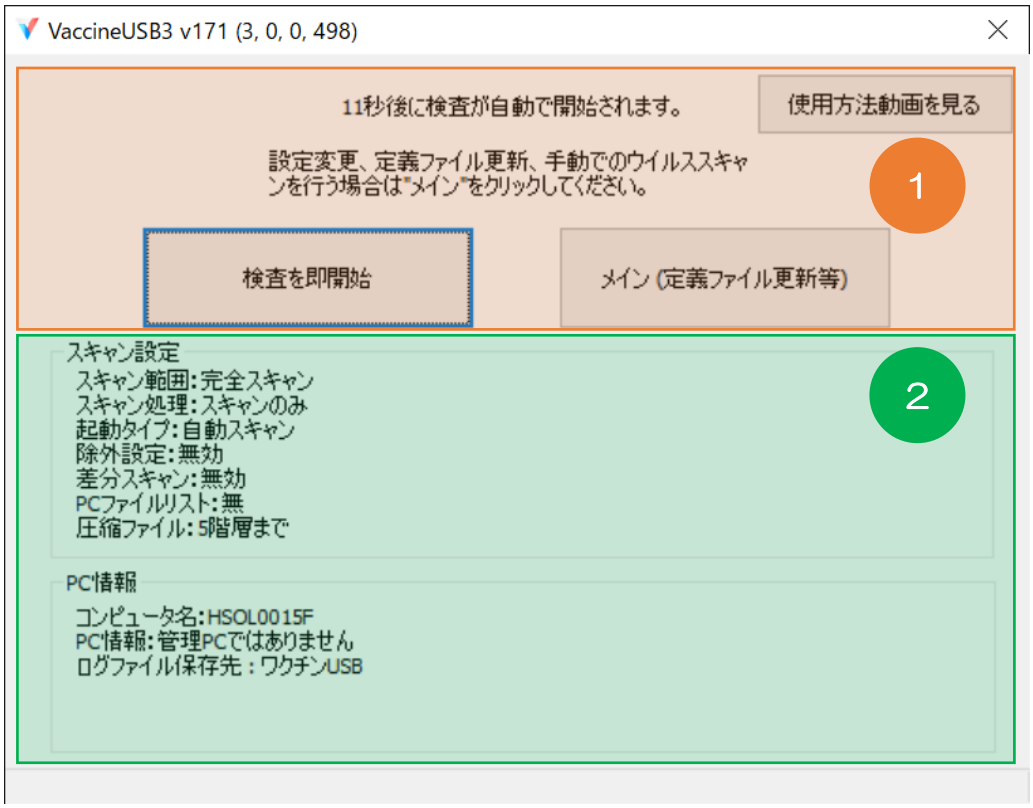


16 ソフトウェア画面の説明(起動・メイン・スキャン)

ワクチン USB で主な３つの画面(起動画面、メイン画面、スキャン画面)について説明します。

起動画面

ワクチン USB 起動時に表示される画面です。



1 カウントダウン表示とスキャンボタンです

ボタン	内容
検査を即開始	ウイルススキャンを開始します。設定はスキャン設定欄で確認できます。
メイン(定義ファイルを更新等)	メイン画面へ移動します。メイン画面ではウイルス定義ファイル更新、設定変更、ログ確認などが可能です。
使用方法動画を見る	ワクチン USB の基本的な使用方法についての動画をみることができます

2 ワクチン USB 状態・設定等を表示します。

■スキャン設定

項目	内容
スキャンモード	ウイルススキャン範囲を表示します。以下のモードがあります。 ・完全スキャン：すべてドライブをチェックします ・簡易スキャン：感染率が高い範囲を限定してスキャンします ・SD カード・USB メモリ・FDD スキャン：PC に接続されている、SD カードなどのリムーバブルディスクと認識されるメモリ媒体をウイルススキャンします。PC のウイルススキャンは一切行いません。 ・カスタムスキャン：ユーザーが決定した場所をスキャンします。 ・プロセススキャンのみ：PC で動作しているプロセスのみ検査します。
スキャンタイプ	ウイルススキャン動作を表示します。以下のモードがあります。 ・スキャンのみ：ウイルスの検知のみ行い、削除・隔離はしません。 ・スキャン＋即削除：ウイルスを検知次第、すぐに削除処理を行います。 ・スキャン＋即隔離：ウイルスを検知次第、すぐに隔離処理を行います。

