

ウイルス対策 USB ソリューション



リトマス USB2

HUD-MVDT1A

HUD-MVDT3A

HUD-MVDT5A

取扱説明書

この度はリトマス USB2（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。

1 ご使用になる前に

本製品は、米国 McAfee Co.,Ltd.（以下、McAfee 社）製エンジンを搭載したウイルス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、McAfee 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 McAfee 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。

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が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ます、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、McAfee 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いたします。
- ・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。また McAfee 社サイト等で、最新のウイルス情報を確認ください。
- ・本製品に組み込まれた McAfee 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。その場合は McAfee 社のサイトから専用の削除ツールをダウンロードすることで削除できる可能性があります。
- ・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。McAfee 社のサイトで削除方法を確認してください。
- ・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、McAfee 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。その様なウイルスにつきましては McAfee 社のデータベースなどをご確認の上、対処を行なってください。
- ・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、McAfee 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。

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。

- ・直射日光があたる場所
- ・水濡れの可能性のある場所
- ・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場所、急激に温度の変化がある場所
- ・平坦でない場所、土台が安定していない場所、振動の発生する場所
- ・強い磁界や静電気の発生する場所
- ・ほこりの多い場所

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、あらかじめ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 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、お買い求めの販売代理店までご連絡ください。

ロリトマス USB2（製品本体）..... 1 個

3 本製品について

本製品は、McAfee 社製ウイルススキャンエンジン、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）に感染しているコンピュータウイルスの検出および削除をする機能を搭載した製品です。

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

✓ ウィルススキャン機能

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、対象機器のウイルススキャンを実行します。

- ウィ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
- ウィルスを検知した場合 本体の赤色●LED が点灯します
- ウィ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。
- ウィルスが検知し、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：

ウイルス検知のみを実行します。ウイルスを削除・隔離しません。

スキャン+即削除：

ウイルス検知を実行しながら、ウイルスを検知すると即削除処理を行います。

スキャン+即隔離：

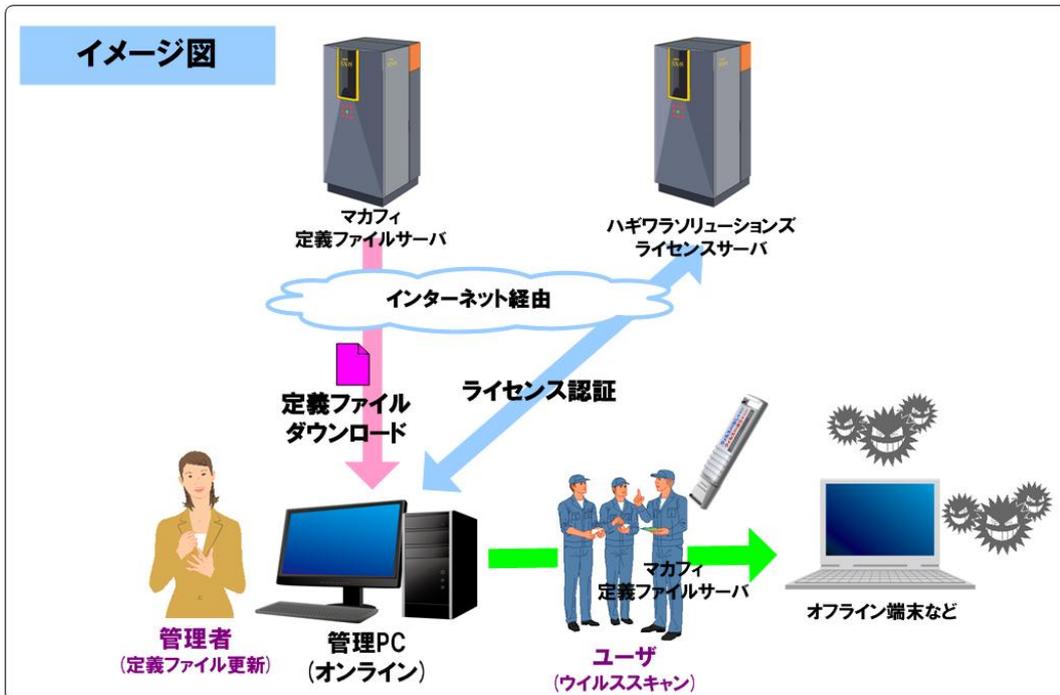
ウイルス検知を実行しながら、ウイルスを検知すると隔離処理を行います。

✓ 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。更新情報が確認されると、ソフトウェアの更新が可能になり、許可することでアップデートされます。

✓ 本製品へのウイルス感染防止機能

スキャン設定保存、ウイルス定義ファイル更新、ソフトウェア更新処理以外で、リムーバブルディスク領域への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です。

(ログを本製品のリムーバブルディスク内に保存する設定にした場合は、ウイルス感染のリスクがあります。)

✓ 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。

本製品の各部名称とLED点灯ルール



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。 もしくは感染ファイルを削除/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。

動作環境／製品仕様

USB インターフェース	USB1.1 (Full Speed)/USB 2.0 (High Speed/Full 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 512MB 以上 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)	Windows XP (SP2/SP3) Windows Vista (SP2) (*4) Windows 7 (*4) Windows 8/8.1 Windows10 Windows Server 2003 SP2 Windows Server 2003 R2 SP2 Windows Server 2008 SP2 Windows Server 2008 R2(*8) Windows Server 2012,2012R2(*8) Windows XP Embedded SP2 32bit(*6) Windows Embedded Standard 7(*10) Windows Embedded POSReady 7(*10) Windows Embedded Standard 2009(*10)	
対応ユーザーカウント	コンピュータの管理者 (Administrator) 制限ユーザー(*9)	
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	VCCI ClassB、CE、FCC	
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¥System32 へのアクセスは、Windows¥SysWOW64 にリダイレクトされます。
- *6 以下の関連するコンポーネントが組み込まれている必要があります。(※動作基準は弊社環境下での動作確認としております)
 - USB 関連全般のコンポーネント
 - ネットワーク関連のコンポーネント
 - ドライブ関連のコンポーネント
 - アプリケーション API 関連のコンポーネント
- *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 プロセススキャン機能は動作しません。
- *9 制限ユーザー下では OS の制限により、アクセス制限がかけられています。そのため以下のフォルダ以外で検知したウイルスは削除・隔離することができません。
 - Documents and Settings¥ログインユーザー名¥ 以下のフォルダ
- *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。(推奨の物理空きメモリ容量は 1GB 以上です)

 NOTE	<p>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。</p> <p>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ります。</p> <p>※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</p>
--	---

通信環境

ウイルス定義ファイルの更新、ソフトウェアの更新、ライセンスを管理するために通常インターネット環境に接続されたパソコンをご準備いただく必要があります。インターネットに接続するための設定は下記のとおりです。

- <http://www.udrw.com/>のドメインへのアクセスが許可されていること
- <http://update.nai.com/>のドメインへのアクセスが許可されていること
- <http://dl.hscjpn.co.jp/>のドメインへのアクセスが許可されていること
- http プロトコルによる接続ができること

NOTE	<p>proxy サーバーを経由した環境でもウイルス定義ファイルのダウンロードが可能です。 環境により「ユーザー認証」が表示される場合があります。</p> <ul style="list-style-type: none">• ユーザーID• パスワード <p>を入力するとインターネットへの接続が可能になります。 ユーザーID とパスワードはネットワーク管理者にお問い合わせください。 ユーザー認証を行う際には、モニタ、キーボードが必要です。</p>
------	---

4 セットアップからご使用まで

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。

<セットアップ>

管理 PC の設定	本製品の設定変更を許可するPC に本製品を接続し、管理PC の設定を行うことで、管理PC 以外では本製品の設定変更を禁止することができます。 * 管理 PC の設定は任意です。
ウイルス定義ファイルの更新	本製品をインターネットに接続されている PC に接続します。 起動画面が表示されたら[メイン]をクリックしてメイン画面を表示します。 [定義ファイル更新]をクリックすると、本製品内のウイルス定義ファイルを更新します。 ウイルススキャンソフトウェアのアップデートがあった場合は、定義更新後、ユーザーによる許可をした場合、ウイルススキャンソフトウェアのアップデート処理が行われます。

<製品のご使用>

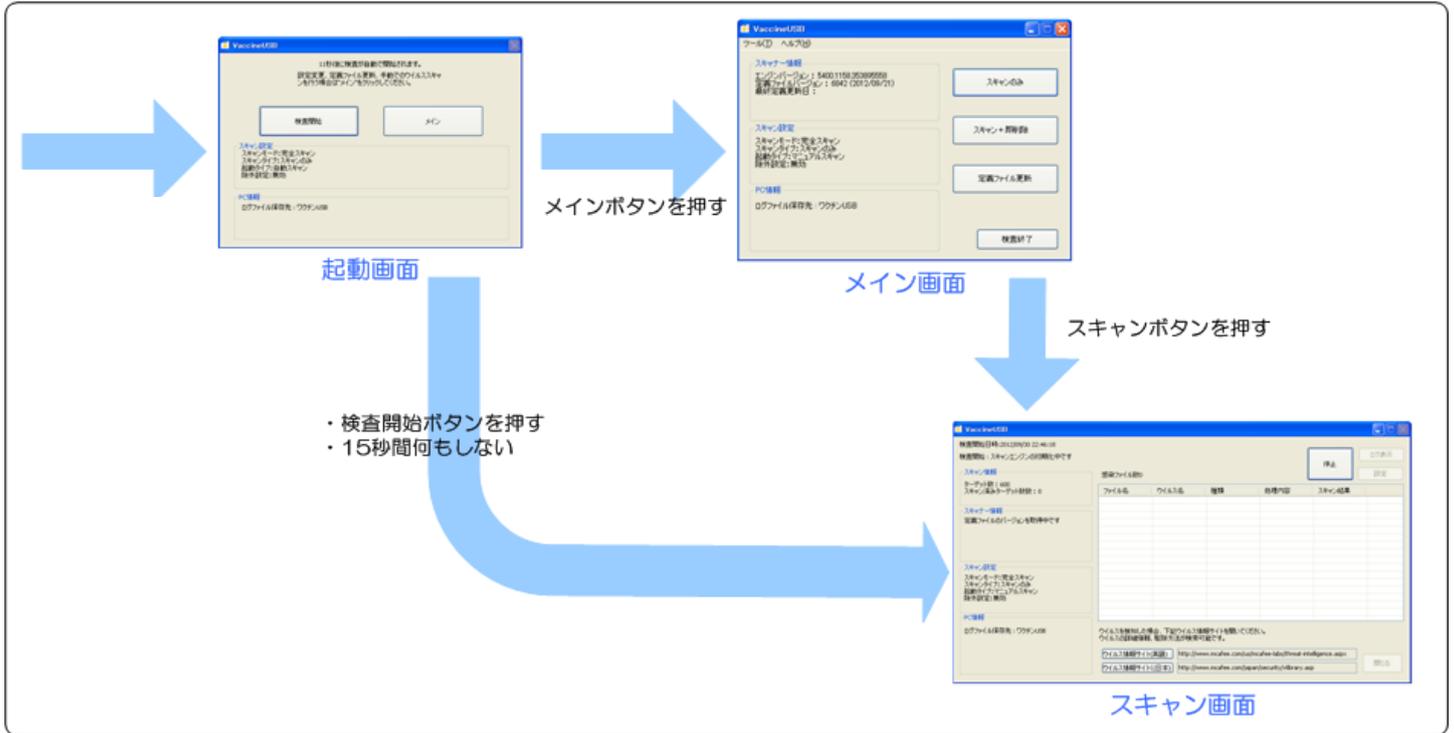
スキャンモードの設定	メニュー画面より設定ツールを起動し、スキャンターゲット、自動実行時のモードなどを設定していただき、書き込み保存をします。 メニュー画面より設定ツールを起動し、スキャンターゲット、自動実行時のモードなどを設定していただき、書き込み保存をします。 * 管理 PC の設定をしている場合、管理 PC 以外では設定変更はできません。 * 設定を書き込む際、ウイルスに感染するリスクがありますのでご注意ください。
ウイルススキャン実行	ウイルススキャンの対象機器に接続すると自動的にウイルススキャンを実行します。 自動実行をキャンセルすると、スキャンモードを選択してからスキャンを実行できます。 * 対象機器の設定によっては自動起動しない場合があります。
LED/スキャンログの確認	ウイルススキャンが終了すると、ウイルス検出結果を本製品に搭載された 2 つの LED で標示します。また、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。
ウイルス削除の実行	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、ウイルスの削除を行なってください。



スキャン対象機器にウイルススキャンソフトが既に入っている場合は、そのウイルススキャンソフトを無効に設定してください。著しくスキャン時間が長くなる場合があります。
ウイルススキャンを実行することにより、対象機器のパフォーマンスが著しく低下する場合があります。対象機器での作業が終了してから、本製品を接続してウイルススキャンを実行してください。

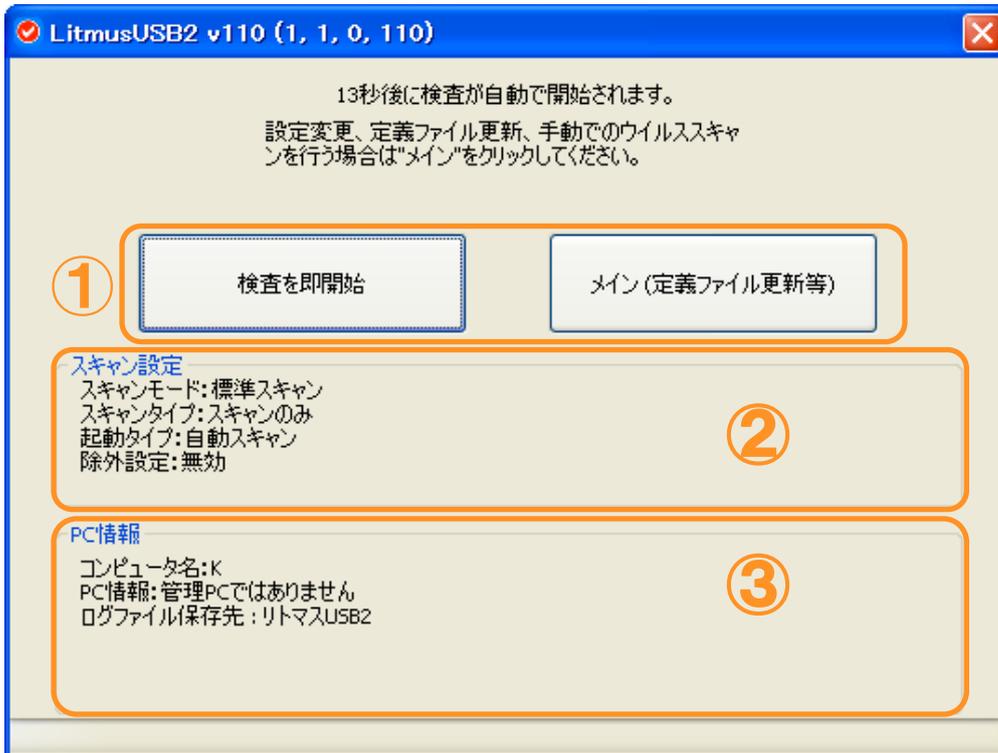
5 起動画面、メイン画面、スキャン画面の説明

リトマス USB2 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

リトマス USB 起動時に表示される画面です。



① 各種ボタン

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	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。

② 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4つのモードがあります。 <ul style="list-style-type: none"> • 完全スキャン：すべてドライブをチェックします • 標準スキャン：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：プロセスのみスキャンします。
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。 <ul style="list-style-type: none"> • 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。 • スキャン+削除：ウイルス検知を1度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。
起動タイプ	リトマスUSB2 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> 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。

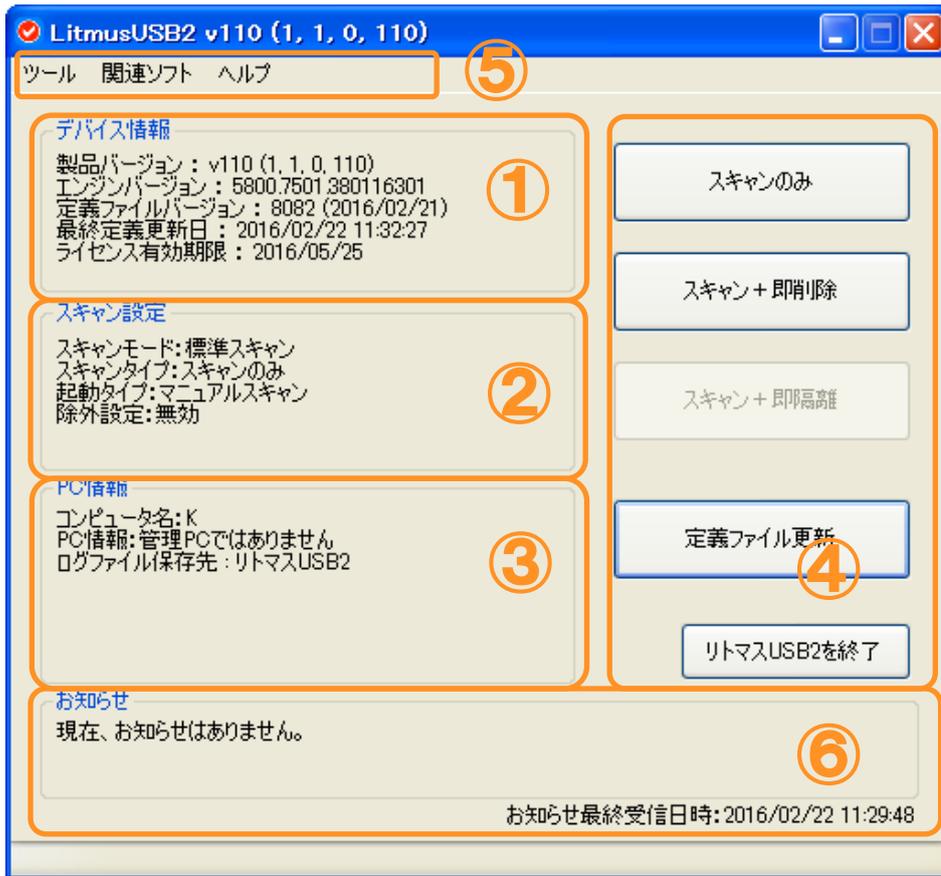
スキャン設定を変更する場合、メイン画面へ移動し、ツールバーから設定を選択してください。

