

Quick Heal®

Security Simplified

ユーザーガイド

Quick Heal Total Security
Quick Heal AntiVirus Pro
Quick Heal Internet Security
Quick Heal AntiVirus Server Edition
Quick Heal Internet Security Essentials

Quick Heal Technologies (P) Ltd.
<http://www.quickheal.co.jp>

著作権情報

Copyright © 2014 Quick Heal Technologies (P) Ltd. All Rights Reserved.

本書のいかなる部分も、事前に Quick Heal Technologies (P) Ltd. (603 Mayfair Towers II, Wakdewadi, Shivajinagar, Pune-411 005, India) の許可を得ることなく、形態を問わず模造、複製または変更してはならず、いかなる情報検索システム、電子またはその他のメディアに組み込んではならず、いかなる形態であっても伝送してはなりません。

Quick Heal Technologies (P) Ltd. の許可を得ないマーケティング、配布または使用は法的責任を問われます。

この文書は公開日時点のものであり、Quick Heal によって随時変更される可能性があります。

商標

Quick Heal および DNAScan は、Quick Heal Technologies (P) Ltd. の登録商標であり、Microsoft および Windows は Microsoft Corporation の登録商標です。その他のブランドおよび製品の名称は各所有者の商標です。

エンドユーザー使用許諾契約書 (EULA)

QUICK HEAL ANTIVIRUS SECURITY エンドユーザー使用許諾契約書 (EULA)

重要

本ソフトウェアをご使用になる前に、エンドユーザー使用許諾契約書 (EULA) に記載された Quick Heal の契約条件をよくお読みください。エンドユーザー使用許諾契約書は製品のインストール時に、または www.quickheal.com/eula からお読みいただけます。

お客様が本ソフトウェアをご使用になるか、ソフトウェア使用許諾契約条件に合意される場合、またはいかなる方法であれソフトウェアを読み込もうとする試みを行った場合も (そうした行為はお客様の合意と署名を表すものとみなされます)、お客様が Quick Heal のエンドユーザー使用許諾契約書 (以下「使用許諾契約書」とする) のすべての契約条件を読み、理解し、合意したことを確認および承認するものとします。以下の諸条件に同意できない場合は、本ソフトウェアを未使用の状態に迅速に返却するか、またはお手元にある本ソフトウェアすべてのコピーを削除してください。

本使用許諾契約書は、ライセンシーである本ソフトウェアを使用するお客様個人 (19歳以上であること)、企業、または法人 (以下「お客様」とする) と、Quick Heal Technologies (P) Ltd. (以下「Quick Heal」とする) との間の法的拘束力を有する契約書です。

1. 期間

Quick Heal ソフトウェアの本ライセンスは、有効化を行った日から〇〇日間 (以下「当該期間」とする) のみ有効となります。本ソフトウェアの当該期間の終了間近または終了後にお知らせします。

2. 評価および登録

本契約によりお客様は、譲渡不能かつ非独占かつサブライセンス不能な本ソフトウェアの使用を許諾されます。当該期間を超えて本ソフトウェアを使用することは、インド国著作権法および国際著作権法の違反に当たります。

Quick Heal は、明示的に付与されていないすべての権利を留保し、すべての知的財産権および所有権、媒体を問わずすべての複製物を含む本ソフトウェアの権原と所有権を保持します。本ソフトウェアと付属資料は Quick Heal の所有物であり、著作権により保護されています。本ソフトウェアまたは付属資料をコピーすることは、明示的に禁止されています。

3. 第三者のウェブサイトへのリンク

本ソフトウェア製品の使用に際し、特定の場面において第三者のウェブサイトへのリンクが含まれている場合があります。本ソフトウェアの使用者であるお客様は、こうした第三者のウェブサイトにはリダイレクトされる可能性があります。第三者のウェブサイト

は Quick Heal の管理下にあるものではなく、Quick Heal はそこに含まれるいかなる内容および/またはいかなるリンクについても責任を負いません。Quick Heal はお客様の参照目的のためにリンクを提供しているにすぎず、Quick Heal は第三者のウェブサイトが原因で発生する損失・損害の責任を負わないものとします。