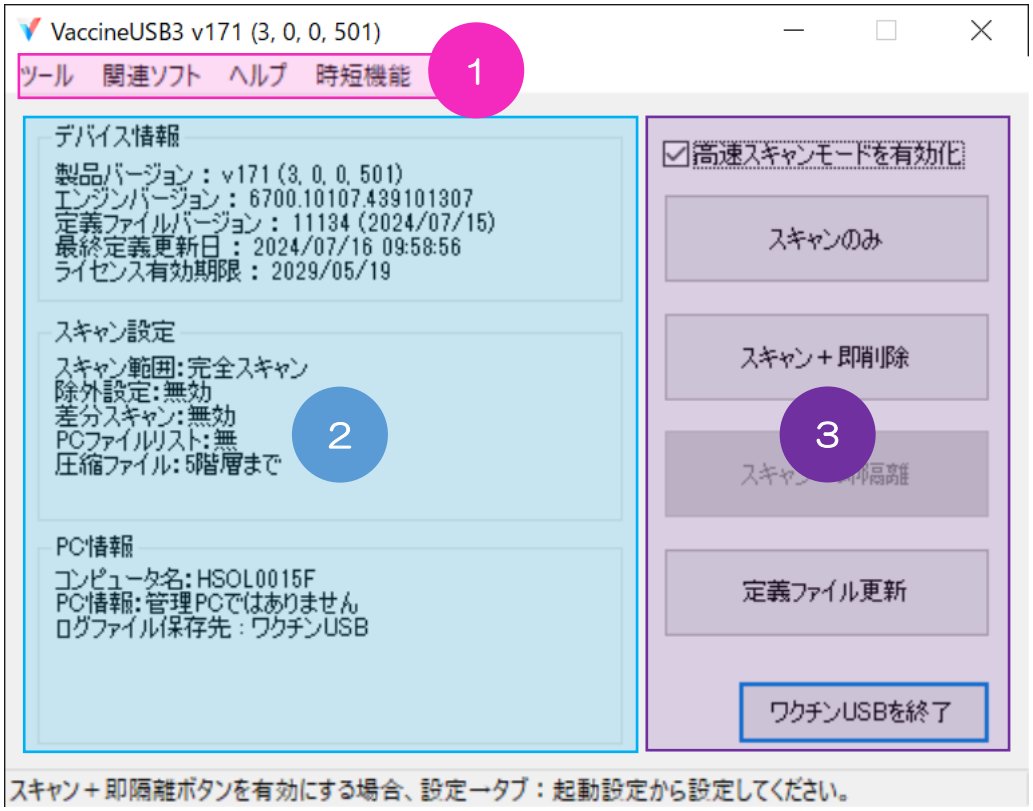
起動タイプ	ワクチン USB 起動時の動作を表示します。以下のモードがあります。 ・カウントダウン：起動時に約 15 秒の起動画面を表示します。「自動スキャン」と表示されます。 ・メイン画面表示：起動時に起動画面を表示せず、メイン画面を表示します。 ・即スキャン：起動時に起動画面は表示せず、すぐにスキャンを開始します
除外設定	ウイルススキャンを行わないフォルダ、拡張子の有無を表示します。 ・有効：除外するフォルダ、拡張子があります。 ・無効：除外するフォルダ、拡張子がありません。
差分スキャン	差分スキャン設定を表示します。 ・有効：差分スキャン設定が有効。 ・無効：差分スキャン設定が無効。 ※差分スキャンが有効でも PC ファイルリストが無い場合、差分ファイルスキャンは動作しません。スキャン後に PC ファイルリストが作成され、次回以降差分ファイルスキャンが動作致します。
PC ファイルリスト	差分スキャン有効時に使用する PC ファイルリストの有無を表示します。 ・有：現在接続されている PC の PC ファイルリストが有る ・無：現在接続されている PC の PC ファイルリストが無い
圧縮ファイル	圧縮ファイルへのスキャン設定を表示します ・スキャンしない ・5 階層まで ・300 階層まで

PC 情報

項目	内容
コンピュータ名	PC のコンピュータ名が表示されます。
PC 情報	管理 PC かどうかを判断します。 ・管理 PC です：接続 PC は管理 PC に設定されています。 ・管理 PC ではありません：接続 PC は管理 PC に設定されていません。
ログファイル保存先	ログ保存場所を表示します。 ・ワクチン USB：ワクチン USB 内へログを保存します。 ・使用中の PC：ワクチン USB 内へログを保存できない場合、PC へログを保存します。
PC へのログファイル保存場所 ※非表示の場合あり	ワクチン USB へのログが保存できない時に PC へログを保存します。 その保存場所を表示します。 例；C:¥Documents and Settings¥user¥My Documents¥VaccineUSB ※ログファイルがワクチン USB へ保存できる場合、本項目は表示されません。
PC 内のログファイルの有無 ※非表示の場合あり	使用中の PC にワクチン USB のログが存在するかを表示します。 ・ログファイルあり：PC 内にワクチン USB のログが保存されています。 ・ログファイルなし：PC 内にワクチン USB のログは保存されていません。 ※ログファイルがワクチン USB へ保存できる場合、本項目は表示されません。

メイン画面

起動画面で[メイン]ボタンを押した時に表示される画面です。



1 各種メニューです

2 ワクチン USB 状態・設定等を表示します。

■デバイス情報

項目	内容
製品バージョン	ワクチン USB の製品バージョンを表示します。
エンジンバージョン	ウイルススキャンエンジンのバージョンを表示します。
定義ファイルバージョン	ウイルス定義ファイルバージョンを表示します。
最終定義更新日	最後にウイルス定義ファイルを更新した日を表示します。
ライセンス有効期間	ライセンスの有効期間を表示します。

■スキャン設定

項目	内容
スキャン範囲	ウイルススキャン範囲を表示します。以下の 5 つのモードがあります。 ・完全スキャン：すべてドライブをチェックします ・簡易スキャン：感染率が高い範囲を限定してスキャンします ・SD カード・USB メモリ・FDD スキャン：PC に接続されている、SD カードなどのリムーバブルディスクと認識されるメモリ媒体をウイルススキャンします。PC のウイルススキャンは一切行いません。 ・カスタムスキャン：ユーザーが決定した場所をスキャンします。 ・プロセススキャンのみ：PC で動作しているプロセスのみ検査します。
除外設定	ウイルススキャンを行わないフォルダ、拡張子の有無を表示します。 ・有効：除外するフォルダ、拡張子があります。 ・無効：除外するフォルダ、拡張子がありません。
差分スキャン	差分スキャン設定を表示します。