③ 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • リトマスUSB2：リトマスUSB2内へログを保存します。 • 使用中のPC：リトマスUSB2内へログを保存できない場合、PCへログを保存します。 <p>※ リトマスUSB2内へのウイルス感染防止のために、ログファイルをリトマスUSB2の特殊な秘匿領域へ保存します。 この領域へはWindowsXP/2000/2003Server/2003ServerR2の制限ユーザーではアクセスできないため、ログはPCへ保存されます。</p>
PC へのログファイル保存場所	リトマスUSB2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。 <p>例；C:\¥Documents and Settings¥user¥My Documents¥LitmusUSB2¥LitmusUSB2_Log</p> <p>※ログファイルがリトマスUSB2へ保存できる場合、本項目は表示されません。</p>
PC 内のログファイルの有無	使用中のPCにリトマスUSB2のログが存在するかを表示します。 <ul style="list-style-type: none"> • ログファイルあり：PC内にリトマスUSB2のログが保存されています。 • ログファイルなし：PC内にリトマスUSB2のログは保存されていません。 <p>※ログファイルがリトマスUSB2へ保存できる場合、本項目は表示されません。</p>

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 デバイス情報

項目	内容
製品バージョン	リトマス USB2 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。

② 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4つのモードがあります。 <ul style="list-style-type: none"> 完全スキャン：すべてドライブをチェックします 標準スキャン：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4つのモードがあります。 <ul style="list-style-type: none"> 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。 スキャン+削除：ウイルス検知を1度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。
起動タイプ	リトマス USB2 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。 <ul style="list-style-type: none"> 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

関連ソフト→リトマス USB2 DatCharger	定義ファイル更新作業支援ソフトウェア 「リトマス USB2 DatCharger」サイト(web)へ移動します。
関連ソフト→Info Banker	ログ集中管理サーバーソフトウェア「Info Banker」サイト(web)へ移動します。
ヘルプ→バージョン情報	リトマス USB2 のバージョン情報を表示します。
ヘルプ→マニュアルを開く	リトマス USB2 のマニュアル(PDF ファイル)を表示します。
ヘルプ→QA サイト(web)へ移動	リトマス USB2 の QA サイト(web)へ移動します。
ヘルプ→ライセンス更新サイトへ移動	リトマス USB2 のライセンス更新サイト(web)へ移動します。

⑥ お知らせ

項目	内容
お知らせ	ハギワラソリューションズからのリトマス USB2 に関するお知らせを表示します。
お知らせ最終受信日時	最後にお知らせを受信した日時を表示します。

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 スキャンの状態を表します。

スキャン中	ウイルスが存在しない場合	ウイルスが存在する場合	エラーが発生した場合	中断した場合

※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 処理中のファイルの名称およびパスを表示します。

③ スキャンの進行状況を表示します。

④ スキャン時間を表示します。

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。

⑤ スキャンの状況を表示します。

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。

⑥ デバイス情報

項目	内容
製品バージョン	リトマス USB2 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。

⑦ 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 4 つのモードがあります。 <ul style="list-style-type: none"> 完全スキャン：すべてドライブをチェックします 標準スキャン：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。 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。
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 4 つのモードがあります。 <ul style="list-style-type: none"> 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。 スキャン+削除：ウイルス検知を 1 度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。
起動タイプ	リトマス USB2 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。

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。

⑧ 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> リトマス USB2：リトマス USB2 内へログを保存します。 使用中の PC：リトマス USB2 内へログを保存できない場合、PC へログを保存します。 ※リトマス USB2 内へのウイルス感染防止のために、ログファイルをリトマス USB2 の特殊な秘匿領域へ保存します。 この領域へは WindowsXP/2000/2003Server/2003ServerR2 の制限ユーザーではアクセスできないため、ログは PC へ保存されます。
PC 内のログファイルの有無	使用中の PC にリトマス USB2 のログが存在するかを表示します。 <ul style="list-style-type: none"> ログファイルあり：PC 内にリトマス USB2 のログが保存されています。 ログファイルなし：PC 内にリトマス USB2 のログは保存されていません。 ※ログファイルがリトマス USB2 へ保存できる場合、本項目は表示されません。

⑨ ウイルススキャンする場所を表示します。

⑩ 発見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	マカフィ社が規定したウイルス名が表示されます
種類	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・隔離していません。 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。

⑪ ウイルス情報サイトへのリンクです。ウイルス情報サイトではウイルス名を入力し検索してください。

⑫ ボタンの機能

ボタン	内容
再検査/停止	再検査：ウイルススキャンを再度行います。 停止：ウイルススキャンを停止します。
ログ表示	リトマス USB2 内に保存されているログ管理画面を表示します。
設定	リトマス USB2 設定画面で表示します。
閉じる	メイン画面に戻ります（自動実行時は、ウイルススキャンソフトを終了します）。

⑬ 製品の注釈を表示します。

■タッチパッドに最適化した画面

The screenshot shows the .itmusUSB2 v100 (1, 0, 0, 100) application window. It features a top navigation bar with buttons for 'SCAN...', '停止' (Stop), '設定' (Settings), 'ログ表示' (Log Display), and '閉じる' (Close). Below this are two main panels: 'スキャン時間' (Scan Time) and 'スキャナー情報' (Scanner Information). The 'スキャン時間' panel displays system details like computer name and scan start/end times. The 'スキャナー情報' panel shows product and engine versions, and scan mode. A 'スキャン情報' (Scan Information) section includes a progress bar and statistics on scanned files. At the bottom, there is a table for scan results and a note about compressed files.

① スキャンの状態を表します。

スキャン中	ウイルスが存在しない場合	ウイルスが存在する場合	エラーが発生した場合	中断した場合

※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 スキャン時間を表示します。

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。

③ スキャナー情報

項目	内容
製品バージョン	リトマス USB2 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。

スキャンモード	<p>ウイルススキャン範囲を表示します。以下の3つのモードがあります。</p> <ul style="list-style-type: none"> • 完全スキャン：すべてドライブをチェックします • 標準スキャン：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。 • プロセススキャンのみ：プロセスのみスキャンします。
スキャンタイプ	<p>ウイルススキャン動作を表示します。以下の4つのモードがあります。</p> <ul style="list-style-type: none"> • 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。 • スキャン+削除：ウイルス検知を1度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。

④ スキャンの状況を表示します。

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。
スキャンパス表示	処理中のファイルの名称およびパスを表示します。スキャンが完了すると検査の結果を表示します。また進行状況をプログレスバーで表示します。
感染ファイル数	ウイルス感染ファイル数を表示します。
感染ファイル削除数	ウイルス感染ファイルを削除したファイル数を表示します。
感染ファイル隔離数	ウイルス感染ファイルを隔離したファイル数を表示します。

⑤ 発見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	シマンテック社が規定したウイルス名が表示されます
種類	シマンテック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	<p>見つかったウイルスへの処理結果を表示します。</p> <p>ウイルスを発見しました：ウイルスを発見のみしました。ウイルスは削除していません。</p> <p>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。</p> <p>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。</p>

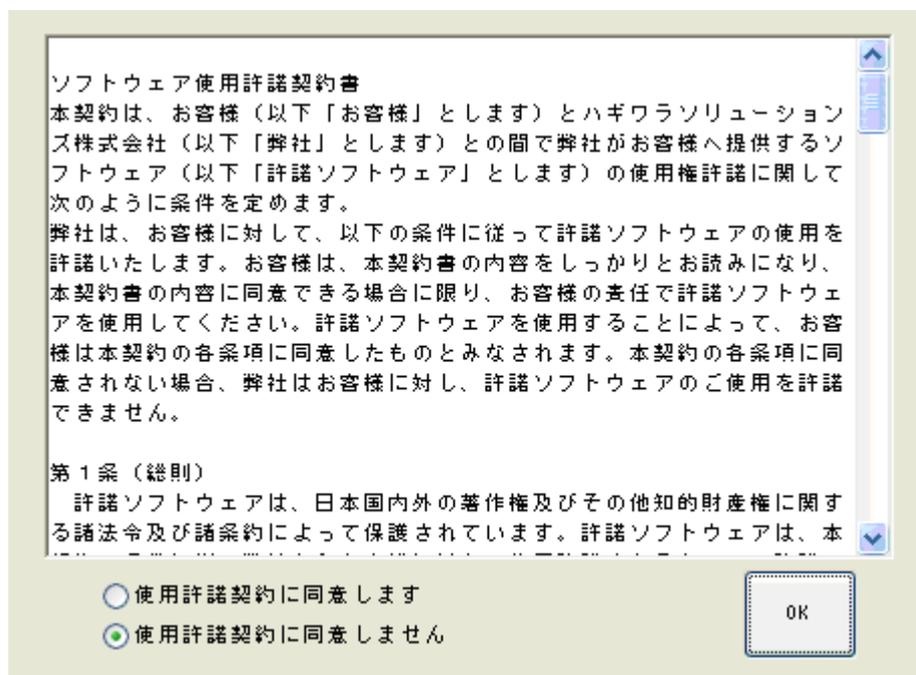
⑥ ボタンの機能

ボタン	内容
再検査/停止	<p>再検査：ウイルススキャンを再度行います。</p> <p>停止：ウイルススキャンを停止します。</p>
ログ表示	リトマス USB2 内に保存されているログ管理画面を表示します。
設定	リトマス USB2 設定画面で表示します。
閉じる	メイン画面に戻ります（自動実行時は、ウイルススキャンソフトを終了します）。

⑦ 製品の注釈を表示します。

使用許諾承認

1. 本製品を接続するソフトウェア使用許諾に関する画面を表示します。内容を確認してください。



2. 問題がない場合「使用許諾契約に同意します」を選択し、[OK]ボタンをクリックしてください。

PCをウイルススキャンする

セットアップが完了しましたら、スキャンを実行することができます。

1. 本製品を対象機器に接続すると、ウイルススキャンソフトが起動します。

※自動的にウイルススキャンソフトが起動しない場合/CD-ROM領域が認識しない環境で使用する場合

マイコンピュータの[リムーバブルディスク]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。

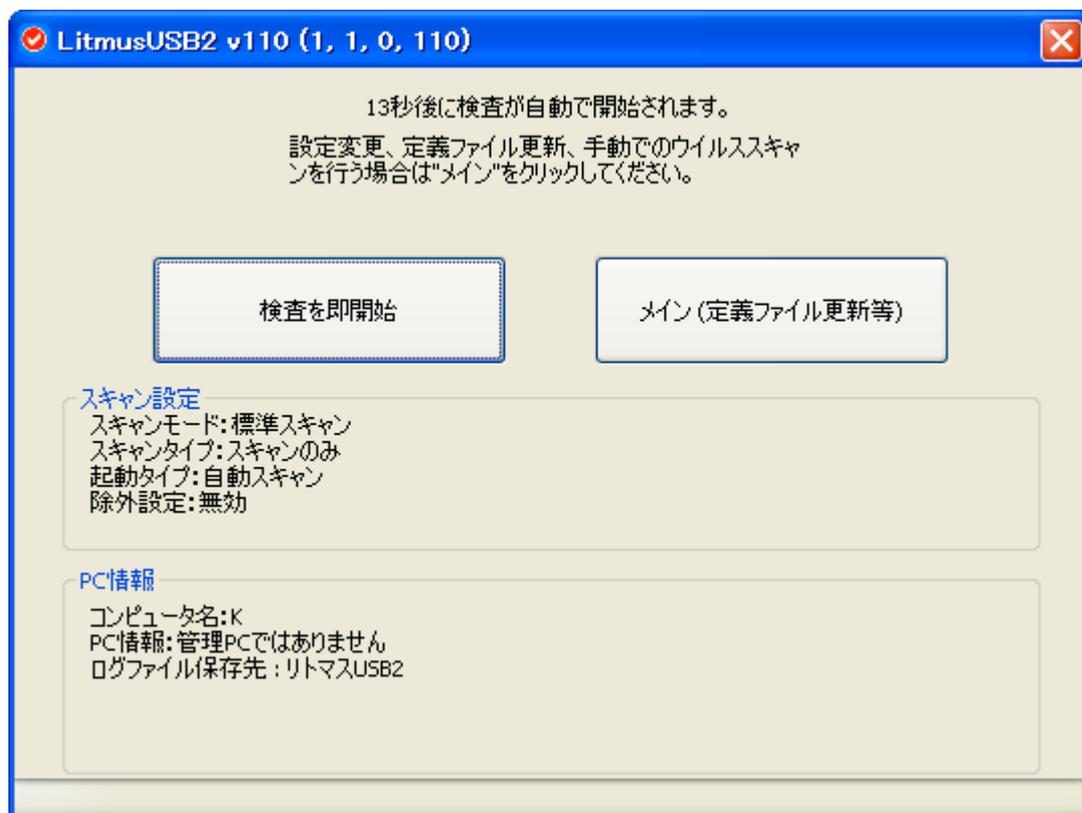


StartUp.exe

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]、[スキャン+削除]、「スキャン*即隔離」を選択しウイルススキャンを行う。

①起動画面からウイルススキャン/②起動画面で15秒待ち自動ウイルススキャン

起動画面で[検査開始]ボタンをクリック、もしくは15秒待つとウイルススキャンを開始します。

本製品のウイルススキャンは以下の2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、十分ご注意ください。
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、十分ご注意ください。 隔離したファイルはPCの特定フォルダに保存されます。
スキャン+削除	ウイルス検知を1度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。

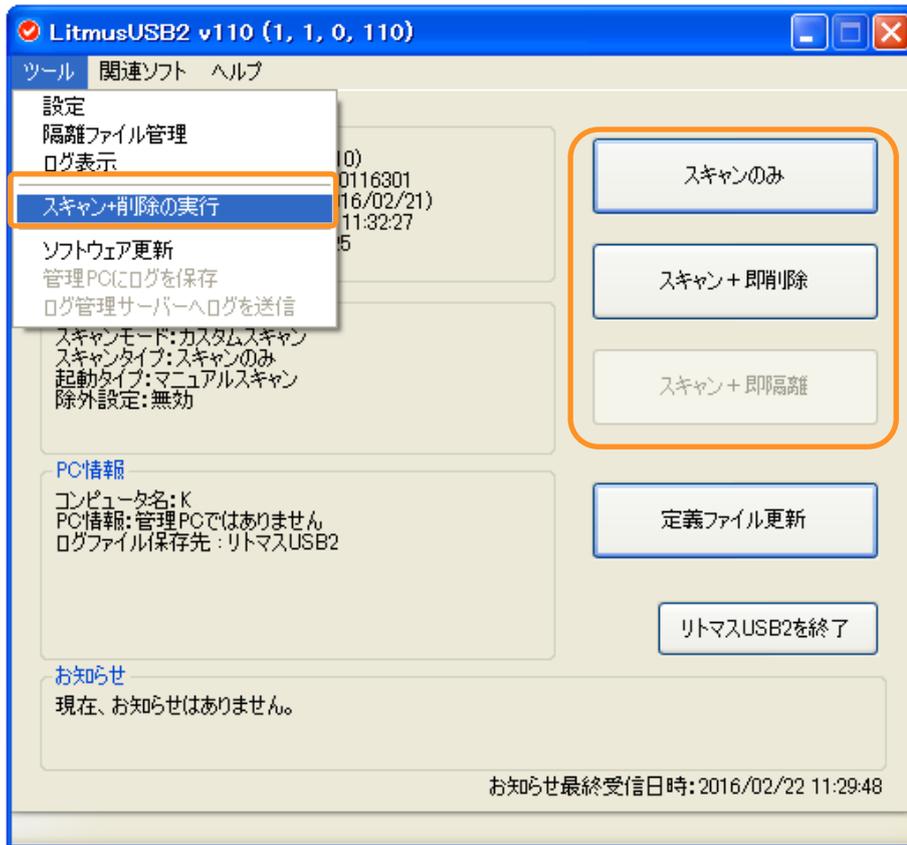
この①、②でウイルススキャンを開始した場合、設定されているモードが実行されます。