本ソフトウェアには、BSD ライセンス、GNU General Public License (GPL)、Oval、Zlib、Apache やその他の同様のフリーソフトウェアライセンスによってユーザーにライセンス（またはサブライセンス）される特定のソフトウェアが含まれている可能性があります。これらのライセンスは、ユーザーに特定プログラムあるいはその一部のコピー、改変、再配布、およびソースコードへのアクセスを許可します（「オープンソースソフトウェア」）。Quick Heal は、アップデートの提供あるいはそれ以外の目的で任意のオープンソースソフトウェアの任意のバージョンを使用または選択する権利を留保します。こうしたライセンスが、実行可能なバイナリ形式で配布される任意のソフトウェアについてユーザーがソースコードも入手できることを求めている場合、ソースコードは、「tpsrc@quickheal.com」に要求を送信することで入手できるか、またはソフトウェアとともに提供されます。オープンソースソフトウェアの情報およびライセンスは、Quick Heal インストールフォルダのファイル「`opensrc.txt`」、または「www.quickheal.com/eula」から製品のエンドユーザー使用許諾契約書 (EULA) を取得して確認できます。オープンソースソフトウェアライセンスにより、オープンソースソフトウェアを使用、コピー、または改変する権利を権利者が提供するように求められ、その権利が、本契約によって付与されている権利よりも広範囲に及ぶ場合、こうした権利は本契約の権利および制限に優先して適用されます。

各オープンソースソフトウェアライセンスに記載された諸条件および Quick Heal Anti virus Security エンドユーザー使用許諾契約書に記載された契約条件に従って――

お客様は以下の事項を行うことはできません。

- ソフトウェアの一部をサブライセンス、賃借、賃貸すること。
- ソフトウェアをデバッグ、逆コンパイル、分解、修正、翻訳、リバースエンジニアリングすること。
- ソフトウェアのソースコードを明らかにしたり見つけたりしようと試みること。
- 許諾されていない目的や違法な目的で使用する事。

4. 有効化

Quick Heal は、本ソフトウェアのインストールを行う際、お客様のコンピュータに他のセキュリティ製品やソフトウェアがインストールされており、それらの製品やソフトウェアに Quick Heal のソフトウェアとの互換性がない場合は、アンインストールまたは無効化される場合があることを通知および警告します。本ソフトウェアはインターネット経由で有効化を行う必要があります。

5. サポート

Quick Heal は、本ソフトウェアご使用の際に、技術サポートチームとのライブチャットやお客様のご希望があればサポートチームが遠隔コンピュータアクセスによってサポートを提供する場合があります。本サポートのご利用はすべてお客様の判断に委ねられており、サポートを受ける前にお手元のコンピュータにある既存データ/ソフトウェア/プログラムのバックアップを取ることは、すべてお客様の責任となります。Quick Heal は、このサポートのプロセス全体を通して発生したデータの損失とデータ/所有物に対する直接/間接的/派生的損失または損害に対し、一切の責任を負わないものとします。Quick Heal はサポート機能の提供においていかなる保証も主張しないため、技術サポートチームがある時点においてサポート内容が対象範囲外であると判断した場合、Quick Heal は単独の裁量においてこのようなサポートを保留、停止、終了または拒否します。

6. 電子メール/電子通信

お客様が本ソフトウェア製品を起動し、ソフトウェアを登録すると、Quick Heal は、電子メールまたは電話や携帯電話などの電子通信機器を使用して、登録処理の際にご提供いただいた連絡先へ、製品の更新または製品検証のためにご連絡をする場合があります。この連絡は、お客様の利便性向上のために行われる製品リニューアルや製品の検証を目的とするものです。

7. QUICK HEAL ステータスアップデート

Quick Heal は単独の裁量において当該ライセンス期間のみソフトウェアのアップデートを提供する場合があります。当該期間中は正規ライセンス版コピーのアップデートのたびに、Quick Heal アップデートモジュールが現在の製品ステータス情報を Quick Heal インターネットセンターに送信します。このインターネットセンターに送信される情報には、システム中でどの監視サービスがどのような状態にあるのか、といったことを示す Quick Heal 保護の診断状況が含まれます。収集される情報には、いかなるファイルも個人データも含まれません。この情報は、正規ライセンス版をご利用のお客様により良い技術サポートを迅速に提供するために使用されます。Quick Heal は、アップデートを提供する目的で、任意のオープンソースソフトウェアのアップデートバージョン/ライセンスの使用を選択する権利を留保します。