	有効：差分スキャン設定が有効。 無効：差分スキャン設定が無効。 ※差分スキャンが有効でも PC ファイルリストが無い場合、差分ファイルスキャンは動作しません。スキャン後に PC ファイルリストが作成され、次回以降差分ファイルスキャンが動作致します。
PC ファイルリスト	差分スキャン有効時に使用する PC ファイルリストの有無を表示します。 有：現在接続されている PC の PC ファイルリストが有る 無：現在接続されている PC の PC ファイルリストが無い
圧縮ファイル	圧縮ファイルへのスキャン設定を表示します ・スキャンしない ・5 階層まで ・300 階層まで

スキャン設定を変更する場合、メイン画面へ移動し、ツールバーから設定を選択してください。

■PC 情報

項目	内容
コンピュータ名	PC のコンピュータ名を表示します。
PC 情報	管理 PC かどうかを判断します。 ・管理 PC です：接続 PC は管理 PC に設定されています。 ・管理 PC ではありません：接続 PC は管理 PC に設定されていません。
ログファイル保存先	ログ保存場所を表示します。 ・ワクチン USB：ワクチン USB 内へログを保存します。 ・使用中の PC：ワクチン USB 内へログを保存できない場合、PC へログを保存します。
PC へのログファイル保存場所 ※非表示の場合あり	ワクチン USB へのログが保存できない時に PC へログを保存します。その保存場所を表示します。 例；C:¥Documents and Settings¥user¥My Documents¥VaccineUSB ※ログファイルがワクチン USB へ保存できる場合、本項目は表示されません。
PC 内のログファイルの有無 ※非表示の場合あり	使用中の PC にワクチン USB のログが存在するかを表示します。 ・ログファイルあり：PC 内にワクチン USB のログが保存されています。 ・ログファイルなし：PC 内にワクチン USB のログは保存されていません。 ※ログファイルがワクチン USB へ保存できる場合、本項目は表示されません

3 スキャンの実施ボタン・設定です

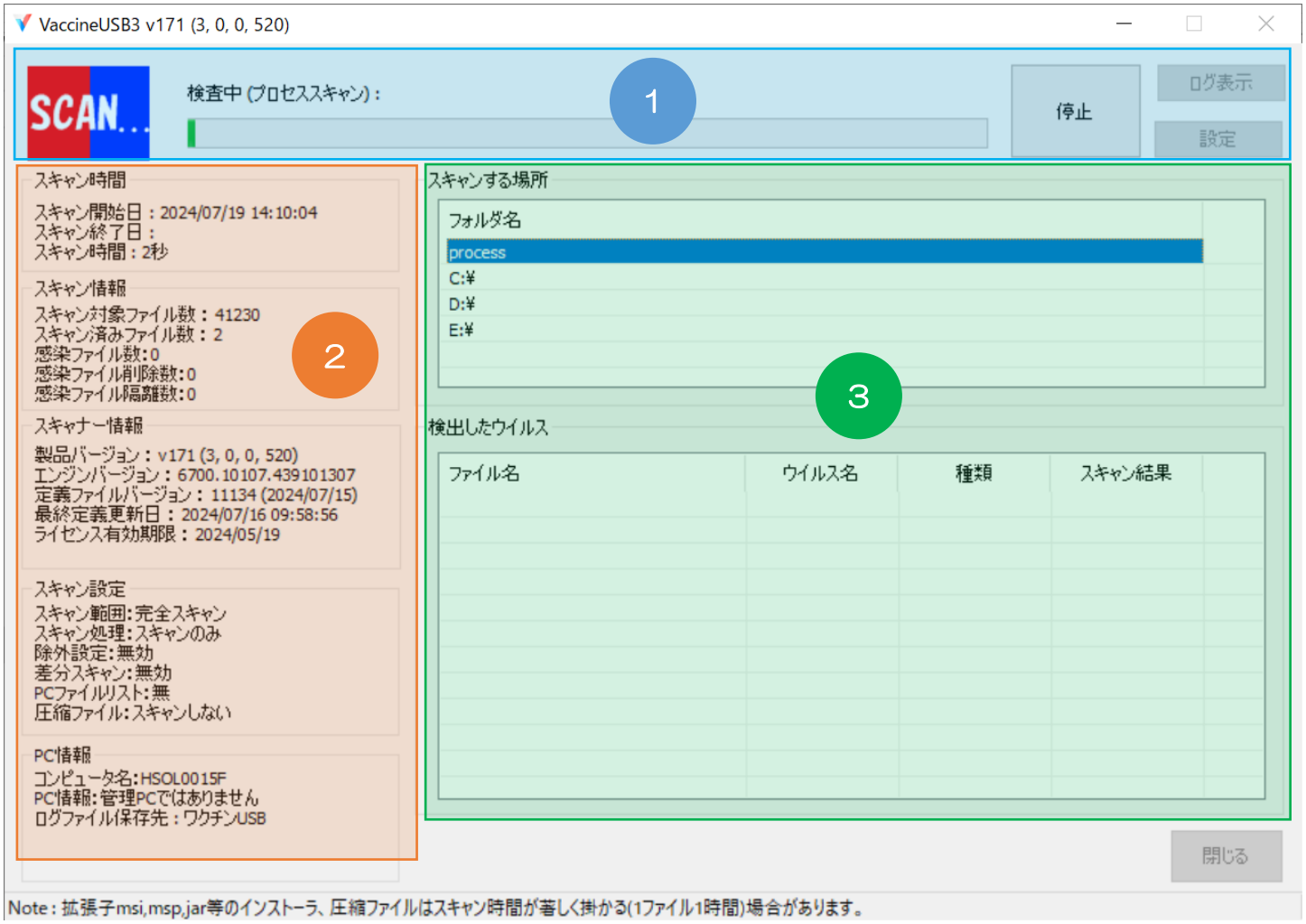
ボタン・チェック	内容
スキャンのみ	PC のウイルススキャンを行います。ウイルスの検知のみ行い、削除はしません。
スキャン＋即削除	PC のウイルススキャンを行います。ウイルスを検知次第、削除処理を行います。
スキャン＋即隔離	PC のウイルススキャンを行います。ウイルスを検知次第、隔離処理を行います。 ※設定→タブ：削除/隔離設定でボタンを有効にすることができます。
定義ファイル更新	ウイルス定義ファイル更新を行います。
高速スキャンモードを有効化	チェックを入れると高速スキャンモードで動作します。高速スキャンモードは CPU、メモリをより多く使用しますが、通常のスキャンよりスキャン時間を短縮することができます。
圧縮ファイルをスキャンしない	チェックを入れると圧縮ファイルをスキャン対象か外します。 スキャン時間を短縮する必要がある場合、ご利用検討してください。
ワクチン USB を終了	ワクチン USB を終了します。