初期モードは[スキャンのみ]に設定されています。設定変更はメイン画面からツール>設定を選択してください。

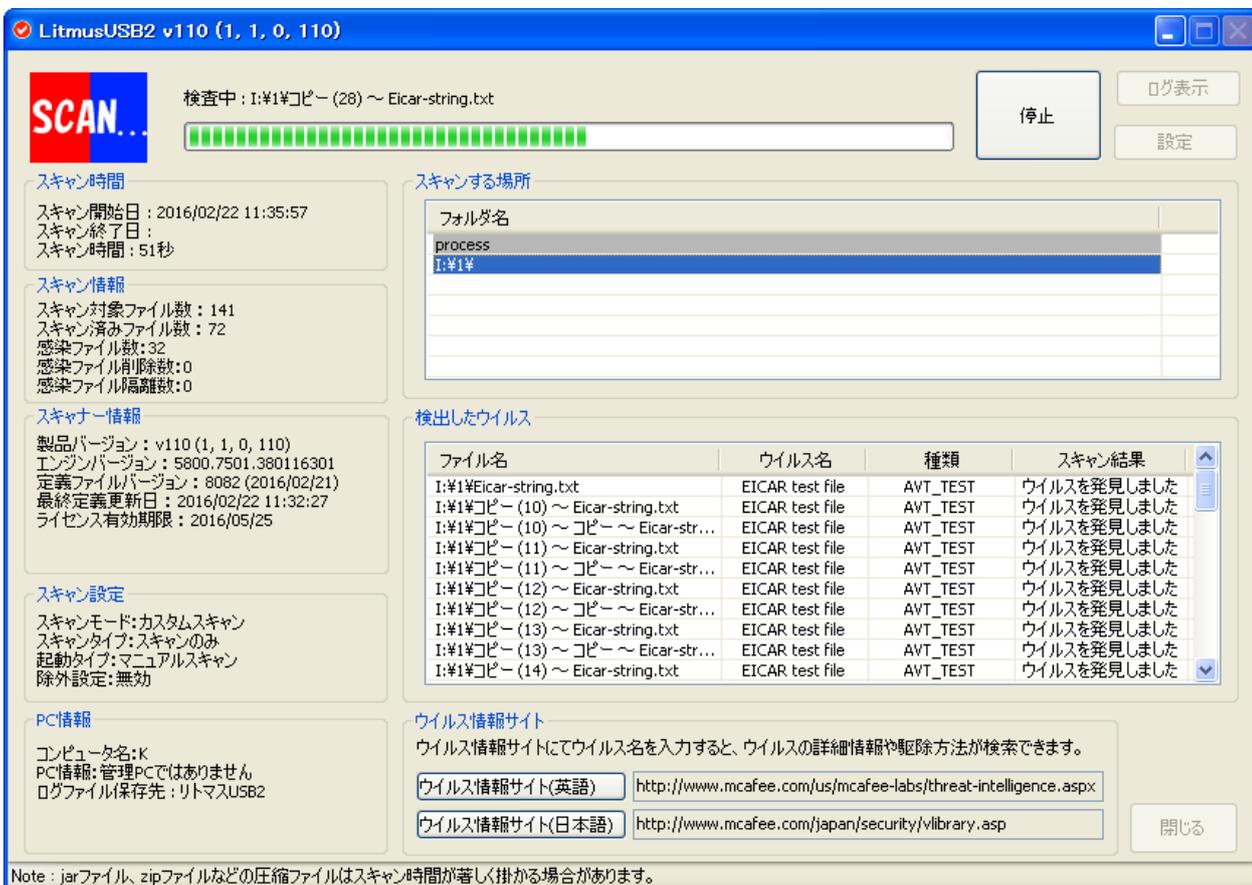
③メイン画面からウイルススキャン方式を選択し、ウイルススキャンを開始する。

起動画面で[メイン]ボタンを押すとメイン画面へ移動します。メイン画面で[スキャンのみ]、

[スキャン+即削除]、[スキャン+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。



3. スキャン画面が表示され、ウイルススキャンが行なわれます。



4.ウイルススキャンが完了すると、検査結果が出ます。ウイルスを発見した場合は本製品の赤色LEDが、発見なかった場合は青色LEDが点灯します。

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。

またウイルス結果が画面上にも表示されます。



■検査結果

検査結果画像	コメント	内容
SAFETY	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。	ウイルスが見つからなかった場合に表示されます。
SAFETY	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。
SAFETY	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。
WARNING	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。
WARNING	ウイルスが見つかり、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、全てのウイルスが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。

WARNING	ウイルスが見つかり、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、全てのウイルスが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。
ERROR	リトマス USB2 にエラーが発生しました。	リトマス USB2 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。
STOPPED	リトマス USB2 をユーザーによって途中で中断しました。	ユーザーによってリトマス USB2 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。

■ 検査情報

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。
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。

発見したウイルス情報を確認するにはスキャン画面よりウイルス情報サイトへ移動し、ウイルス名を入力し検索してください。[ログ表示]ボタンを押すと、実行したウイルススキャンのログを表示することができます。

※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。

<ウイルスを発見した場合は>

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」または「スキャン+削除」を選択し、ウイルスの削除/隔離を行なってください。

リトマス USB2 を取り外す場合は、[閉じる]ボタンを押し、メイン画面から[リトマス USB2 を終了]ボタンを押してください。

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。

詳細は下記の McAfee ホームページへアクセスしてウイルスの削除方法について確認してください。

- ・ 英語サイト：<http://www.mcafee.com/threat-intelligence/malware/latest.aspx>
- ・ 日本サイト：<http://www.mcafee.com/japan/security/vlibrary.asp>

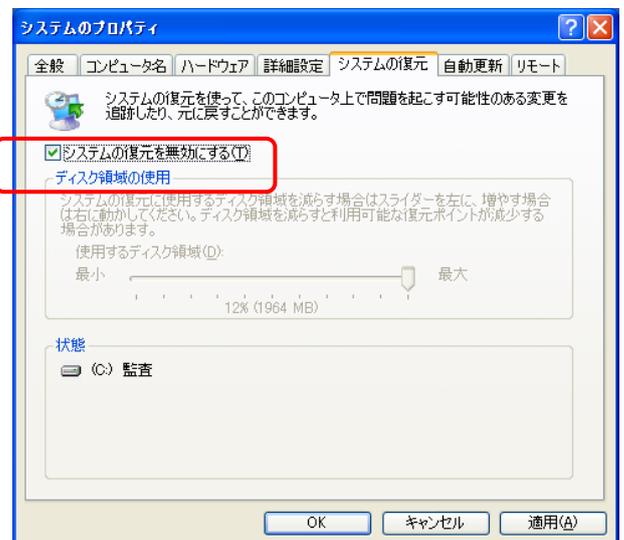
また、次の方法で削除できる場合もあります。

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。

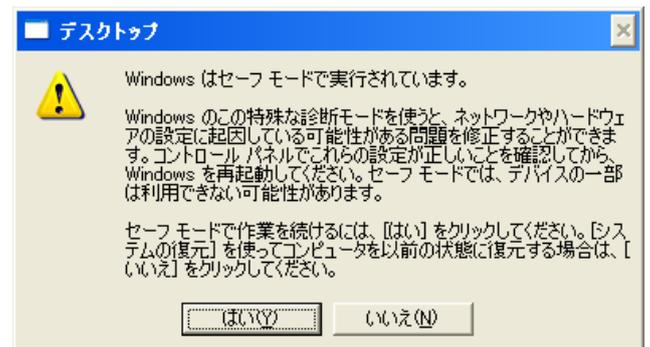
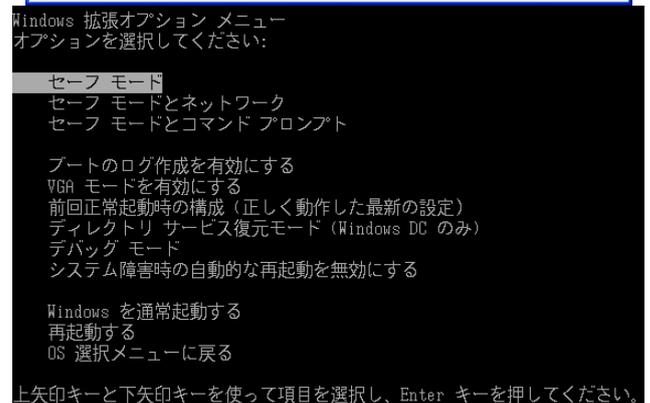
システムリストア機能を無効にする方法

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。
- ※ リ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。

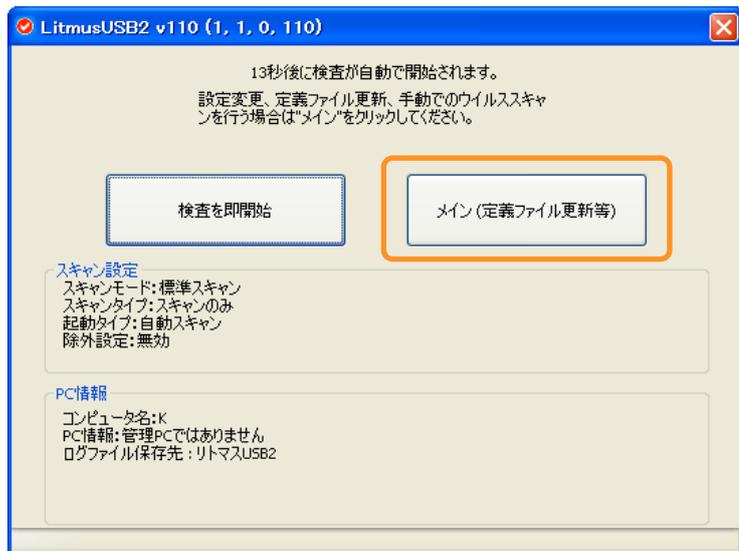


ウイルス定義ファイルを更新する

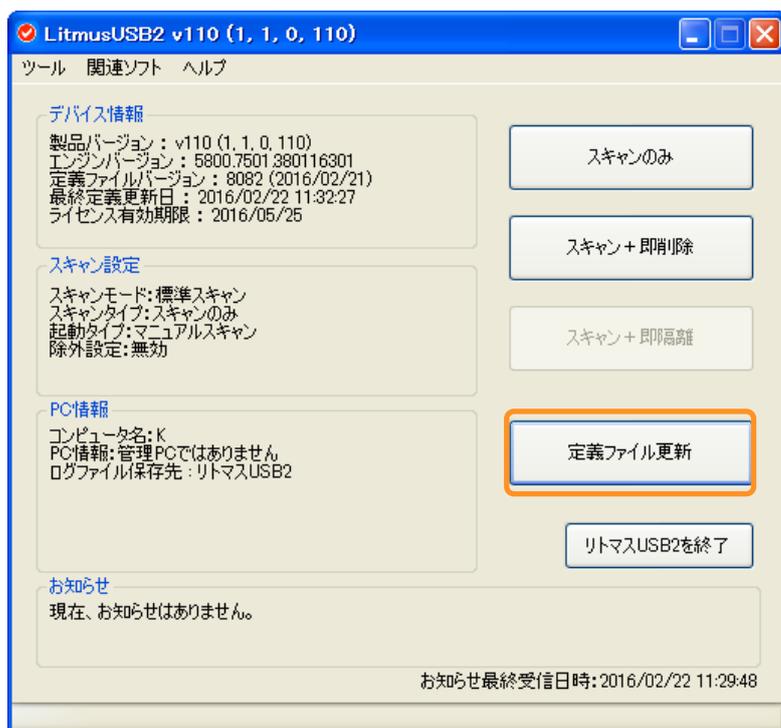
ウイルススキャンする際は必ずウイルス定義ファイルを更新し、最新のウイルス定義ファイルをご使用ください。

1. インターネットに接続している PC に、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. 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を更新する際、リトマス USB2 への書き込み制限を解除します。

書き込み制限を解除するとリトマス USB2 自身にウイルスに感染するリスクが発生します。

必ず最新パターンのウイルス対策製品がインストールされている PC で実行してください。

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。

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、ソフトウェア更新画面が表示されます。

7 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リトマス 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ーへ行うことが容易になります。

隔離ファイル概要

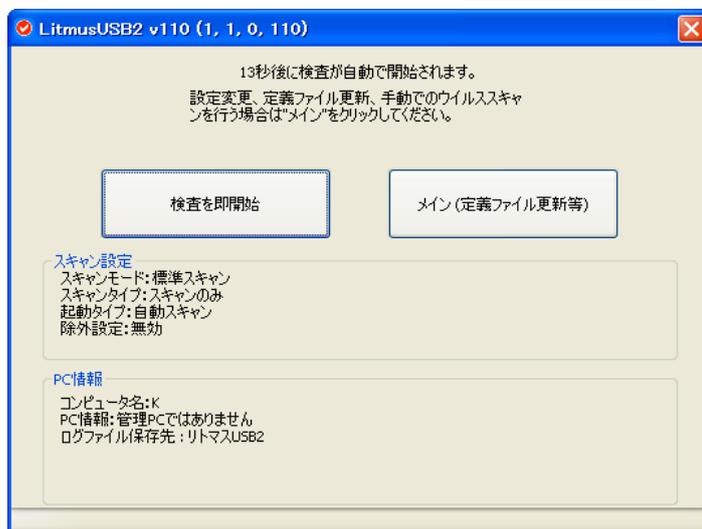
隔離ファイルの仕様は以下になっています。

項目	内容
ファイル圧縮形式	パスワード付圧縮
隔離ファイル保存先	%appdata%\%litusb%\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

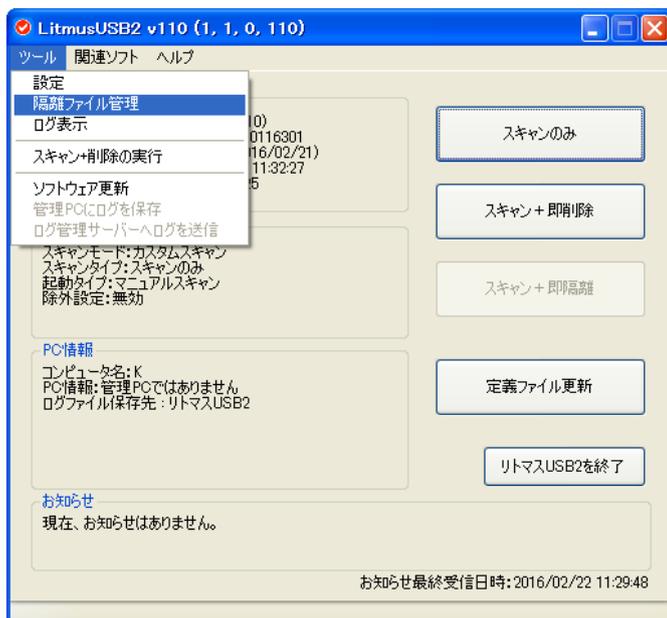
隔離ファイル管理画面への移動

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：現在リトマス 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

項目	内容
検出日時	ウイルスが検出、隔離された日時
ウイルス名	ウイルス名
ウイルス種類	ウイルスの種類
ウイルスが存在したフルパス	ウイルスが存在したフルパス
隔離ファイル名	ウイルスをパスワード圧縮、保存したファイル名
ファイルサイズ	隔離した後のファイルサイズ

- ②：PC に保存されている隔離ファイルへの処理ボタン

項目	内容
選択している PC の隔離ファイルを解凍して元に戻す	選択している PC の特定フォルダに保存されている隔離ファイルを解凍して、元の場所へ戻します。
元に戻した隔離ファイル一覧	過去に元に戻した隔離ファイル一覧を表示します。
選択している PC の隔離ファイルを削除	選択している PC の特定フォルダに保存されている隔離ファイルを削除します。
選択している PC の隔離ファイルをリトマス USB へ移動	選択している PC の特定フォルダに保存されている隔離ファイルをリトマス USB の特殊な領域へ安全に移動します。ウイルスの解析等が必要な時にご使用ください。

- ③：リトマス USB 内に保存されている隔離ファイル一覧

項目	内容
検出日時	ウイルスが検出、隔離された日時
ウイルス名	ウイルス名
ウイルス種類	ウイルスの種類
ウイルスが存在したフルパス	ウイルスが存在したフルパス
隔離ファイル名	ウイルスをパスワード圧縮、保存したファイル名
ファイルサイズ	隔離した後のファイルサイズ

- ④：リトマス USB 内に保存されている隔離ファイルへの処理ボタン

項目	内容
選択しているリトマス USB 内の隔離ファイルを PC へ保存	選択しているリトマス USB 内に保存されている隔離ファイルを PC へ保存します。PC へ保存しても解凍はしません。ウイルスの解析等が必要な時にご使用ください。
選択しているリトマス USB 内の隔離ファイルを削除	選択しているリトマス USB 内の隔離ファイルを削除します。

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。

現在リトマスUSB2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

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフルパス	隔離ファイル名	ファイルサイズ
2016/02/12 10:08:51	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160212100851_12f806c2.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160222114537_1cbea21e.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ Eicar-string.txt	20160222114537_1cbea2f9.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ コピー ~ Eic...	20160222114538_1cbea386.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ Eicar-string.txt	20160222114538_1cbea412.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ コピー ~ Eic...	20160222114538_1cbea49f.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ Eicar-string.txt	20160222114538_1cbea51c.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ コピー ~ Eic...	20160222114538_1cbea5a8.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ Eicar-string.txt	20160222114538_1cbea635.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ コピー ~ Eic...	20160222114538_1cbea6c2.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ Eicar-string.txt	20160222114539_1cbea74e.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ コピー ~ Eic...	20160222114539_1cbea7db.zip	1KB

隔離したウイルスを元に戻す

PCに隔離され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。

現在リトマスUSB2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

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフルパス	隔離ファイル名	ファイルサイズ
2016/02/12 10:08:51	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160212100851_12f806c2.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160222114537_1cbea21e.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ Eicar-string.txt	20160222114537_1cbea2f9.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ コピー ~ Eic...	20160222114538_1cbea386.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ Eicar-string.txt	20160222114538_1cbea412.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ コピー ~ Eic...	20160222114538_1cbea49f.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ Eicar-string.txt	20160222114538_1cbea51c.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ コピー ~ Eic...	20160222114538_1cbea5a8.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ Eicar-string.txt	20160222114538_1cbea635.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ コピー ~ Eic...	20160222114538_1cbea6c2.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ Eicar-string.txt	20160222114539_1cbea74e.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ コピー ~ Eic...	20160222114539_1cbea7db.zip	1KB

PCの隔離ファイルを解凍して元に戻す

元に戻した隔離ファイル一覧

PCの隔離ファイルを削除

PCの隔離ファイルをリトマスUSB2へ移動

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。

現在リトマスUSB2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

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフルパス	隔離ファイル名	ファイルサイズ
2016/02/12 10:08:51	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160212100851_12f806c2.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160222114537_1cbea21e.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ Eicar-string.txt	20160222114537_1cbea2f9.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ コピー ~ Eic...	20160222114538_1cbea386.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ Eicar-string.txt	20160222114538_1cbea412.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ コピー ~ Eic...	20160222114538_1cbea49f.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ Eicar-string.txt	20160222114538_1cbea51c.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ コピー ~ Eic...	20160222114538_1cbea5a8.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ Eicar-string.txt	20160222114538_1cbea635.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ コピー ~ Eic...	20160222114538_1cbea6c2.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ Eicar-string.txt	20160222114539_1cbea74e.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ コピー ~ Eic...	20160222114539_1cbea7db.zip	1KB