登録されたお客様全員に、ライセンス有効化を行った日からライセンス期間が満了するまで無償でアップデートが提供されます。

8. 情報の収集

Quick Heal のソフトウェアは、お客様からの許可の下、または許可なしに、個人を特定できる情報を含むか否かにかかわらず、統計目的または悪質な動作パターン、本質的に不正なウェブサイト、およびその他のインターネットセキュリティ脅威/リスクの特定および検出する Quick Heal 製品の能力、効果、性能の強化と評価のために、以下の情報を収集する場合があります。この情報は個人を特定できる情報と関連付けられることはありません。情報には以下が含まれますが、それらに限定されません。

- Quick Heal のソフトウェアがマルウェアの動作パターンの潜在性があると特定する実行ファイル。
- ソフトウェアのインストール中にエラーが発生するか、またはインストールが正常に完了したことを示すソフトウェアのステータスに関連する情報。
- Quick Heal のソフトウェアが本質的に不正であるとみなしたか、または不正である可能性があるるとみなした閲覧済みウェブサイトの URL。
- Quick Heal のソフトウェアがセキュリティリスク/脅威をもたらす不正が潜在的にあるとみなす情報。
- Quick Heal のソフトウェアがインストールされているコンピュータのメディアアクセス制御 (MAC) アドレスを特定するための情報。
- インターネットプロトコル (IP) アドレスを特定するための情報と効果的なライセンス管理や製品の機能性と有用性を向上するために必要となる情報。
- お客様は、上記の通り収集された情報/データが、潜在的なインターネットセキュリティのリスクを解析、防止、検出するために使用されること、そして収集された統計上のデータ/レポート/プレゼンテーションを公表すること、意識を向上させるために組織およびベンダーとデータを共有することを承認するものとします。

9. 免責事項




本ソフトウェアパッケージは、パッケージの商品性および適合性の黙示的保証を含むがこれに限定されない、一切の明示的または黙示的な保証を行うことなく提供されます。Quick Heal またはそのサプライヤーは、本ソフトウェアパッケージの使用、または本ソフトウェアパッケージを使用できないことに起因するデータの損失、利益逸失、またはその他一切のデータ/所有物の損害を含む直接的、間接的、または派生的な損害について、お客様またはその他の者に対して一切責任を負いません。Quick Heal は法的手続きに協力する権利を有し、お客様による本ソフトウェアの使用に関連する文書や情報を提供することがあります。上記の免責事項および制限事項は、本ソフトウェアの同意にかかわらず適用されます。

本書は *Quick Heal Antivirus Security* エンドユーザー使用許諾契約書の簡略版/抜粋です。実際にソフトウェアを使用する前に、当社のソフトウェア使用許諾契約書の詳細な諸条件をお読みになることをお勧めします。Quick Heal Antivirus Security エンドユーザー使用許諾契約書の詳細版をご覧になるには、次のリンクにアクセスしてください: www.quickheal.com/eula

一切の事項はプネ (インド) の管轄に属します。

本書について

本ユーザーガイドには、Windows オペレーティングシステムに Quick Heal AntiVirus 製品をインストールしてお使いいただく上で必要な情報がすべて記載されています。次の表では、本ガイドの作成にあたって使用した規定について記載しています。

規定	意味
太字	太字はメニュータイトル、ウィンドウタイトル、チェックボックス、ドロップダウンボックス、ダイアログ、ボタンの名称、ハイパーリンクなどを表します。
	この記号は注意を表します。対象のトピックに関連する重要なポイントを補足したり、ただし書きを強調したりします。
	この記号はヒントを表します。ユーザーがこのテクニックと手順を利用して、対象のトピックに関連する作業を遂行するのに役立ちます。
	この記号は警告または注意を表します。データの紛失またはハードウェアへの損害を避けるためのアドバイスです。
<ステップ 1> <ステップ 2>	番号が振られたリストには、実施すべき手順が記載されています。
製品名	Quick Heal AntiVirus という名称は、本ユーザーガイドでは一般名称として使用しています。お客様のご購入内容により、以下の製品のいずれかに言及している可能性があります: Quick Heal Internet Security、Quick Heal Total Security、Quick Heal AntiVirus Pro、Quick Heal Internet Security Essentials、Quick Heal AntiVirus Server Edition (特に指定しない限り)