スキャン画面

ウイルススキャン中に表示される画面です。ウイルススキャン画面は画面解像度によって画面が切り替わります。

800x600 より上の画面解像度の PC	通常のウイルススキャン画面
800x600～640x480 の画面解像度の PC	タッチパッドに最適化した画面

■通常のウイルススキャン画面



1 スキャンの進捗、結果を表示します。

※ウイルス隔離に成功している場合も「ウイルス存在しない場合」の表示がされます。

2 スキャンの進捗、ワクチン USB 状態・設定を表示します。

■スキャン時間：スキャンの進捗状況を表示します。

項目	内容
スキャン開始日時	ウイルススキャンを開始した日時を表示します。
スキャン終了日時	ウイルススキャンを終了した日時を表示します。
スキャン時間	ウイルススキャンの実行時間を表示します。

■スキャン情報：スキャンの進捗状況を表示します。

項目	内容
スキャン対象ファイル数	PC 内のウイルススキャンを行う総ファイル数です。
スキャン済みファイル数	ウイルススキャンが終了したファイル数です。
感染ファイル数	ウイルス感染しているファイル数です。
感染ファイル削除数	ウイルス感染しているファイルを削除した数です。
感染ファイル隔離数	ウイルス感染しているファイルを隔離した数です。

■スキャナー情報：ワクチン USB の状態・設定を表示します。

項目	内容
製品バージョン	ワクチン USB の製品バージョンを表示します。
エンジンバージョン	ウイルススキャンエンジンのバージョンを表示します。
定義ファイルバージョン	ウイルス定義ファイルバージョンを表示します。
最終定義更新日	最後にウイルス定義ファイルを更新した日を表示します。
ライセンス有効期間	ライセンスの有効期間を表示します。

■スキャン設定：ワクチン USB のスキャン設定を表示します。

項目	内容
スキャンモード	ウイルススキャン範囲を表示します。以下の 4 つのモードがあります。 ・完全スキャン：すべてドライブをチェックします ・簡易スキャン：感染率が高い下記のパスをスキャンします ・SD カード・USB メモリ・FDD スキャン：PC に接続されている、SD カードなどのリムーバブルディスクと認識されるメモリ媒体をウイルススキャンします。PC のウイルススキャンは一切行いません。 ・カスタムスキャン：ユーザーが決定した場所をスキャンします。
スキャンタイプ	ウイルススキャン動作を表示します。以下の 3 つのモードがあります。 ・スキャンのみ：ウイルスの検知のみ行い、削除はしません。 ・スキャン＋即削除：ウイルスを検知次第、すぐに削除処理を行います。 ・スキャン＋即隔離：ウイルスを検知次第、すぐに隔離処理を行います。
起動タイプ	ワクチン USB 起動時の動作を表示します。以下の 3 つのモードがあります。 ・カウントダウン：起動時に約 15 秒の起動画面を表示します。 ・メイン画面表示：起動時に起動画面を表示せず、メイン画面を表示します。 ・即スキャン：起動時に起動画面は表示せず、すぐにスキャンを開始します
除外設定	ウイルススキャンを行わないフォルダ、拡張子の有無を表示します。 ・有効：除外するフォルダ、拡張子があります。 ・無効：除外するフォルダ、拡張子がありません。
差分スキャン	差分スキャン設定を表示します。 有効：差分スキャン設定が有効。 無効：差分スキャン設定が無効。 ※差分スキャンが有効でも PC ファイルリストが無い場合、差分ファイルスキャンは動作しません。スキャン後に PC ファイルリストが作成され、次回以降差分ファイルスキャンが動作致します。
PC ファイルリスト	差分スキャン有効時に使用する PC ファイルリストの有無を表示します。 有：現在接続されている PC の PC ファイルリストが有る 無：現在接続されている PC の PC ファイルリストが無い
圧縮ファイル	圧縮ファイルへのスキャン設定を表示します ・スキャンしない ・5 階層まで ・300 階層まで