PCの隔離ファイルを解凍して元に戻す

元に戻した隔離ファイル一覧

PCの隔離ファイルを削除

PCの隔離ファイルをリトマスUSB2へ移動

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。現在リトマス 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。

現在リトマスUSB2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

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフォルパス	隔離ファイル名	ファイルサイズ
2016/02/12 10:08:51	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160212100851_12f806c2.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160222114537_1cbea21e.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ Eicar-string.txt	20160222114537_1cbea2f9.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ コピー ~ Eic...	20160222114538_1cbea386.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ Eicar-string.txt	20160222114538_1cbea412.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ コピー ~ Eic...	20160222114538_1cbea49f.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ Eicar-string.txt	20160222114538_1cbea51c.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ コピー ~ Eic...	20160222114538_1cbea5a8.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ Eicar-string.txt	20160222114538_1cbea635.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ コピー ~ Eic...	20160222114538_1cbea6c2.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ Eicar-string.txt	20160222114539_1cbea74e.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ コピー ~ Eic...	20160222114539_1cbea7db.zip	1KB

PCの隔離ファイルを解除して元に戻す

元に戻した隔離ファイル一覧

PCの隔離ファイルを削除

PCの隔離ファイルをリトマスUSB2へ移動

管理画面で①でウイルスを選択し、[元に戻した隔離ファイル一覧] ボタンを押してください。以下画面の様にファイル一覧が表示されます。

元に戻した隔離ファイル一覧

復元日時	復元先	検出日時	ウイルス名	ウイルス種類
2016/02/05 13:34:57	I:\¥1¥Eicar-string.txt	2016/02/05 13:27:00	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (10) ~ Eicar-string.txt	2016/02/05 13:27:00	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (100) ~ Eicar-string.txt	2016/02/05 13:27:00	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (101) ~ Eicar-string.txt	2016/02/05 13:27:00	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (102) ~ Eicar-string.txt	2016/02/05 13:27:00	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (103) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (104) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (105) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (106) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (107) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (108) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (109) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (11) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (110) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (111) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (112) ~ Eicar-string.txt	2016/02/05 13:27:01	EICAR test file	AVT_TEST
2016/02/05 13:34:57	I:\¥1¥コピー (113) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (114) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (115) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (116) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (117) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (118) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (12) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (13) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST
2016/02/05 13:34:58	I:\¥1¥コピー (14) ~ Eicar-string.txt	2016/02/05 13:27:02	EICAR test file	AVT_TEST

閉じる

リトマス 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リトマス 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。リトマス 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。



移動する隔離ファイルを選択して、[選択しているPCの隔離ファイルをリトマス USBへ移動]ボタンを押してください。

現在リトマスUSB2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

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフォルパス	隔離ファイル名	ファイルサイズ
2016/02/12 10:08:51	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160212100851_12f806c2.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥Eicar-string.txt	20160222114537_1cbea21e.zip	1KB
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ Eicar-string.txt	20160222114537_1cbea2f9.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (10) ~ コピー ~ Eic...	20160222114538_1cbea386.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ Eicar-string.txt	20160222114538_1cbea412.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (11) ~ コピー ~ Eic...	20160222114538_1cbea49f.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ Eicar-string.txt	20160222114538_1cbea51c.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (12) ~ コピー ~ Eic...	20160222114538_1cbea5a8.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ Eicar-string.txt	20160222114538_1cbea635.zip	1KB
2016/02/22 11:45:38	EICAR test file	AVT_TEST	I:\¥1¥コピー (13) ~ コピー ~ Eic...	20160222114538_1cbea6c2.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ Eicar-string.txt	20160222114539_1cbea74e.zip	1KB
2016/02/22 11:45:39	EICAR test file	AVT_TEST	I:\¥1¥コピー (14) ~ コピー ~ Eic...	20160222114539_1cbea7db.zip	1KB

PCの隔離ファイルを解凍して元に戻す

元に戻した隔離ファイル一覧

PCの隔離ファイルを削除

PCの隔離ファイルをリトマスUSB2へ移動

移動後、隔離ファイルがリトマス USB に保存されている場合、以下のメッセージが表示されます。

✓ LitmusUSB2 v110 (1, 1, 0, 110)

ツール 関連ソフト ヘルプ

デバイス情報

製品バージョン : v110 (1, 1, 0, 110)
 エンジンバージョン : 5800.7501.380116301
 定義ファイルバージョン : 8082 (2016/02/21)
 最終定義更新日 : 2016/02/22 11:32:27
 ライセンス有効期限 : 2016/05/25

スキャン設定

スキャンモード: カスタムスキャン
 スキャンタイプ: スキャン+ 即隔離
 起動タイプ: マニュアルスキャン
 除外設定: 無効

PC情報

コンピュータ名: K
 PC情報: 管理PCではありません
 ログファイル保存先: リトマスUSB2

お知らせ

現在、お知らせはありません。

お知らせ最終受信日時: 2016/02/22 11:29:48

スキャンのみ

スキャン+ 即削除

スキャン+ 即隔離

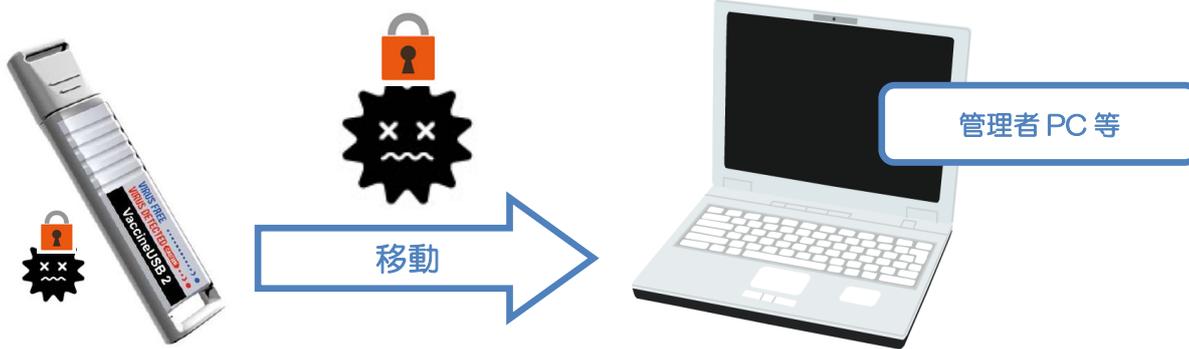
定義ファイル更新

リトマスUSB2を終了

リトマスUSB2内に隔離ファイルが保存されています。

リトマス USB に保存した隔離ファイルを PC へ移動する

リトマス 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。



移動する隔離ファイルを選択して、[選択しているリトマス 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。

↓

リトマスUSB2内に保存されている隔離ファイル一覧 空き領域 93 MB

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフルパス	隔離ファイル名	ファイルサイズ
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\#1\Eicar-string.txt	20160222114537_1cbea21e.zip	1KB

**リトマスUSB2内の隔離ファイルをPCへ保存
(解凍はしません)**

リトマスUSB2内の隔離ファイルを削除

閉じる

リトマス USB に保存した隔離ファイルを削除する

リトマス 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を選択して、[選択しているリトマス USB 内の隔離ファイルを削除]ボタンを押してください。

↓

リトマスUSB2内に保存されている隔離ファイル一覧 空き領域 93 MB

検出日時	ウイルス名	ウイルス種類	ウイルスが存在したフルパス	隔離ファイル名	ファイルサイズ
2016/02/22 11:45:37	EICAR test file	AVT_TEST	I:\#1\Eicar-string.txt	20160222114537_1cbea21e.zip	1KB

リトマスUSB2内の隔離ファイルをPCへ保存
(解凍はしません)

リトマスUSB2内の隔離ファイルを削除

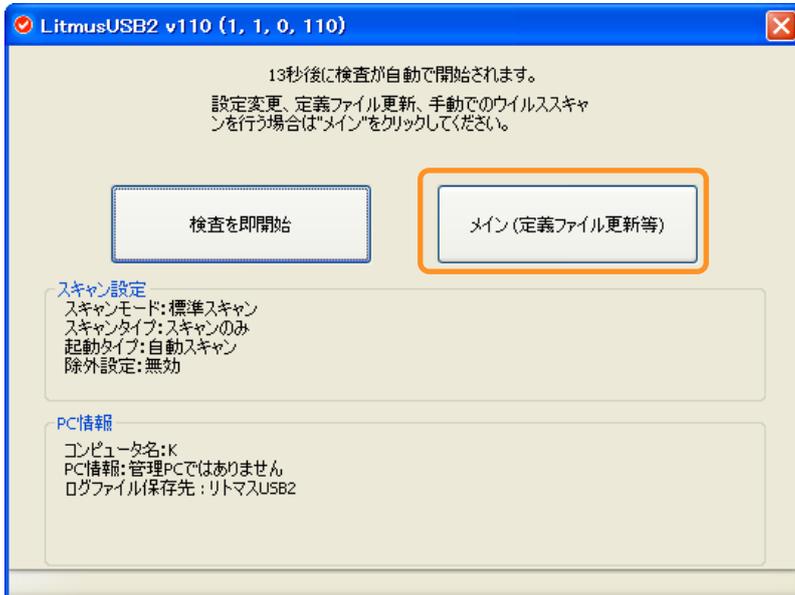
閉じる

8 機能設定を変更する

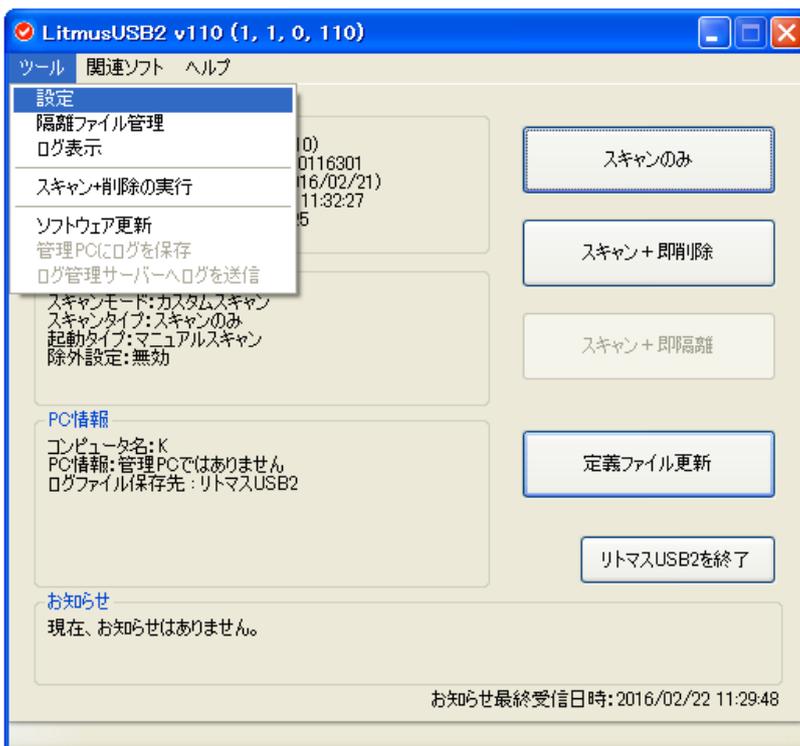
リトマス USB2 の機能設定を変更することができます。

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。

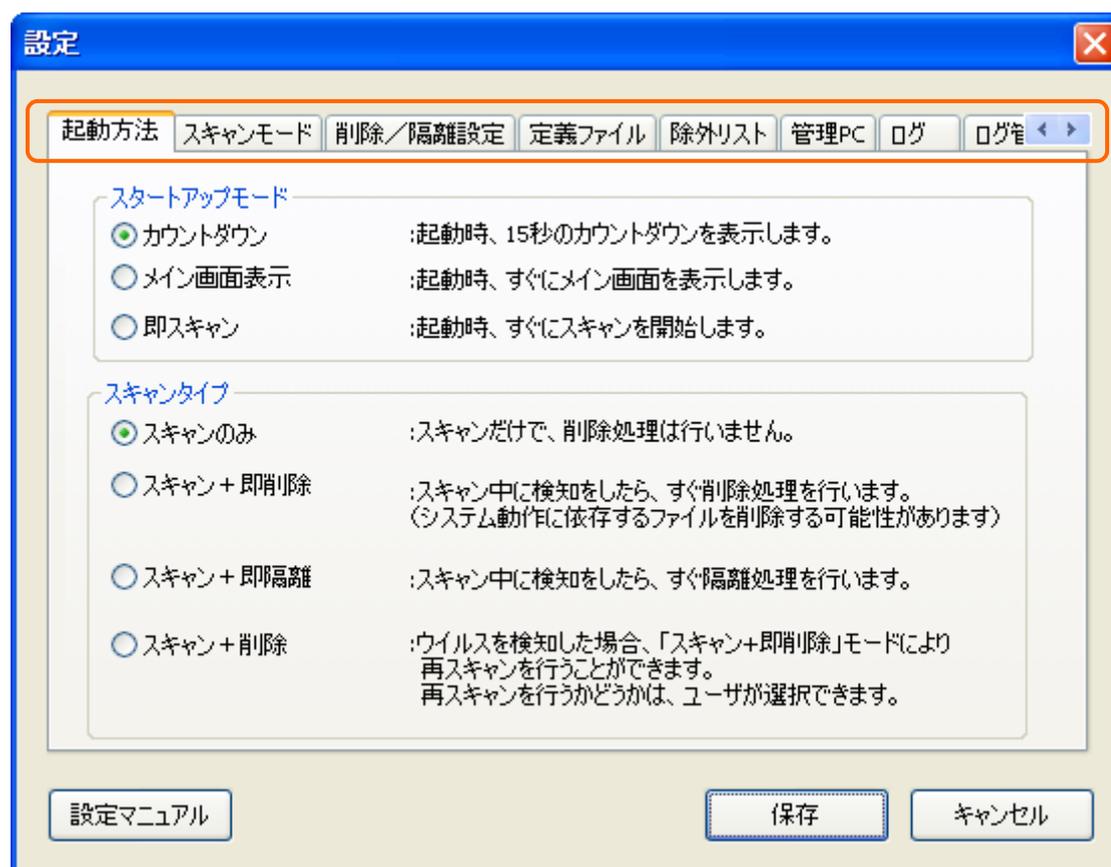


2.ツールバーの[ツール]を選択し、[設定]をクリックしてください。



ウイルス定義ファイルを更新する際、リトマス USB2 への書き込み制限を解除します。
書き込み制限を解除するとリトマス USB2 自身にウイルスに感染するリスクが発生します。
必ず最新パターンのウイルス対策製品がインストールされている PC で実行してください。

3.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	リトマス USB2 起動時の動作を設定することができます。
スキャンモード	リトマス USB2 スキャンモードを設定することができます。
削除/隔離設定	メイン画面の削除ボタンか隔離ボタンどちらを有効にするか設定することができます。
定義ファイル	定義ファイルの取得先を設定することができます。
除外リスト	スキャンを除外するファイル、フォルダ、拡張子を設定することができます。
管理 PC	管理 PC の設定を行うことができます。
ログ	ログの保存設定を行うことができます。
ログ管理	ログ管理サーバーの設定を行うことができます。
画面	リトマス USB2 の画面設定を行うことができます。
ユーザー	PC の権限/ユーザーに関する設定を行うことができます。
お知らせ	弊社からのお知らせに関する設定を行うことができます。

 NOTE

- 設定を保存する場合は、管理者の許可を得てください。
- 設定変更の際にリトマス USB2 へのウイルス感染リスクがございます。必ず最新パターンのウイルス対策製品がインストールされている PC で行ってください。