Quick Heal 製品比較表

機能	Quick Heal				
	AntiVir us Pro	Internet Security Essentia ls	AntiViru s Server Edition	Interne t Secur ity	Total S ecurity
高度な DNA スキャン	✓	✓	✓	✓	✓
主要システム保護					
<ul style="list-style-type: none"> • アンチウイルス • アンチスパイウェア • アンチマルウェア • アンチルートキット • ファイアウォール 	<ul style="list-style-type: none"> • 侵入検知 • 侵入防止 • 脆弱性スキャン 	✓	✓	✓	✓
メール保護					
<ul style="list-style-type: none"> • スпам対策 		✓	✓	✓	✓
インターネット保護					
<ul style="list-style-type: none"> • ブラウザサンドボックス 	✓	✓		✓	✓
<ul style="list-style-type: none"> • セーフバンキング 				✓	✓
<ul style="list-style-type: none"> • フィッシング対策 		✓	✓	✓	✓
<ul style="list-style-type: none"> • ウェブセキュリティ • ペアレンタルコントロール 				✓	✓
プライバシー保護					
<ul style="list-style-type: none"> • データ盗難対策 			✓		✓
<ul style="list-style-type: none"> • 安全な削除 					✓
PC 最適化					
<ul style="list-style-type: none"> • レジストリのクリーンアップ • ディスクの 	<ul style="list-style-type: none"> • レジストリのデフラグ • 重複ファイルファイン 				✓

機能		Quick Heal				
		AntiVirus Pro	Internet Security Essentials	AntiVirus Server Edition	Internet Security	Total Security
クリーンアップ • 履歴のクリーンアップ	ダ					
携帯電話保護						
• PC2Mobile スキャン						✓

目次

1. はじめに.....	1
前提条件.....	1
システム要件.....	1
Quick Heal AntiVirus をインストールする.....	5
Quick Heal AntiVirus をアンインストールする.....	6
2. 登録、再有効化、更新.....	8
登録.....	8
オンライン登録.....	8
SMS で登録.....	9
マルチユーザーパックの登録.....	10
再有効化.....	10
更新.....	11
オンライン更新.....	11
3. Quick Heal ダッシュボード.....	13
Quick Heal ダッシュボードについて.....	13
右枠メニューオプション.....	16
4. Quick Heal 保護センター.....	18
ファイルとフォルダ.....	19
スキャン設定.....	19
アーカイブファイルのスキャン.....	21
スキャンするアーカイブの種類を選択.....	22
パックファイルのスキャン.....	22
受信ボックスのスキャン.....	22
ウイルス対策.....	23
高度な DNA スキャン.....	24
疑わしいパックファイルのブロック.....	26
自動偽装セキュリティツールスキャン.....	27
スキャンスケジュール.....	27
スキャンスケジュールの設定.....	27
除外ファイルおよびフォルダ.....	30
除外ファイルおよびフォルダの設定.....	30
隔離とバックアップ.....	31