■PC 情報

項目	内容
コンピュータ名	PC のコンピュータ名を表示します。
PC 情報	管理 PC かどうかを判断します。 • 管理 PC です：接続 PC は管理 PC に設定されています。 • 管理 PC ではありません：接続 PC は管理 PC に設定されていません。
ログファイル保存先	ログ保存場所を表示します。 • ワクチン USB：ワクチン USB 内へログを保存します。 • 使用中の PC：ワクチン USB 内へログを保存できない場合、PC へログを保存します。
PC 内のログファイルの有無	使用中の PC にワクチン USB のログが存在するかを表示します。 • ログファイルあり：PC 内にワクチン USB のログが保存されています。 • ログファイルなし：PC 内にワクチン USB のログは保存されていません。 ※ログファイルがワクチン USB へ保存できる場合、本項目は表示されません。

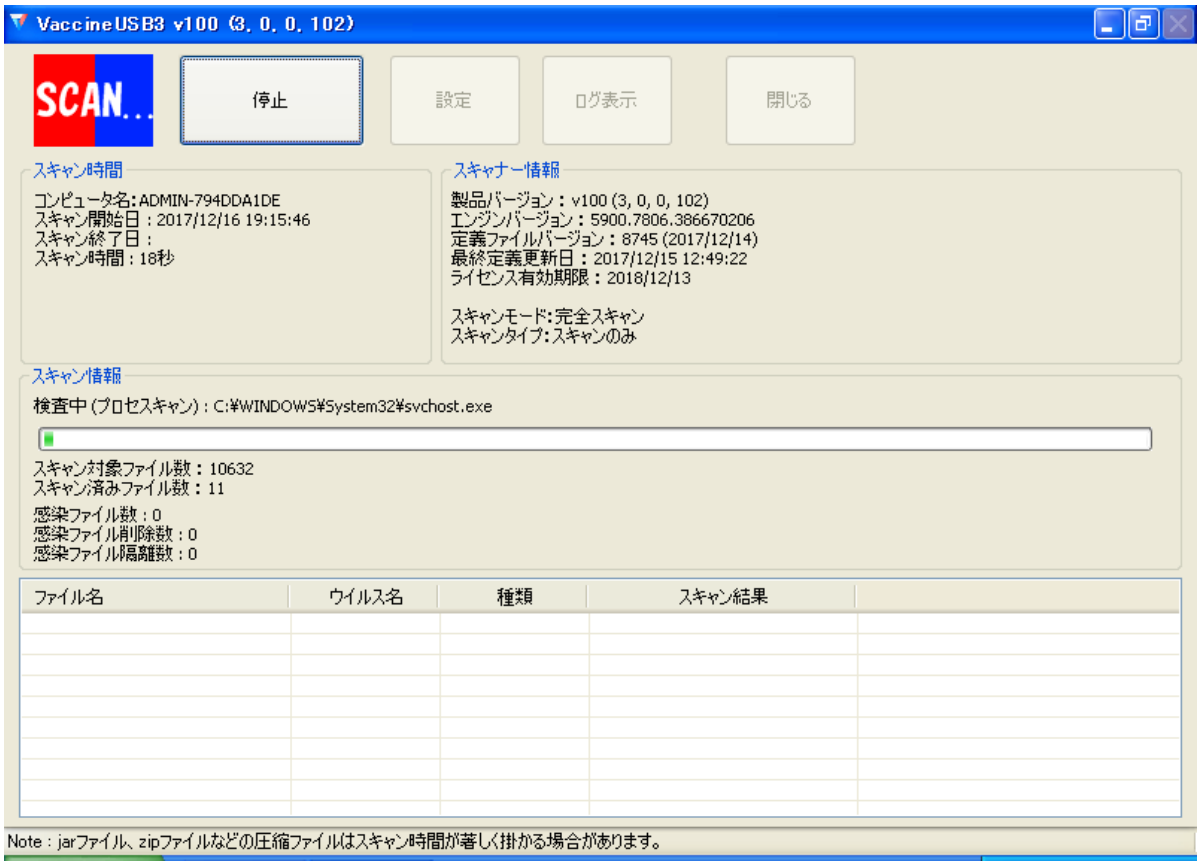
3 スキャンする場所と検出したウイルス情報を表示します。

■スキャンする場所：ウイルススキャンする場所を表示します。
■検出したウイルス：検出したウイルス情報を表示します。

項目	内容
ファイル名	ウイルスの見つかった場所(ファイルパス)を表示します。
ウイルス名	Trellix 社(旧マカフィ社)が規定したウイルス名が表示されます
種類	Trellix 社(旧マカフィ社)が規定したウイルスの種類が表示されます。
スキャン結果	見つかったウイルスへの処理結果を表示します。 ウイルスを発見しました：ウイルスを発見のみしました。ウイルスは削除・隔離しておりません。 ウイルスを削除しました：ウイルスの削除に成功しました。 ウイルスを隔離しました：ウイルスの隔離に成功しました。 ウイルスの削除に失敗しました：ウイルスの削除に失敗しました。 ウイルスの隔離に失敗しました：ウイルスの隔離に失敗しました。