■タブ：起動方法

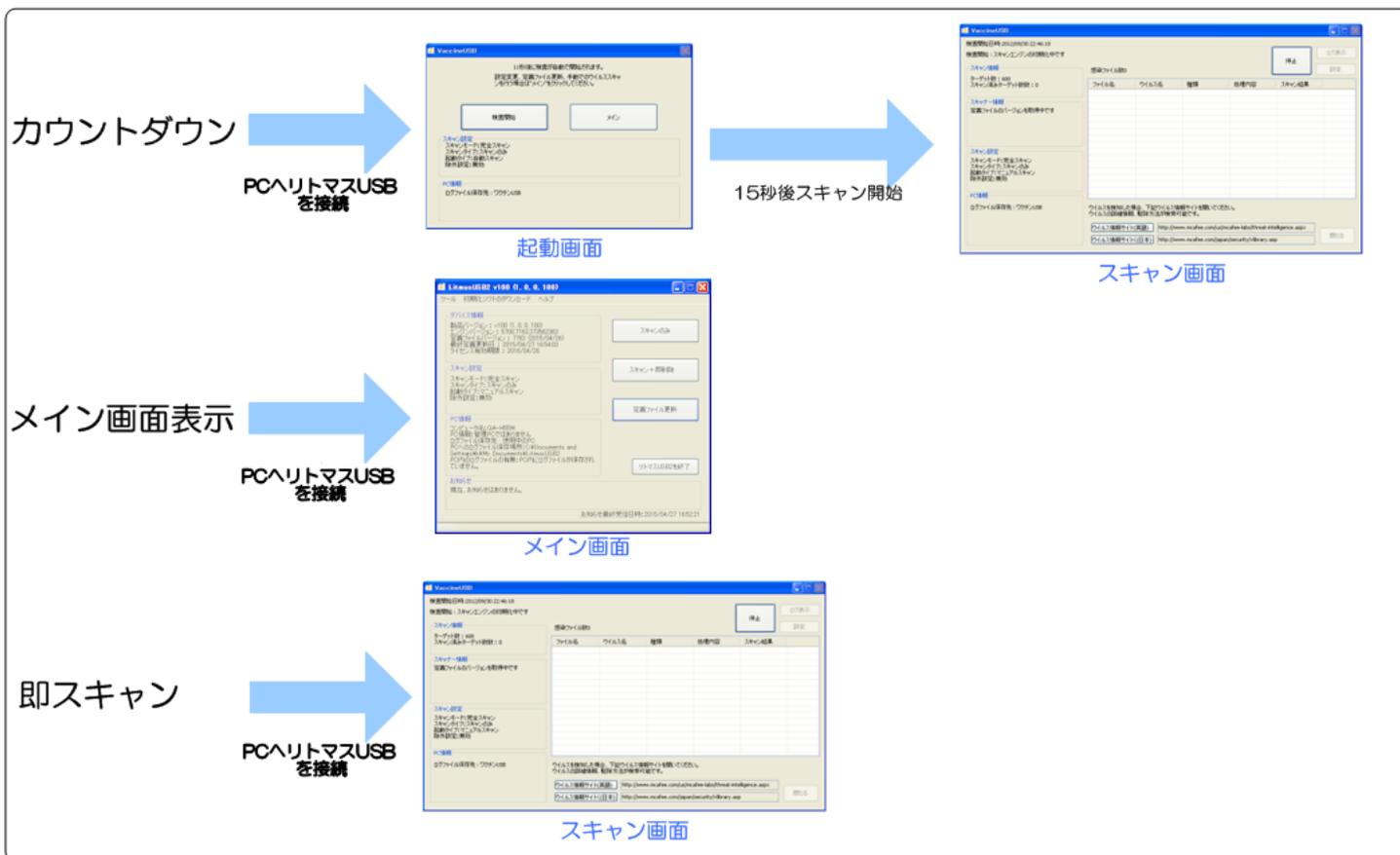
■スタートアップモード

リトマス USB2 起動時の動作を設定することができます。

スタートアップモード

- カウントダウン : 起動時、15秒のカウントダウンを表示します。
- メイン画面表示 : 起動時、すぐにメイン画面を表示します。
- 即スキャン : 起動時、すぐにスキャンを開始します。

- ・ **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。



■タブ：起動方法
 ■スキャンタイプ

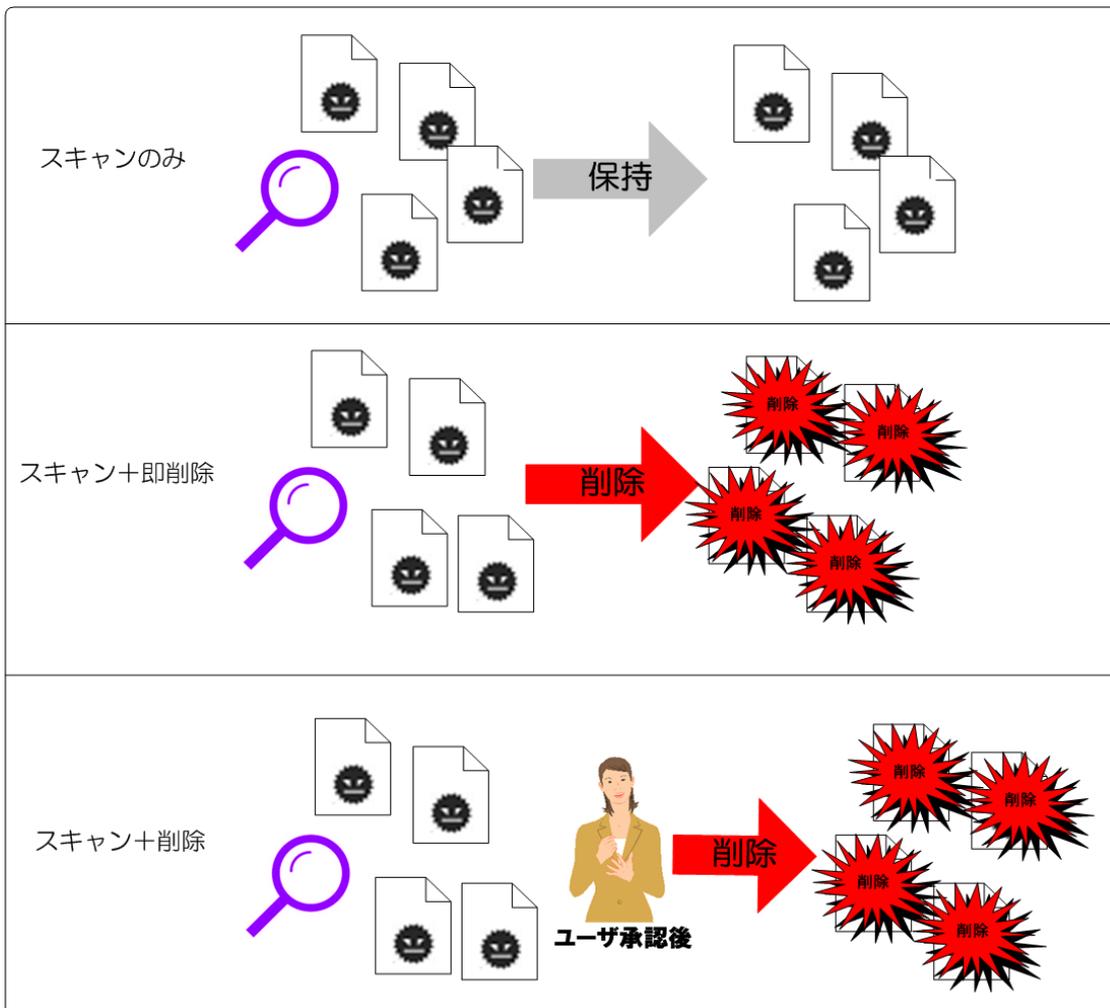
リトマスSB2のウイルススキャンのタイプを選択することができます。

スキャンタイプ

- スキャンのみ :スキャンだけで、削除処理は行いません。
- スキャン+即削除 :スキャン中に検知したら、すぐ削除処理を行います。
(システム動作に依存するファイルを削除する可能性があります)
- スキャン+削除 ウイルスを検知した場合、「スキャン+即削除」モードにより再スキャンを行うことができます。
再スキャンを行うかどうかは、ユーザが選択できます。

項目	内容
スキャンのみ	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。
スキャン+削除	ウイルス検知を1度行い、ウイルス検知終了後、ウイルスが発見されるとウイルスファイルリストを表示します。ユーザー承認後にウイルス感染したファイルを削除します。

まず[スキャンのみ]を選択しウイルススキャンを行なって頂き、そのウイルスが削除・隔離しても問題無い事を確認して頂いた後に、[スキャン+即削除]または[スキャン+即隔離]をして頂くことを推奨致します。



■タブ：スキャンモード

■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。

スキャンモード

- 完全スキャン :認識しているドライブ全て検査します。
- 標準スキャン :感染率が高い場所を指定して検査することができます。
- 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・USBメモリ・FDDを検査します。
- カスタムスキャン :スキャン場所を選択して調査することができます。
- 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。

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
標準スキャン	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。

スキャンリスト

C:¥386¥

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ォ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。

■タブ：削除/隔離設定

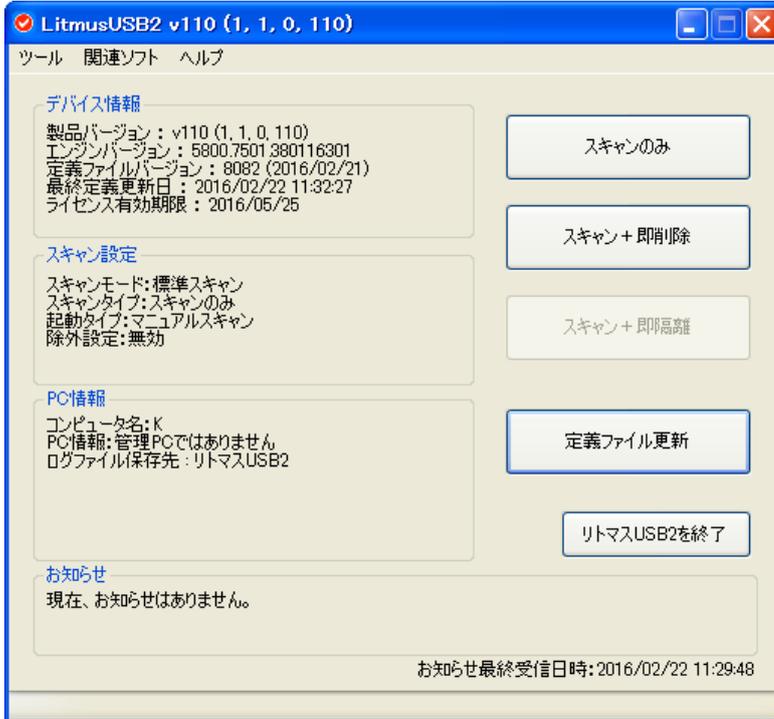
メイン画面で有効にするボタンを設定します。[スキャン+即削除]、[スキャン+即隔離]のどちらかを選択できます。同時に両ボタンを有効にすることはできません。

削除/隔離設定

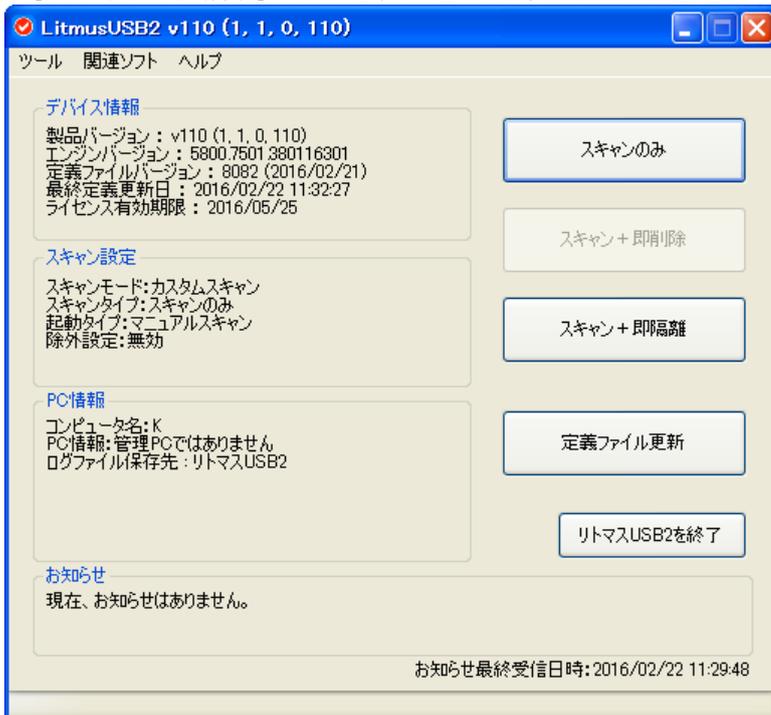
メイン画面で有効にするボタンを選択します。標準設定は[スキャン+即削除]です。

- メイン画面の[スキャン+即削除]ボタンを有効化
- メイン画面の[スキャン+即隔離]ボタンを有効化

■[スキャン+即削除]ボタンを有効化した場合のメイン画面



■[スキャン+即隔離]ボタンを有効化した場合のメイン画面



■タブ：定義ファイル

■定義ファイル更新方法

定義ファイル更新方法

- 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またはLocal Updater経由で定義ファイルを更新します
- ローカルネットワークを使用して、LocalUpdaterから定義ファイルを更新します

LocalUpdaterで設定した定義ファイル保存先の共有フォルダパスを入力してください。
 入力例：\\¥192.168.0.1¥LocalUpdate

- インターネット経由またはMcAfee VirusScan Enterpriseから定義ファイルを更新します
- McAfee VirusScan Enterpriseから定義ファイルを更新します

[LocalUpdaterをダウンロード](#)

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。
インターネット経由または Local Updater 経由で定義ファイルを更新します	インターネットまたはLocal Updaterで定義ファイルをダウンロードします。
ローカルネットワークを使用して、Local Updater から定義ファイルを更新します。	Local Updater から定義ファイルをダウンロードします。
インターネット経由または McAfee VirusScan Enterprise から定義ファイルを更新します。	PCにインストールされているMcAfee VirusScan Enterpriseが持っている定義ファイルまたはインターネットで定義ファイルをダウンロードします。
McAfee VirusScan Enterprise から定義ファイルを更新します。	McAfee VirusScan Enterpriseが持っている定義ファイルをダウンロードします。
LocalUpdater をダウンロード	定義ファイル中継ソフトウェア「ローカルアップデータ」ダウンロードサイト(web)へ移動します。

※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。
 本ソフトウェアの詳細ならびにご提供方法につきましては、別途ご案内いたします。

■タブ：除外リスト
 ■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・フォルダ・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。

■タブ：管理 PC

■リトマス USB2 への動作制限

管理 PC 以外の PC でリトマス USB2 の動作制限を掛けることができます。ユーザー様に設定変更等を禁止したい場合にご使用ください。

リトマスUSB2への動作制限

管理PC以外のPC上でのリトマスUSB2動作制限を設定します。

- 設定変更などの動作制限をかけます
- 設定変更などの動作制限をかけません

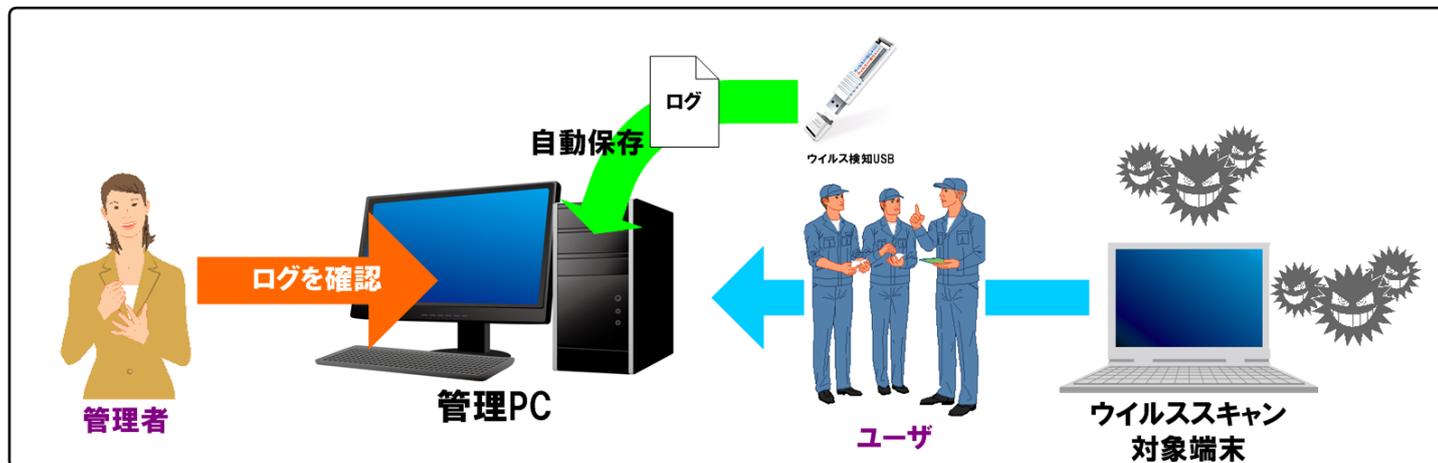
管理PC設定ソフトウェアを開く

項目	内容
動作制限をかける	管理 PC 以外の PC 上で以下の動作制限をかけます。 <ul style="list-style-type: none"> ソフトウェア更新 設定変更 ログファイルの出力/ログファイルの削除
動作制限をかけない	動作制限をかけません。
管理 PC 設定ソフトウェアを開く	管理 PC 設定ソフトウェアが格納されているフォルダへ移動します

■管理 PC ログファイル設定

管理 PC 用に自動的にログを保存するかどうかを設定することができます。

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。



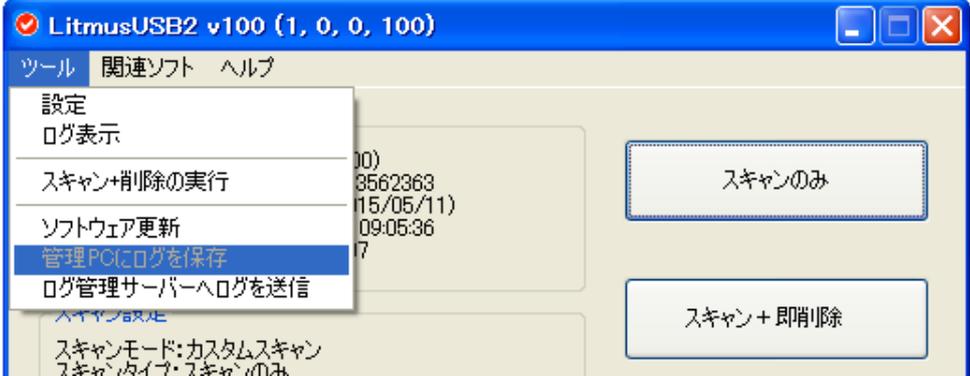
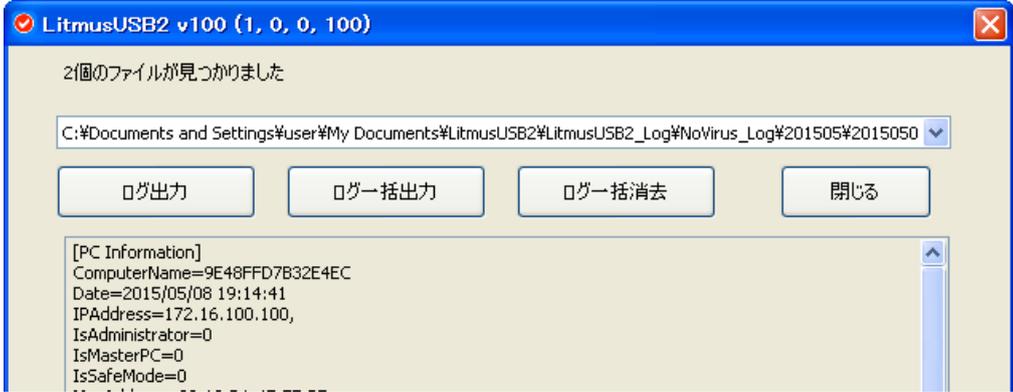
管理PCログファイル設定