タッチパッドに最適化した画面

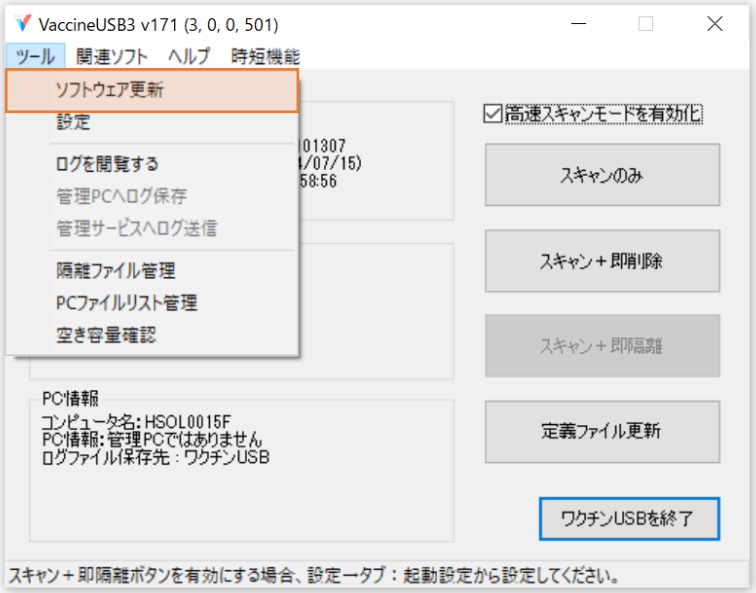
800x600～640x480 の画面解像度の PC で使用した場合、自動的に以下の画面に切り替わります。
※設定画面は 800x600 より上の画面解像度の PC で使用してください。



17 その他の機能

ソフトウェアを更新する

ウイルススキャンソフトの更新は、[ツール]メニューの[ソフトウェア更新]で行うことができます。更新情報があった場合は、ソフトウェアの更新を行なってください。またはこちらからアップデートソフトをダウンロードしてください。



製品の初期化を行う

何かしらの原因でワクチン USB が正常に動作しなくなった場合、初期化を行なってください。

初期化用のソフトウェアはこちらからダウンロードしてください。

注意：初期化を行うとログ,設定が削除されます。

ワクチン USB3 の関連ソフトを確認

ワクチン USB3 には以下の関連ソフトがあります。

項目	概要
オンプレミス型管理サービス サービス名：Info Banker	ワクチン USB3 が出力するログを集中管理するオンプレミス型サービスです。 収集したログを管理者がネットワーク経由で離れた場所から管理/確認することが可能です。別売りの有償サービスになります。
クラウド型管理サービス サービス名：Info Banker Cloud	ワクチン USB3 が出力するログを集中管理するクラウド型サービスです。 収集したログを管理者がインターネット経由で離れた場所から管理/確認することが可能です。別売りの有償サービスになります。
自動起動補助ソフト ソフト名：AutorunAssist	ワクチン USB の自動起動を補助するソフトウェアです。本ソフトウェアをインストールすることにより、OS の設定等によりオートランが禁止されている環境下で、ワクチン USB を自動起動することができます。