管理PCに自動的にログを保存することができます。

- 管理PC用ログを作成しません
- 管理PC用ログを作成します

項目	内容
管理 PC 用ログを作成しません	管理 PC 用ログをリトマス USB2 内に作成しません。
管理 PC 用ログを作成します	管理 PC 用ログをリトマス USB2 内に作成し、管理 PC へ自動的にログを保存します。

■ その他詳細事項

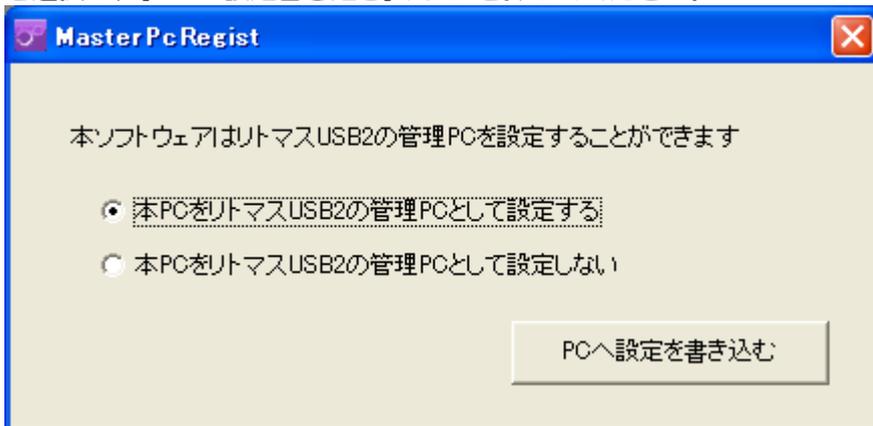
項目	内容
管理 PC へのログ送信タイミング	<ul style="list-style-type: none"> ウイルス定義ファイル更新後 ウイルススキャン処理終了後 メイン画面→ツール→[管理 PC にログを保存]ボタンを押した時 
管理 PC へのログの保存場所	<p>ログインユーザーの My Documents¥AdminLitmusUSB2_Log フォルダの下です。</p> <p>※ 環境変数を実際のパス： %USERPROFILE%¥My Documents¥AdminLitmusUSB2_Log</p> <p>ログファイルは以下のフォルダに分けられ保存されます。 AdminLitmusUSB2_Log¥*****¥@@@¥ログファイル</p> <ul style="list-style-type: none"> *****：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リトマス USB2 内の管理 PC ログ	管理 PC へログファイルを送信後、送信に成功したリトマス USB2 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 ログはリトマス USB2 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。
リトマス USB2 内の管理 PC 用ログ削除方法	<p>リトマス USB2 のログ画面から[ログ一括消去]を押してください。</p> <p>※通常のログも削除されるのでご注意ください。</p> 
リトマス USB2 内に管理 PC 用ログ有無の確認方法	<p>リトマス USB2 のログ画面に下部に表示されます。</p> <p>ログ管理サーバー用ログファイル：なし 管理PC用ログファイル：なし</p>

■管理 PC の設定方法

管理 PC を設定するには管理 PC 設定ソフトウェアを使用してください。

[管理 PC 設定ソフトウェアを開く]ボタンで管理 PC 設定ソフトウェアが格納されているフォルダへ移動します。

管理 PC へ設定する PC 上で管理 PC 設定ソフトウェアを実行し、[本 PC をリトマス USB2 の管理 PC として設定する]を選択し、[PC へ設定書き込む]ボタンを押してください。



以下の OS/権限では管理 PC を設定しないでください。ログを保存することができません。

対象 OS/権限	<ul style="list-style-type: none">• Windows2000 /管理者権限を持っていないユーザー• WindowsXP /管理者権限を持っていないユーザー• Windows2003 Server /管理者権限を持っていないユーザー• Windows2003 ServerR2 /管理者権限を持っていないユーザー
----------	---

■タブ：ログ

■ログファイル保存設定

リトマス USB のログ保存先を設定します。

ログファイル保存設定

- ログをリムーバブルディスク内に保存します。(非推奨)
*リトマスUSB2がウイルス感染する可能性があります。
- リトマスUSB2の秘匿領域へログを保存します(強く推奨)
リトマスUSB2はウイルス感染しません。
WindowsXPの制限ユーザーではPCへ保存します
- ログ領域が少なくなったら、警告を表示します。

PCへのログファイル保存設定(リトマスUSB2内へログ保存ができない場合)

- ログをPCへ保存する場合、強制的にログを保存します
- ログをPCへ保存する場合、確認メッセージを表示します
- PCへはログを保存しません

スキャンエラーの記載

- スキャンできないファイルをエラーとしてログへ記載する
- スキャンできないファイルをエラーとしてログへ記載しない

項目	内容
ログをリムーバブルディスク内に保存します(非推奨)	ログをリトマス USB のリムーバブルディスクへ保存します。ログ保存時にリトマス USB へウイルス感染する可能性があるので推奨いたしません。
リトマス USB の秘匿領域へログを保存します(強く推奨)	ログをリトマス USB の秘匿領域へ保存します。ログ保存時もウイルス感染しません。WindowsXP の制限ユーザーでは PC へログを保存します。
チェックボックス ログ領域が少なくなったら、警告を表示します。	ログ保存領域の空き容量が少なくなった場合、警告を表示するかを設定します。

以下の OS/権限ではリトマス USB 内にログを保存することができません。

対象 OS/権限	<ul style="list-style-type: none"> • WindowsXP /管理者権限を持っていないユーザー • Windows2003 Server /管理者権限を持っていないユーザー • Windows2003 ServerR2 /管理者権限を持っていないユーザー
----------	---

上記環境ではログを PC へ保存します。その時の処理について設定を行うことができます。

PCへのログファイル保存設定(ワクチンUSB内へログ保存ができない場合)

- ログをPCへ保存する場合、強制的にログを保存します
- ログをPCへ保存する場合、確認メッセージを表示します
- PCへはログを保存しません

• ログを PC へ保存する場合、強制的にログを保存します

対象 OS/権限でウイルススキャンを終了した後に強制的に PC へログを保存します。
保存場所は「Documents and Settings¥user 名¥My Documents¥LitmusUSB2」フォルダです。

• ログを PC へ保存する場合、確認メッセージを表示します

対象 OS/権限でウイルススキャンを終了した後に以下のメッセージが表示され PC へログを保存するか選択することができます。



[はい]を選択した場合、ログがPCへ保存されます。

保存場所は「Documents and Settings¥user 名¥My Documents¥LitmusUSB2」フォルダです。

- **PCへはログを保存しません**

対象 OS/権限でウイルススキャンを行った場合であっても、PCへログを保存しません。

PCへログを残したくないユーザー様は本項目を選択してください。

■スキャンエラーの記載

リトマス USB 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。

※ver110 以降の標準は「スキャンできないファイルをエラーとしてログへ記載しない」です。

■タブ：ログ管理

■PC へのログファイル保存設定

InfoBanker(別売り)/SKYSEA Client View(別売り)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、リトマス USB2 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。

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なくなります。



設定画面

ログ管理サーバー設定

InfoBankerを使用します

ログ管理サーバー設定

ログ管理サーバーのIPアドレスを入力してください。
入力例：127.0.0.1

項目	内容
ログ管理サーバー設定	ログをどこに送信するか設定してください。 <ul style="list-style-type: none"> • ログ管理サーバーを使用しません：ログを送信しません。 • Info Banker を使用します：Info Banker へログを送信します。 • SkySea C/V を使用します：SKYSEA Client View へログを送信します。
ログ管理サーバー設定	Info Banker/LogManager/SKYSEA Client View(管理サーバ)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。

送信するログの種類

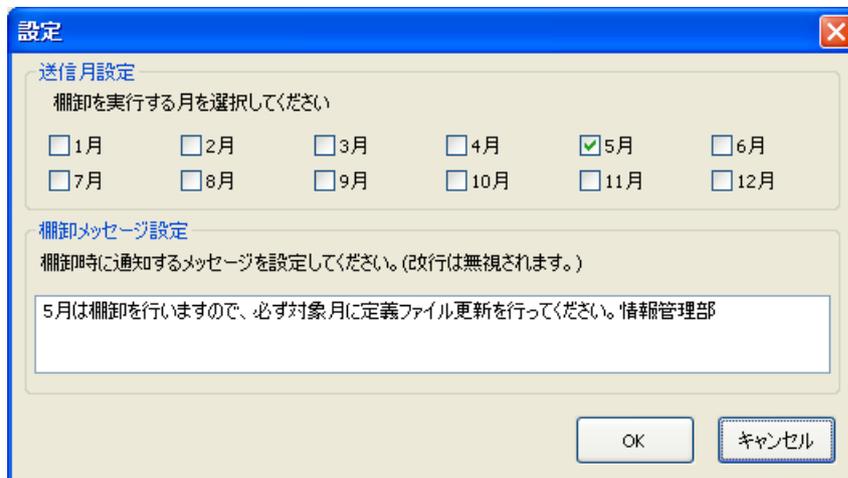
通常ログ

ウィルス検知ログ

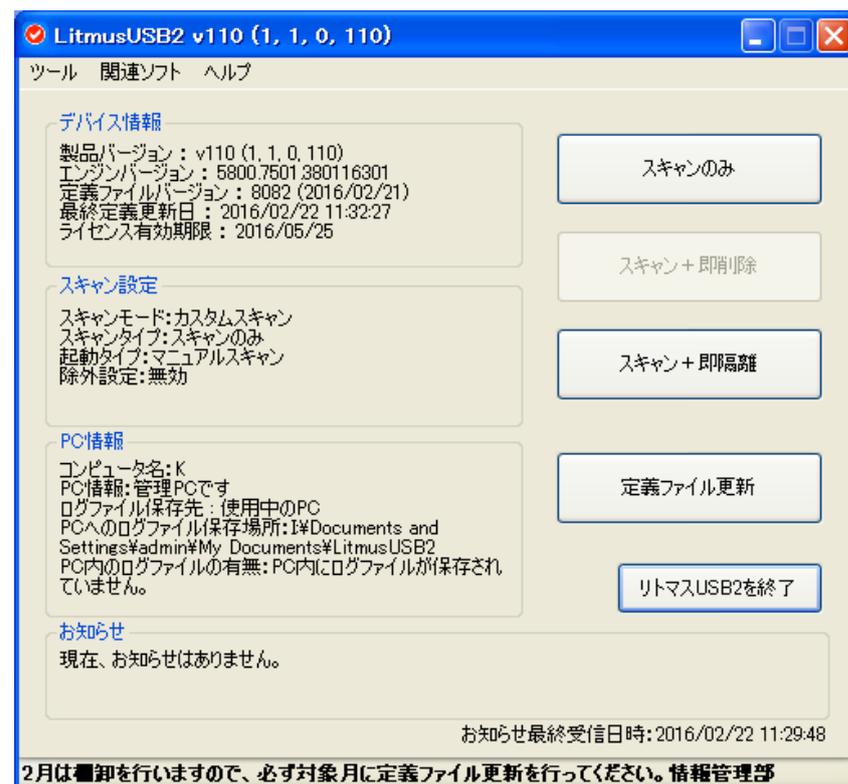
欄卸ログ

Info Banker への送信ログ設定 各ログ詳細については Info Banker のマニュアルをご確認ください。
 ※SKYSEA Client View では通常ログ、ウイルス検知ログ、棚卸しログはございません。

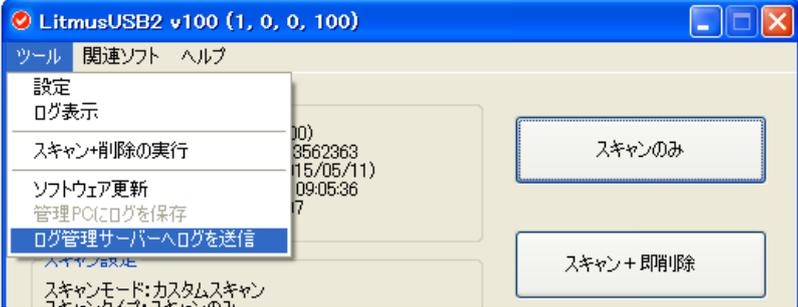
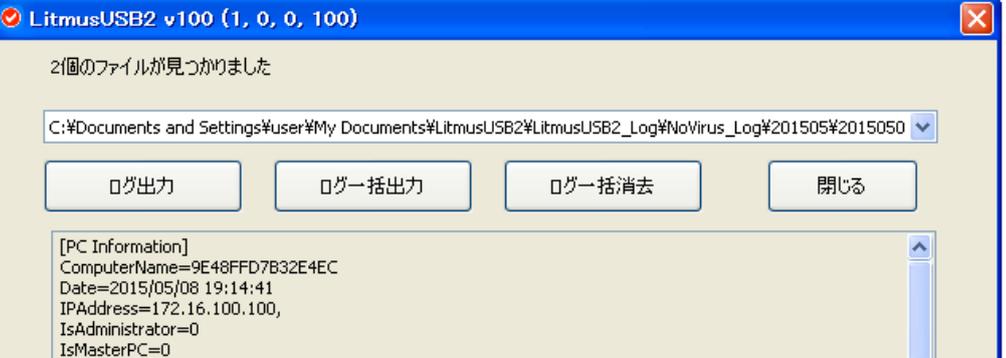
項目	内容
通常ログ	リトマス USB2 が毎回取得するログを送信します。
ウイルス検知ログ	リトマス USB2 がウイルスを検知したログのみ送信します。
棚卸ログ	棚卸に使用するログを送信します。 棚卸ログ詳細設定ボタンを押すと、棚卸を行う月、対象月にユーザーに表示するメッセージを設定できます。



メッセージ表示例※棚卸設定した月のみ表示されます



■ その他詳細事項

項目	内容
<p>ログ送信タイミング</p>	<ul style="list-style-type: none"> 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 [ログ管理サーバーへログを送信]ボタンを押した時 
<p>InfoBanker/LogManager/SKYSEA Client View 用ログの内容</p>	<p>InfoBanker/LogManager/ SKYSEA Client View の取扱説明書を御覧ください。</p>
<p>InfoBanker/LogManager/SKYSEA Client View へログを送信した後のログについて</p>	<p>InfoBanker/LogManager/ SKYSEA Client View へ ログファイルを送信後、送信に成功した リトマス USB 内のログは削除されます。</p>
<p>InfoBanker/LogManager/SKYSEA Client View 用ログの閲覧方法</p>	<p>InfoBanker/LogManager/ SKYSEA Client View 用ログはリトマス USB から閲覧することはできません。 InfoBanker/LogManager/ SKYSEA Client View へアクセスし閲覧してください</p>
<p>リトマス USB 内の InfoBanker/LogManager/SKYSEA Client View 用ログ削除方法</p>	<p>リトマス USB2 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。</p> 
<p>リトマス USB 内に InfoBanker/LogManager/SKYSEA Client View 用ログがあるかの確認方法</p>	<p>リトマス USB2 のログ画面に下部に表示されます。</p> <p>ログ管理サーバー用ログファイル：なし 管理PC用ログファイル：なし</p>

■タブ：画面

■画面の最前面表示

リトマス USB2 のウィンドウを最前面にするかどうかを設定できます。

画面の最前面表示

- 通常表示します
- リトマスUSB2を常に最前面に表示します

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リトマス USB2 の画面上に被せることが可能です。
リトマス USB2 を常に最前面に表示します	常に最前面にリトマス USB2 の画面を表示します。

■ユーザー

■権限昇格制御

制限ユーザーでは管理者に比べアクセスできる範囲が制限されており、それに伴いウイルススキャンできる範囲も狭くなります。Windows Vista 以降の OS で実行時に権限昇格画面を強制的に出し、容易に管理者としてご使用できるようにアシストする機能です。権限昇格にはそのアカウントの ID、パスワードが必要になります。

権限昇格制御

有効

無効

※有効の場合、Windows Vista以降のOSでは起動時にダイアログ(昇格画面)が表示されます。無効にすると本ダイアログは表示されなくなりますが、Windowsのシステムフォルダに存在するウイルスファイルを削除できません。

項目	内容
有効	Windows Vista 以降の OS で強制的に権限昇格画面を表示します。 ログインするアカウントを選択し、ID/パスワードを入力してください。 確認ダイアログが表示されるため自動実行できなくなります。 (ユーザーアカウント制御 (UAC) を OFF にすることで権限昇格した状態で自動実行が可能になります) 注意：管理者権限の ID/パスワードを知らない場合は、[有効]に設定しないでください。 有効の場合、ID/パスワードを入力しないと、リトマス USB2 は起動できません。
無効	権限昇格画面を表示しません。

■各種ボタン

各種ボタンについて説明致します。

設定マニュアル

保存

キャンセル

ボタン	内容
設定マニュアル	設定に関するマニュアルを開きます。マニュアルは PDF ファイルで作成されているため、PDF が閲覧できる環境で実行してください。
保存	設定をリトマス USB2 へ保存します。リトマス USB2 の電源を抜いても設定は保存されています。
キャンセル	設定を保存せず、設定画面を閉じます。