マニュアルを表示する

本製品のマニュアル(PDF)はメイン画面から[ヘルプ]メニューの[マニュアルを開く]を選択してください。

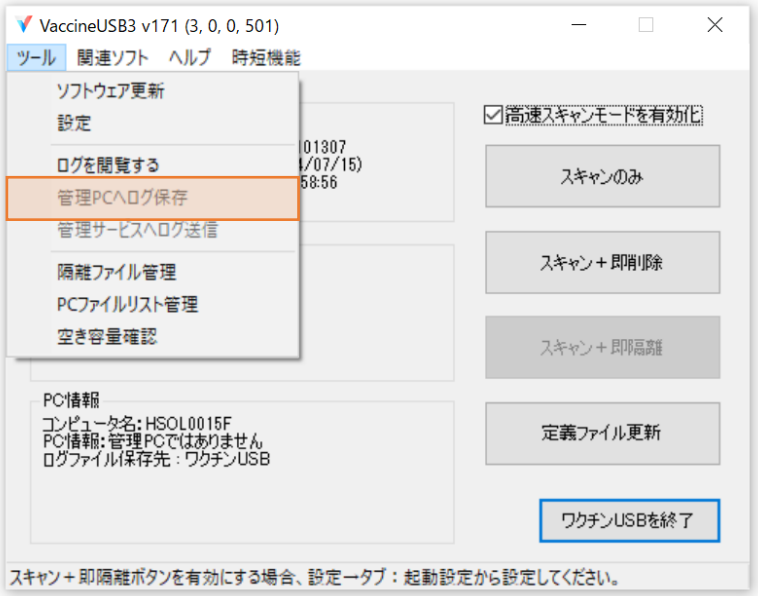
またはこちらからご確認ください。

本製品の QA サイト(web)を表示する

本製品の QA サイト(web)はメイン画面から[ヘルプ]メニューの[QA サイト(web)へ移動]を選択してください。

またはこちらからご確認ください

その他の詳細事項

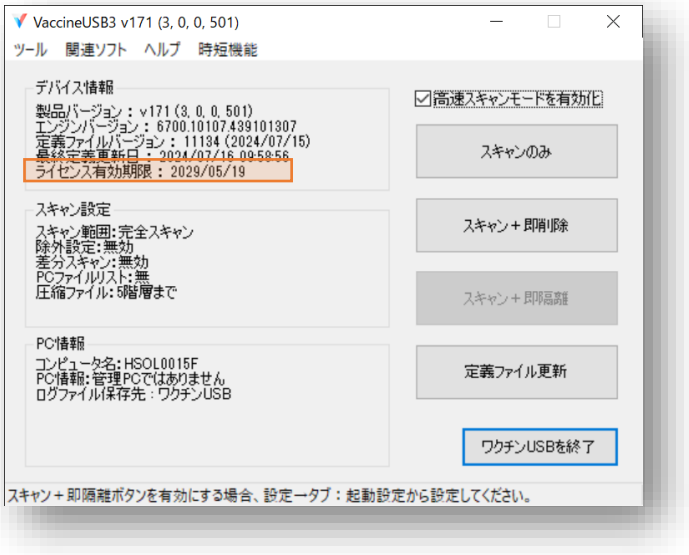
項目	内容
管理 PC へのログ送信タイミング	• ウイルス定義ファイル更新後 • ウイルススキャン処理終了後 • メイン画面→ツール→[管理 PC へログ保存]ボタンを押した時 
管理 PC へのログの保存場所	ログインユーザーの My Documents¥VaccineUSB フォルダの下です。 ※ 環境変数を実際のパス： %USERPROFILE%¥My Documents¥AdminVaccineUSB ログファイルは以下のフォルダに分けられ保存されます。 Admin¥VaccineUSB¥*****¥@@@@@¥ログファイル • *****：ウイルス有り無しで格納フォルダが変わります。 -ウイルス有り：Virus_Log -ウイルス無し：NoVirus_Log • @@@@@：スキャンを行った月(YYYYMM)が入ります。
管理 PC 用ログ内容	通常のログ内容と同じです。
管理 PC へログを送信した後のワクチン USB 内の管理 PC ログ	管理 PC へログファイルを送信後、送信に成功したワクチン USB 内の管理 PC 用ログは削除されます。
管理 PC ログの閲覧方法	管理 PC ログはワクチン USB から閲覧することはできません。 管理 PC へ出力した管理 PC ログを閲覧ください。
ワクチン USB 内の管理 PC 用ログ削除方法	ワクチン USB のログ閲覧から[ログ一括消去]を押してください。 ※通常のログも削除されるのでご注意ください。
ワクチン USB 内に管理 PC 用ログ有無の確認方法	ワクチン USB のログ閲覧画面に下部に表示されます。 管理 PC 用ログファイル：あり/なし

18 ライセンス更新手順について

ウイルススキャンソフトはライセンス製品です。ライセンスが切れた場合、「定義ファイル更新」ができなくなります。ライセンス更新を行ってください。

ライセンス有効期限の確認方法

メイン画面のライセンス有効期限を確認してください。空白の場合、まだライセンスが開始されておりません。

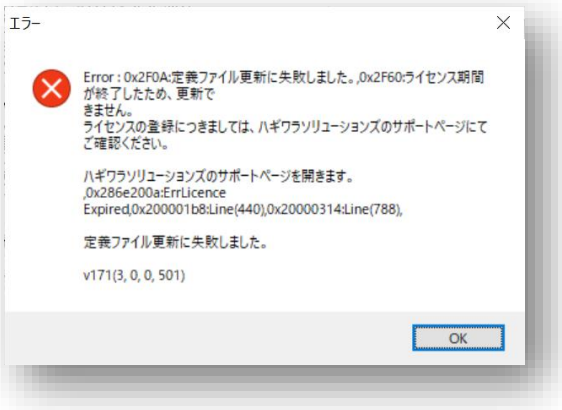


ライセンスが切れた場合の動作

・ライセンスが切れると定義ファイル更新ができなくなります。

・ウイルススキャン・削除・隔離等の機能は使用可能です。

・ライセンスが切れた後に定義ファイル更新を行うと以下の警告メッセージが表示されます。



ライセンス更新方法

ライセンスを更新する場合は、弊社ホームページのライセンス更新手順をご確認ください。

ライセンス関連でよくあるご質問

ライセンスが切れた後にライセンス更新できますか	ライセンス更新できます。ライセンスは新たに更新した日から 1 年延長されます。
ライセンス有効期限内にライセンス更新できますか	ライセンス更新できます。ライセンスは現在のライセンス終了日から 1 年延長されます。
ライセンス更新パックにエレコムブランドと、ハギワラブランドの２種類がありますが、エレコムとハギワラブランドのワクチン USB3 どちらにも使用可能ですか	使用可能です

19 WindowsXP での使用について

WindowsXP のサポートは終了しております。
弊社保証外となりますが、WindowsXP で動作する旧エンジン:5600 をご使用できます。
設定変更はこちらをご確認ください。

本設定ですが、サポートは 2015 年に終了しており、動作不可/機能不全等、一切問い合わせはお受けできませんので、ご了承上、ご利用ください。

20 ワクチン USB 自体へのウイルス感染防止対策

ワクチン USB3 は、製品自体にウイルス感染防止機能を搭載しています。
この機能により、ワクチン USB3 発売以降、感染事例は報告されていません。安心してご使用いただけます。

ウイルス感染防止策	ワクチン USB3 の CD-ROM ドライブとリムーバブルドライブは常時書き込み禁止に設定されています。これにより、 ウイルスを含むファイルの書き込みが完全に防止されています。

常時書き込み禁止の設定は、ウイルススキャン、定義ファイルの更新、ソフトウェアのアップデートなど、すべての操作に適用されます。そのため、ウイルスがワクチン USB に感染（書き込まれる）することはありません。
定義ファイルとログファイルは、ワクチン USB の隠し領域に安全に保存されます。この領域は、ドライブが書き込み禁止状態であっても、特殊な方法で書き込みが行われるため、セキュリティが確保されています。

21 Q&A

ワクチン USB の製品 Q&A はこちらをご確認ください。

ワクチン USB が途中で強制終了してしまう場合はこちらをご確認ください。

22 サポート

サポート・メンテナンスの内容

項目	サポート内容
製品	ワクチン USB3
サポート内容	本製品には、技術サポート（ウイルススキャンソフトサポート、ハードウェアサポート）、ウイルス定義ファイルの更新、ウイルススキャンソフトのマイナーアップデートのサポート・メンテナンスをご用意しております。
サポート・保証期間	ULD-VAU31A/HUD-MVDT31A：ご購入後 1 年 ULD-VAU33A/ HUD-MVDT33A：ご購入後 3 年 ULD-VAU35A/ HUD-MVDT35A：ご購入後 5 年 ※ハードウェア本体の保証期間は、本製品納品日起算となります。

お問合せ窓口

ご連絡先		受付
電話（ナビダイヤル）	0570-080-900	9:00～12:00／13:00～18:00 月曜日～金曜日 （祝祭日、夏期、年末年始特定休業日を除く）
電子メール	vsolsupport@hagisol.co.jp	24 時間受付

※ナビダイヤルについて
弊社では、お問い合わせ窓口にナビダイヤルを採用しています。
ナビダイヤルは、全国一律の通話料でご利用いただける NTT コミュニケーションズ（株）が提供するサービスです。
ナビダイヤル通話料から弊社が利益を得るシステムではありません。
通話料金の目安はナビダイヤルサービス接続時に、音声ガイダンスにてご案内しております。
一部の PHS、IP 電話はご利用いただけません。その際は固定電話、または携帯電話からおかけ直しください。
お待ちいただいている間も通話料がかかります。混雑時はしばらくたってからおかけ直しください。

※個人情報に関する保護方針はホームページをご参照ください。
ハギワラソリューションズ株式会社ホームページ：http://www.hagisol.co.jp

- 弊社は品質、信頼性の向上に努めておりますが、一般に半導体を使用した製品は誤作動したり故障したりすることがあります。
- 弊社半導体使用製品をご使用いただく場合は、半導体使用製品の誤作動や故障により、生命・身体・財産が侵害されることのないように、お客様の責任において、使用されるようにお願い致します。
- スキャンプログラム及びそれを組み込んだ本製品は fault-tolerant（その構成部品の一部が故障しても正常に処理を続行するシステム）ではなく、fail-safe（故障や操作ミス、設計上の不具合などの障害が発生することをあらかじめ想定し、起きた際の被害を最小限にとどめること）なパフォーマンスを必要とする危険な環境での使用を意図していません。斯かる使用には、原子力施設の稼動、航空機ナビゲーション／通信システム、武器システム、直接生命維持装置、又は本製品（スキャンプログラムを含む）の障害が死亡、人身障害、又は身体的／物的損害に直接結びつくようなその他の使用（以下、総称して「ハイリスク活動」という）が含まれますが、これに限定されません。Trellix 及び弊社は、明示／黙示を問わず、ハイリスク活動への適合性については明示的にこれを否認します。
- 本書に掲載されている技術情報は、製品の代表的動作・応用を説明するためのもので、その使用に関して弊社および第三者の知的財産権その他の権利に対する保証を行うものではありません。
- 本書の掲載内容は、技術の進歩などにより予告なしに変更されることがあります。
-

◆ 本製品は、本製品は、CD-ROM 領域とリムーバブル領域を併せ持つ USB ストレージ技術「UDRW Technology」（特許取得済み）を搭載しております。
日本：特許第 3914949 号 特許第 3699717 号 特許第 3513147 号 米国：Patent No.7,111,121 B2 中国：特許番号 ZL200410038475.6 香港：特許番号 HK1068990 B 台湾：発明第 I 261757 号 韓国：特許 第 589521 号 欧州特許：(イタリア、フランス、ドイツ、イギリス) Patent No.149182 号

◆ 掲載されている商品の仕様・外観、およびサービス内容等については、予告なく変更する場合があります。あらかじめご了承ください。

◆ Microsoft Windows は米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

◆ その他掲載されている会社名、商品名は各社の商標または登録商標です。なお、本文中には©および ™ マークは明記しておりません。

◆ オープンソースライセンス
- 7-Zip : www.7-zip.org
  -7z.dll : GNU LGPL + unRAR restriction
  -All other files : GNU LGPL

ウイルス対策 USB ソリューション
ワクチン USB3　取扱説明書
2024 年 10 月 発行
発行　ハギワラソリューションズ株式会社