■タブ：お知らせ

■お知らせ

弊社からのお知らせを受信して、メイン画面に表示するかどうかを設定できます。

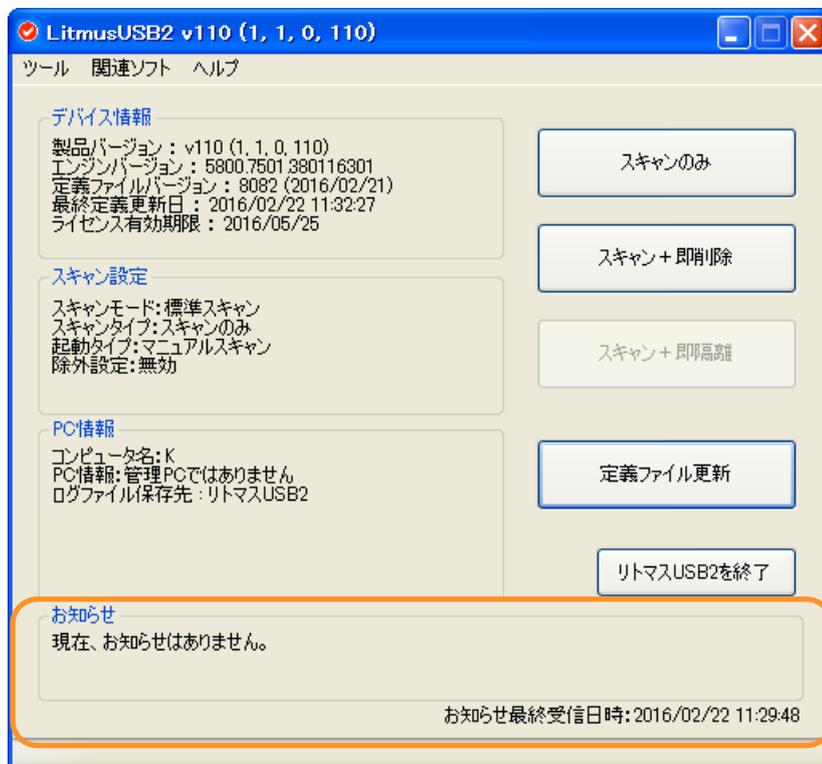
お知らせ

受信する
 受信しない

リトマスUSB2のアップデート情報や障害情報をリトマスUSB2のメイン画面に表示します。
お知らせは定義ファイル更新時に更新されます。

項目	内容
受信する	定義ファイル更新時に弊社のサーバーからお知らせを受信し、メイン画面に表示します。
受信しない	お知らせを受信しません。

お知らせは、下記の位置に表示されます。



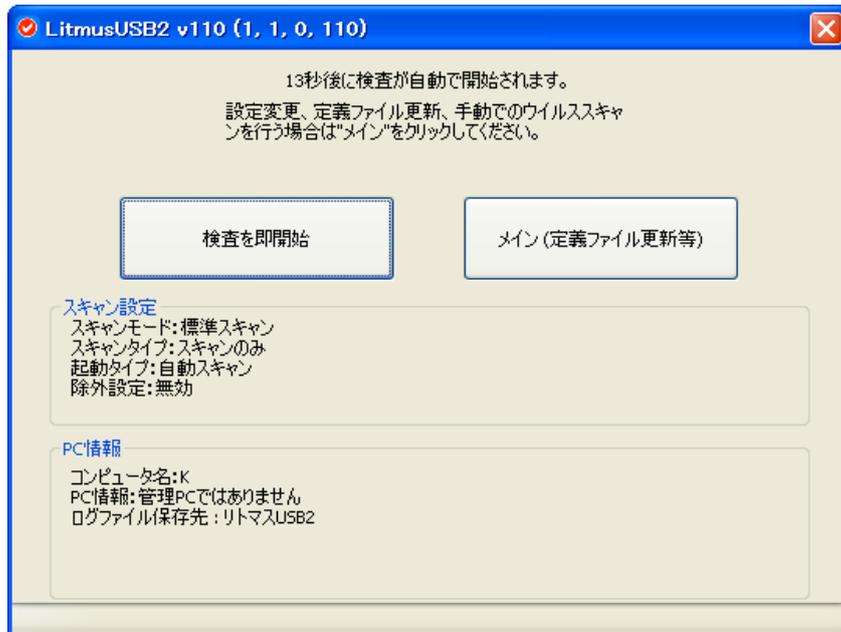
8 スキャンログを確認する

スキャンした結果（ログ）は、ログファイルとして保存します。ログファイルは、スキャンするたびに生成します。スキャンログファイルは、本製品内のリムーバブル領域とは別の場所に保存され、リトマス USB2 ソフトウェアからのみアクセス可能です。

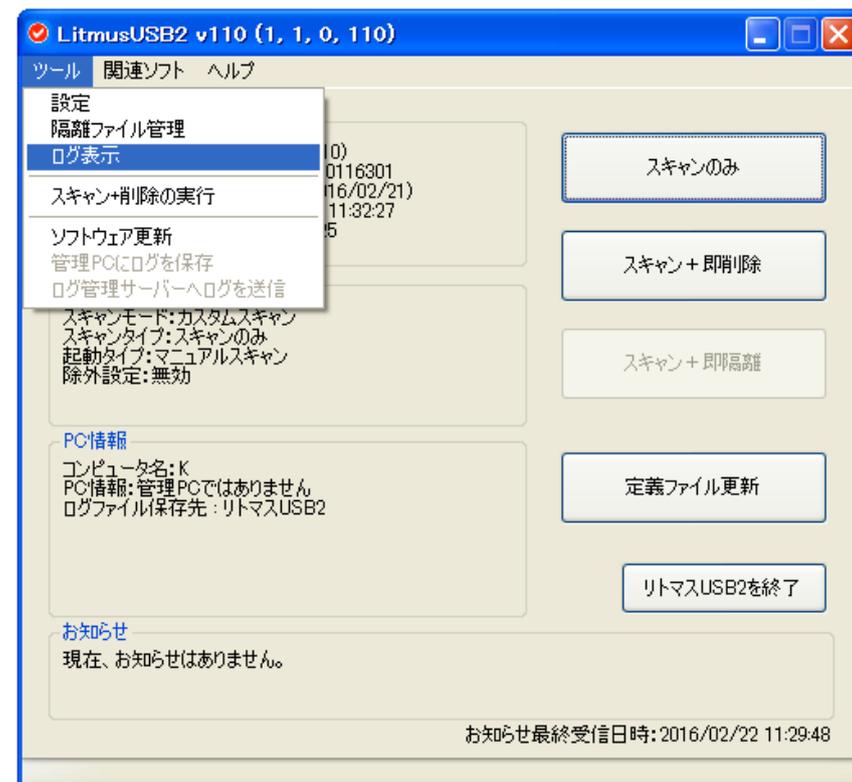
スキャンログファイルの確認は、以下の方法か、もしくはスキャン画面にある「ログ表示」ボタンをクリックすることで確認することができます。

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。

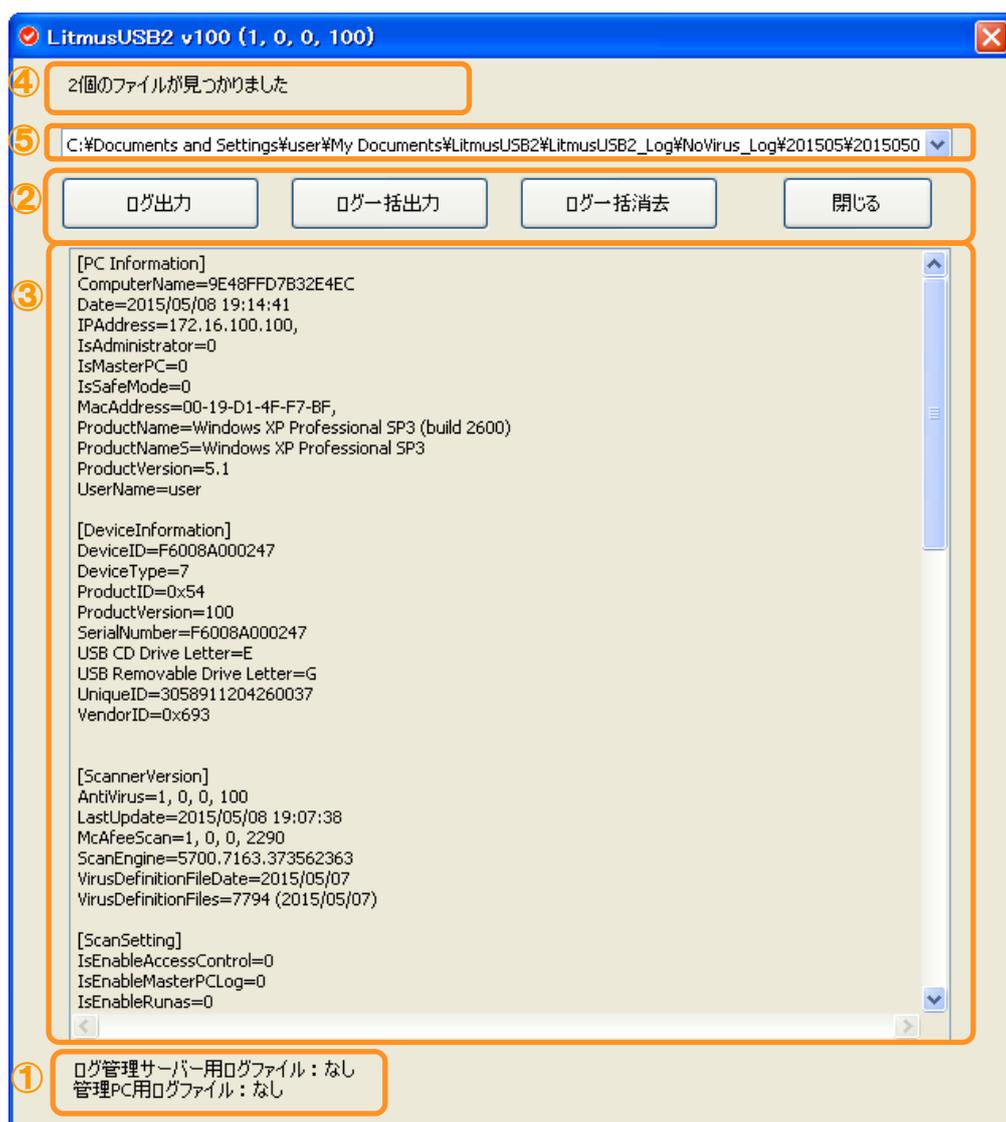
※この画面が表示され約 15 秒が経つと、自動的にスキャンが始まりますので、それまでに操作を行なってください。



2.ツールバーの[ツール]を選択し、[ログ表示]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します。

② ログファイル：表示するログファイルを選びます。

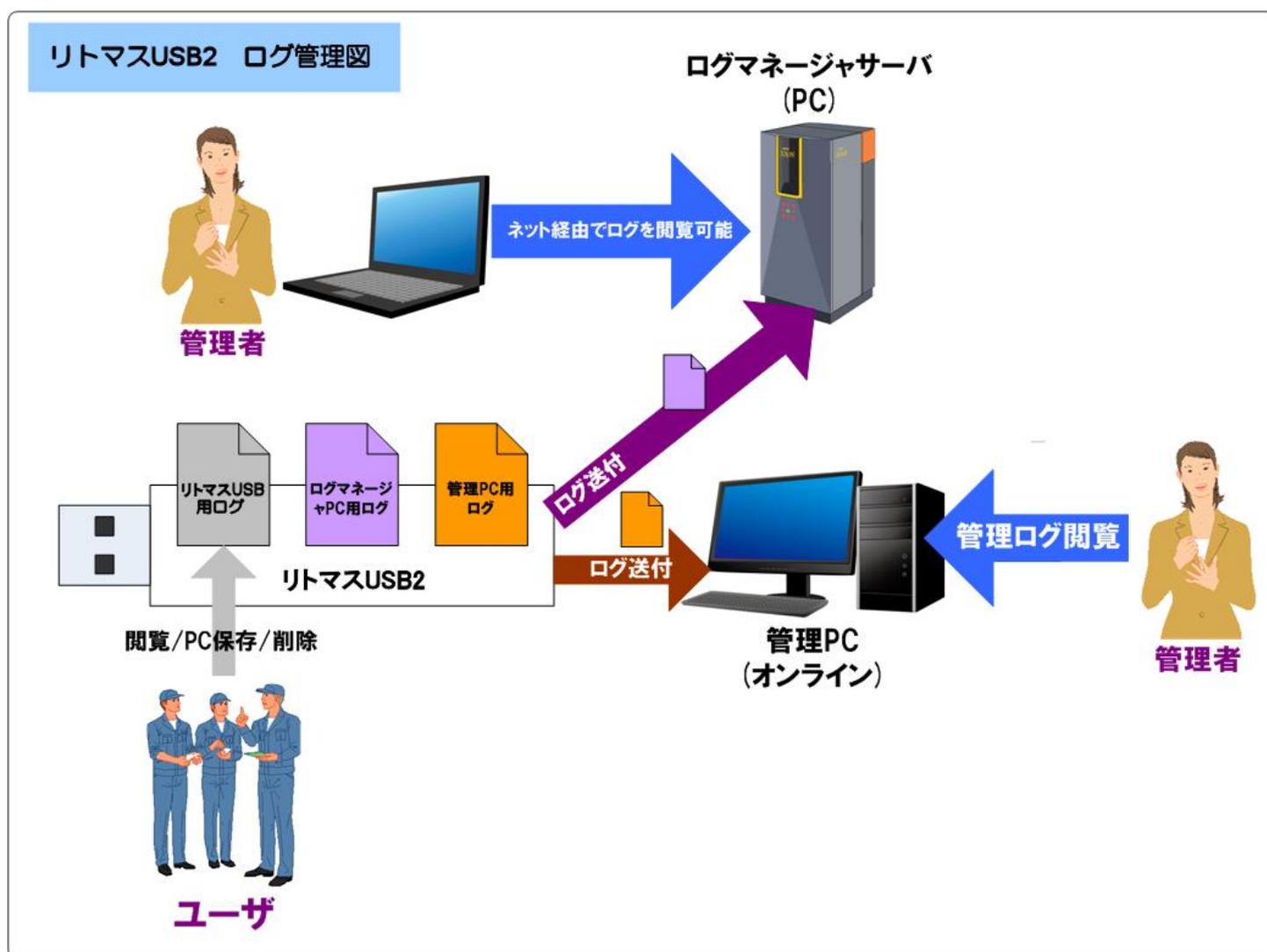
項目	内容
ログファイル名	YYYYMMDDHHMMSS_スキャンしたコンピュータ名.txt
ログ格納フォルダ	YYYYMM フォルダの下にウイルス有り/ウイルス無しで分けられ保存されます。 ウイルス有り：Virus_Log フォルダに格納 ウイルス無し：NoVirus_Log フォルダに格納 例：2012年9月にウイルススキャンを行い、ウイルス有りの場合の格納フォルダ フォルダ：LitmusUSB2_Log\¥Virus_Log¥201209

③ 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。 Info Banker 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。

④Info Banker/SKYSEA Client View 用ログファイルと管理 PC 用ログファイルがリトマス USB2 内にあるかを表示します。

ログ	役割	ログ内容	ログ保存を有効にする方法
通常のリトマス USB2 ログ	リトマス USB2内に保存するログです。	次の⑤に記載されているログファイル内容。3つの	本ログはリトマス USB2 の標準ログのため、自動的にログはリトマス USB2 内へ保存されます。
管理 PC 用ログ	管理 PC へ送信するためのログです。	ログとも同じ内容です。	リトマス USB2 の設定画面から[管理 PC ログファイル設定]で[管理 PC 用ログを作成する]を設定すると、管理 PC 用ログがリトマス USB 内に保存されるようになります。
ログ管理サーバー用ログ	Info Banker SKYSEA Client View へ送信するためのログです。		リトマス USB2 の設定画面から[ログ管理]で Info Banker/SKYSEA Client View を使用する設定にすると、ログ管理サーバーへ送信されるようになります。



- ⑤ 選択されたログファイルの内容を表示します。ログ内容は以下になります。
 ログファイル内容を以下に記載します。

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
HDD Capacity	HDD/SSD 容量
HDD Free Space	HDD/SSD 空き容量
RAM Size	メモリ容量
Workgroup	ワークグループ名
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
UserName	ログインユーザー名 (アカウント名)
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 (リトマス USB : 7 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	リトマス USB2 の CD ドライブのドライブレター 例 : E
USB Removable Drive Letter	リトマス USB2 のリムーベディスクディスクドライブのドライブレター 例 : G
UniquelD	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	リトマス USB2 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:有効 1:無効)
LogSaveType	PC へのログファイル保存設定 0:PC へはログを保存しない 1:ログを PC へ保存する場合、確認メッセージを表示する。 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 : 標準スキャン、 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 2:スキャン+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)
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[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	マカフィ社が規定しているウイルスの種類
VirusName	マカフィ社が規定しているウイルス名
CleanAction	弊社の管理項目
Result	ウイルススキャンの結果 <ul style="list-style-type: none"> • 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。
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

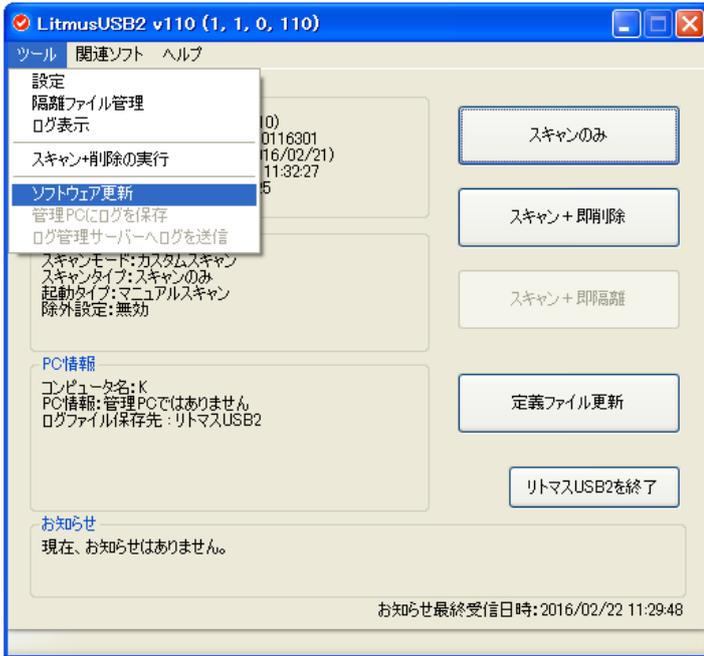
ScanErrorFiles	スキャンエラーの数
ScanResult	最終的なスキャン結果 • ウイルスなし : No Virus • ウイルスあり : Virus Found

9 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。

1. メイン画面から[ツール]メニューの[ソフトウェア更新]を選ぶ。指示に従い進めてください。

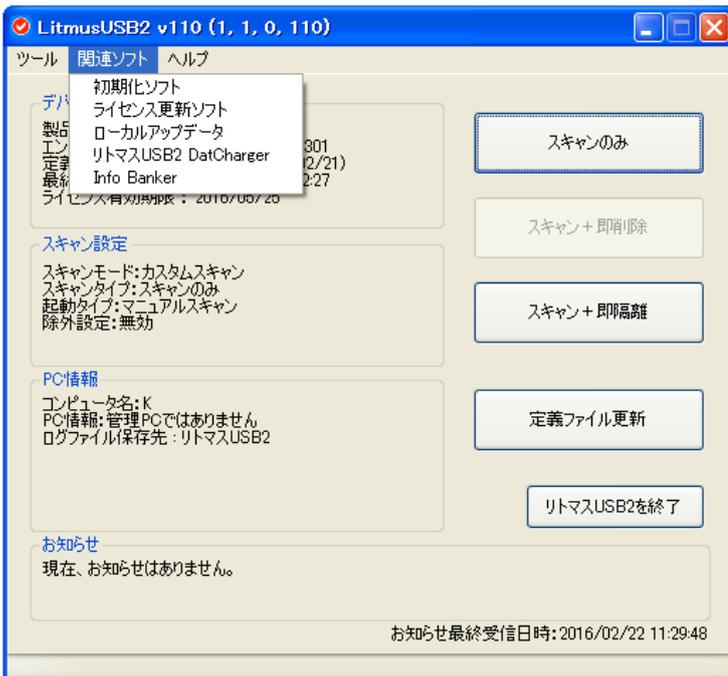


製品の初期化を行う

何かしらの原因でリトマス USB2 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。

注意：初期化を行うとログが削除されます。

1: メイン画面から[ツール]メニューの[関連ソフト]→[初期化ソフト]を選してください。HP に移動しますので、HP 内の指示に従い進めてください。



リトマス USB2 の関連ソフトのサイトへ移動する。

リトマス USB2 には以下の関連ソフトがあります。

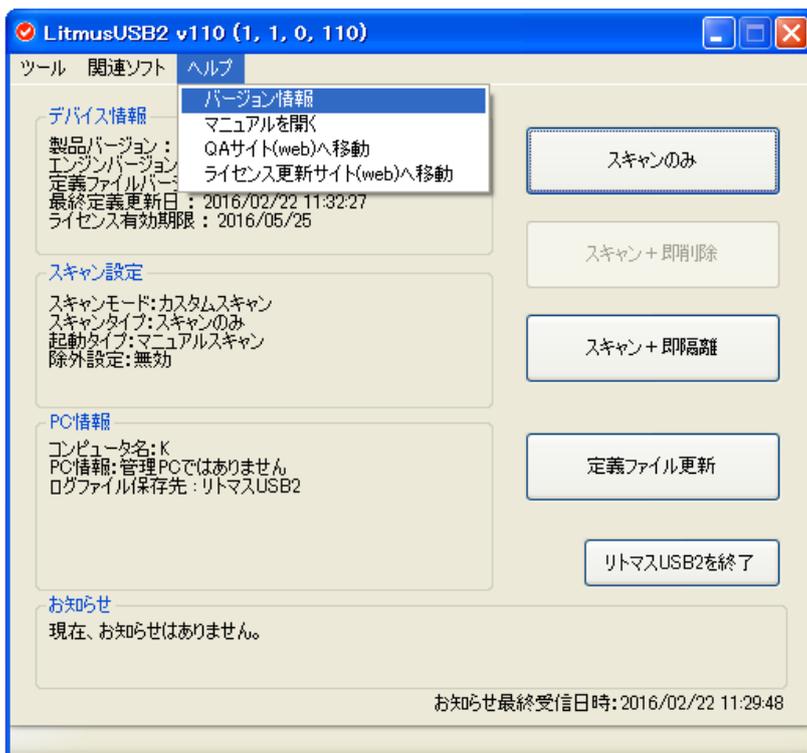
項目	概要
ライセンス更新ソフト	リトマス USB2 のライセンス更新するためのソフトウェアです。
ローカルアップデータ	リトマス USB2 の定義ファイル中継をするためのソフトウェアです。
リトマス USB2 DatCharger	リトマス USB2 を8台同時に定義ファイル更新ができる作業支援ソフトウェアです。 別売りの有償ソフトウェアになります。
Info Banker	リトマス USB2 が出力するログを収集、管理するサーバソフトウェアです。 収集したログを管理者がネットワーク経由で離れた場所から管理/確認することが可能です。 別売りの有償ソフトウェアになります。

メイン画面から[ツール]メニューの[関連ソフト]から各ソフトウェアを選んでください。各ソフトウェアの HP に移動します。

製品バージョン情報/更新履歴を表示する

使用中のウイルススキャンソフトの情報を表示します。

メイン画面から[ヘルプ]メニューの[バージョン情報]を選ぶ



2.使用中のウイルススキャンソフトの情報が表示されます。

- [更新履歴]ボタン : ウイルススキャンソフトの更新履歴を表示します。
- [OK]ボタン : 使用中のウイルススキャンソフトの情報を表示する画面を閉じます。



マニュアルを表示する

本製品のマニュアル（本ファイル）を表示します。

メイン画面から[ヘルプ]メニューの[マニュアル(Ver2:標準)を開く]を選ぶ

- ・ 本製品のマニュアルが表示されます。

メイン画面から[ヘルプ]メニューの[マニュアル(Ver1 互換画面版)を開く]を選ぶ

- ・ 本製品の Ver1 互換画面版のマニュアルが表示されます。

※ マニュアルは PDF ファイル形式です。PDF ファイルを閲覧できる環境が必要です。

本製品の QA サイト(web)を表示する

本製品の QA サイト(web)を表示します。

メイン画面から[ヘルプ]メニューの[QA サイト(web)へ移動]を選ぶ

- ・ 本製品の QA サイトへ移動します。

※ インターネットに接続できる環境が必要です。

本製品のライセンス更新サイト(web)を表示する

本製品のライセンス更新方法が記載されたライセンス更新サイト(web)を表示します。

メイン画面から[ヘルプ]メニューの[ライセンス更新サイト(web)へ移動]を選ぶ

- ・ 本製品のライセンス更新サイトへ移動します。

※ インターネットに接続できる環境が必要です。

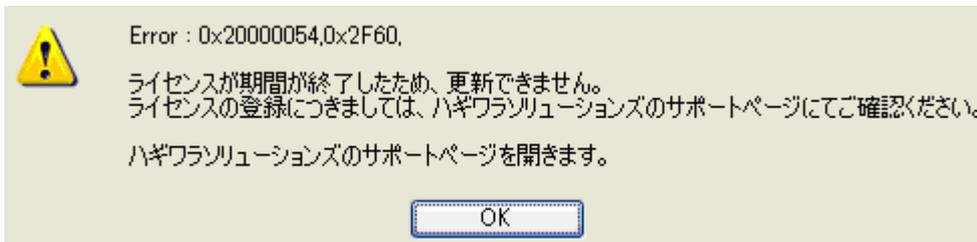
10 ウィルススキャンソフトのライセンスについて

ウィ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。

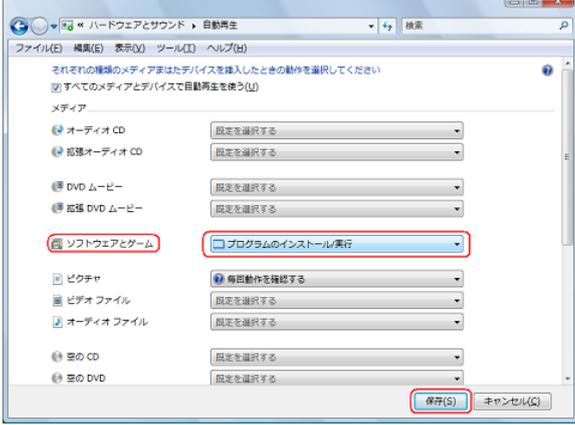
ライセンス有効期限切れ

ライセンス有効期限日を過ぎますと、以下の警告メッセージが表示されます。

ライセンスを更新する場合は、[OK]ボタンをクリックし、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。

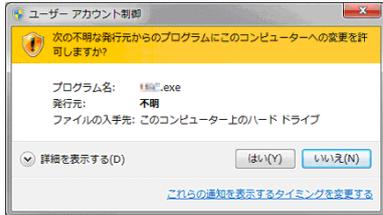


もしくはメイン画面から[ヘルプ]メニューの[ライセンス更新サイト(web)へ移動]をクリックしてください。

質問	回答
<p>Q1 本製品を PC の USB ポートに接続してもソフトウェアが自動起動しません。</p>	<p>A1 自動起動しない場合は「マイコンピュータ」→「LitmusUSB2」または「マイコンピュータ」→「REMOVABLE」の中の「StartUp.exe」をダブルクリックしてソフトウェアを実行してください。</p> <p>Windows Vista/Windows 7 でオートラン機能を有効にするには以下の設定が必要となります。</p> <ol style="list-style-type: none"> 1. 「スタート」→「コントロールパネル」をクリックします。  <ol style="list-style-type: none"> 2. 「ハードウェアとサウンド」から「CD または他のメディアの自動再生」をクリックします。  <ol style="list-style-type: none"> 3. 「ソフトウェアとゲーム」より「プログラムのインストール / 実行」を選択し、[保存] ボタンをクリックします。  <p>以上でオートラン機能の設定は完了です。</p>

質問		回答	
Q2	スキャン対象の機器が本製品を認識しません。	A2	<p>1. 対象機器に本製品が正しく挿入されていますか？ もう一度奥までしっかりと差し込んでください。</p> <p>2. ネットワークドライブをお使いの場合は、ドライブレター（マイコンピュータ上のドライブアイコンに割り当てられている文字）にご注意ください。Windows PC で本製品を使用する場合は、ネットワークドライブのドライブレターが本製品のドライブレターと重ならないようにネットワークドライブのドライブレターを変更するか、一時的にネットワークドライブの接続を解除してください。</p> <p>本製品を PC に接続すると、仮想 CD-ROM ディスクとリムーバブルディスクの 2 つのドライブが表示されます。お使いの PC の CD/DVD-ROM ディスクまたはハードディスクの最終のドライブレターから 2 つ使用します。例えば、C ドライブがハードディスク、D ドライブが DVD-ROM をお使いの場合、本製品は E ドライブと F ドライブを使用します。</p> <p>この状態でネットワークドライブを E ドライブや F ドライブに割り当てている場合、ネットワークドライブが優先されて表示されてしまうため、本製品で使用するドライブが表示されず、正しく動作できません。</p> <p>3. USB ハブ経由では使用できない場合があります。その場合は直接 PC に接続してください。</p>
Q3	本製品の取り付け、取り外しで再起動を要求されますが、再起動は必要ですか？	A3	<p>本製品を初めてセットアップした場合に限り、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、再起動メッセージの「いいえ」を選択してください。</p>
Q4	暗号化されたファイル、パスワードが掛かったファイルをウイルススキャンできますか？	A4	<p>暗号化されたファイル、パスワードが掛かったファイルのウイルススキャンはできません。</p>
Q5	プログラムエラーを示す、赤色 LED が点滅しました。	A5	<p>1. スキャン対象となる機器の動作環境（OS やメモリ容量等）が、本書に記載されている動作環境に該当するかご確認ください。</p> <p>2. ウイルススキャンソフトが実行できずにエラーになっている可能性があります。本製品を取り外して、再度接続してみてください。</p>
Q6	ウイルス定義ファイルはどのくらいの頻度で更新しますか？	A6	<p>1 日 1 回程度です。</p>
Q7	ウイルス定義ファイルの更新時間はどのくらいですか？	A7	<p>更新間隔(日)、通信環境によりますが、更新間隔が 1 日、国内内の標準的なネットワーク回線の場合、1 分程度掛かります。</p>
Q8	モニタとキーボードがない機器で取り外し操作ができません。スキャン終了後にアクセス LED（緑色）が点灯していますが、そのまま取り外しても問題ありませんか？	A8	<p>アクセス LED（緑色）が点滅していないことを確認してから取り外してください。</p>

質問		回答	
Q9	ネットワークドライブのスキャンが可能ですか？	A9	ネットワークドライブのウイルススキャンには対応しておりません。
Q10	PCに接続した場合に、CD-ROMアイコンが表示されなくなり、デバイスマネージャにHAGIWARA LitmusUSB Device が「！」マークで表示される。プロパティを開くとエラーコード 19, 31, 39, 41 等が表示されている。	A10	<p>【原因】 CD/DVDの書き込みプログラム、又は類似プログラムをアンインストールした場合に発生します。</p> <p>【対処法】</p> <ol style="list-style-type: none"> 1. スタートメニューからファイル名を指定して実行をクリックします。 2. regedit.exe と入力してOKをクリックしてレジストリエディタを開きます。 3. HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Class¥{4D36E965-E325-11CE-BFC1-08002BE10318}を開いて、UpperFilters というキーと LowerFilters というキーを選択して削除してください。 4. 再起動後にドライブアイコンが認識されます。
Q11	ライセンス期間が切れるとどうなりますか？	A11	ライセンス期間が切れると、定義ファイルへの更新ができなくなります。
Q12	リトマス USB2 は、PC 内へファイルを書き込みますか？	A12	ウイルス定義ファイル更新時、ソフトウェア更新時、圧縮ファイル内スキャン時に一時的に PC の temp フォルダ内に書き込みが発生しますが、アプリケーション終了時にすべて削除します。
Q13	「起動情報が見つかりません」と表示され、ウイルススキャンソフトが起動しません。	A13	REMOVABLE ディスクを認識していない可能性があります。再度挿し直して「マイコンピュータ」上に表示されているか確認してください。
Q14	「設定情報の取得に失敗しました」と表示され、ウイルススキャンソフトが起動しません。	A14	ウイルススキャンソフトに必要な設定データが壊れている可能性があります。お問い合わせ窓口までご連絡してください。
Q15	ウイルス定義ファイルの更新が成功しません。	A15	<p>ネットワークにアクセス制限、ファイルサイズ制限などなされていませんか？</p> <p>ウイルス定義ファイルのサイズは、約 130MB となります。ファイルサイズは日々増加していきます。</p> <p>また以下ドメインへのアクセス、ファイルダウンロードが許可されているか確認ください。</p> <p>http://www.udrw.com/ http://update.nai.com/ http://dl.hscjpn.co.jp/</p>
Q16	スキャンログファイルは、どこにありますか？	A16	<p>本製品内の特殊な場所に保存されております。そのため直接ログファイルを閲覧することはできません。本製品機能の「ログ表示」から確認してください。</p> <p>またログ表示機能より、ログファイルをユーザー任意の場所にテキストとして出力することはできます。</p>

質問		回答	
Q17	設定画面にある権限昇格制御とは何ですか？	A17	<p>ユーザーアカウント制御（UAC）という、Windows Vista 以降の OS から導入されたセキュリティ機能であり、ユーザーによる許可が無いソフトウェアをシステムに影響を与えない（アクセスできない）で動作させる仕組みのことです。</p> <p>起動時に権限昇格確認表示の有効/無効設定ができます。設定を反映させるには、ウイルススキャンソフトの再起動が必要となります。</p> <p>起動時に権限昇格をすることで、管理者権限を持った状態でソフトウェアを動作させることができます。ウイルスの削除を完全に行なうには設定は有効のままにしておくことをお勧めします。</p> <p>無効の場合は昇格しません。</p> 

12 サポート・メンテナンス・ライセンス

サポート・メンテナンスの内容

項目	サポート・メンテナンスの内容
製品	リトマス USB2
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。
サポート期間	リトマス USB2 ライセンスの契約期間内*1
保証期間(ハードウェア本体 ライセンス期間)	HUD-MVDT1A：1年 HUD-MVDT3A：3年 HUD-MVDT5A：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時～19時（年中無休）

※ナビダイヤル：

全国の固定電話から1分間10円の通話料（発信者負担）でご利用いただける「全国统一番号」で、NTTコミュニケーションズ株式会社が提供するサービスのひとつです。

ダイヤルQ2などの有料サービスではなく、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。

- ・携帯電話からは20秒10円の通話料でご利用いただけます。
- ・PHS・一部のIP電話からはご利用いただけません。
- ・お待ちいただいている間も通話料がかかりますので、混雑時はしばらくたってからおかけ直してください。

※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、原子力施設の稼働、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「ハイスリスク活動」という）が含まれますが、これに限定されません。マカフィ及び弊社は、明示/黙示を問わず、ハイス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。
- ・本書の著作権は弊社に帰属します。弊社に無断で本書の一部または全部を複製、転載、改変することは禁じられています。

- ◆ 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 1261757 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 ™ マークは明記していません。
- ◆ 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

リトマス USB2 取扱説明書
2016年2月
発行 ハギワラソリューションズ株式会社