隔離とバックアップの設定.....	31
電子メール.....	32
電子メール保護.....	32
電子メール保護の設定.....	32
信頼できる電子メールクライアントの保護.....	34
信頼できる電子メールクライアントの保護の設定.....	34
スパム対策.....	34
スパム対策の設定.....	34
インターネットとネットワーク.....	37
ファイアウォール保護.....	37
ファイアウォール保護の設定.....	38
ブラウジング保護.....	41
ブラウジング保護の設定.....	41
マルウェア対策.....	41
マルウェア対策の設定.....	41
フィッシング対策.....	41
フィッシング対策の設定.....	42
ブラウザサンドボックス.....	42
ブラウザサンドボックスの設定.....	42
セーフバンキング.....	43
セーフバンキングの設定.....	44
セーフバンキングの起動.....	45
ニュースアラート.....	45
ニュースアラートを無効にする.....	45
不正侵入防御・検知システム (IDS/IPS).....	46
[IDS/IPS] を ON にする.....	46
ペアレンタルコントロール.....	46
ペアレンタルコントロールの設定.....	47
特定のウェブサイトカテゴリへのアクセスを制限する.....	48
特定のウェブサイトへのアクセスを制限する.....	49
インターネットアクセス時間のスケジュールを設定する.....	49
管理者アカウントを作成する.....	50
Quick Heal パスワード保護.....	50
制限付きユーザーアカウントを作成する.....	51
外部ドライブとデバイス.....	52
自動実行保護.....	52

自動実行保護の設定.....	52
外部ドライブのスキャン.....	52
外部ドライブのスキャンの設定.....	52
データ盗難対策.....	53
データ盗難対策の設定.....	53
Windows Mobile のスキャン.....	54
Windows Mobile のスキャンの設定.....	54
5. クイックアクセス機能.....	55
スキャン.....	55
システム全体のスキャンの実行.....	55
カスタムスキャンの実行.....	56
メモリスキャンの実行.....	56
ブートタイムスキャンの実行.....	57
モバイルスキャンの実行.....	57
PC2Mobile スキャンで携帯端末をスキャンする.....	58
Quick Heal PCTuner.....	59
最新情報.....	59
6. Quick Heal メニュー.....	60
設定.....	60
インポートとエクスポート設定.....	60
自動アップデート.....	61
自動アップデートの設定.....	61
インターネット設定.....	62
インターネット設定.....	62
レジストリの復元.....	63
レジストリの復元の設定.....	63
セルフプロテクション.....	64
セルフプロテクションの設定.....	64
パスワード保護.....	64
セーフモード保護.....	64
パスワード保護の設定.....	64
レポート設定.....	65
レポート設定を行う.....	65
ウイルス統計レポート.....	65

ウイルス統計レポートの設定.....	65
Quick Heal を遠隔管理.....	66
Quick Heal リモートデバイスマネジメント.....	66
初期設定に復元.....	69
初期設定に復元.....	69
ツール.....	69
ハイジャック復元.....	69
ハイジャック復元の使用.....	70
追跡クリーナ.....	71
追跡クリーナの使用.....	71
アンチルートキット.....	71
Quick Heal アンチルートキットの使用.....	72
Quick Heal アンチルートキットの設定.....	73
スキャン結果およびルートキットの除去.....	74
Quick Heal 緊急ディスクを用いたルートキットの除去.....	75
緊急ディスクの作成.....	76
アンチマルウェアの起動.....	77
Quick Heal アンチマルウェアの開始.....	77
Quick Heal アンチマルウェアの使用.....	78
隔離ファイルの表示.....	78
隔離ファイルの起動.....	79
USB ドライブの保護.....	79
System Explorer.....	80
Windows スパイ.....	80
Windows スパイの使用.....	81
ファイル拡張子の除外.....	81
ウイルス対策の除外リストの作成.....	81
レポート.....	82
レポートの閲覧.....	82
ヘルプ.....	83
7. Quick Heal のアップデートとウイルスの除去.....	86
インターネットから Quick Heal をアップデートする.....	86
Quick Heal を定義ファイルを用いてアップデートする.....	87
ネットワーク環境のアップデートガイドライン.....	87
ウイルスの除去.....	88

スキャン実行中に検出されたウイルスの削除.....	88
スキャンオプション.....	88
メモリ内で検出されたウイルスの除去.....	89
8. Quick Heal PCTuner	91
Quick Heal PCTuner ダッシュボード.....	91
ステータス.....	92
チューンアップ.....	93
自動チューンアップ.....	93
自動チューンアップのカスタマイズ.....	94
自動チューンアップの実行.....	94
ディスクのクリーンアップ.....	94
ディスクのクリーンアップの実行.....	94
レジストリのクリーンアップ.....	95
レジストリのクリーンアップの実行.....	95
履歴のクリーンアップ.....	96
履歴のクリーンアップの実行.....	96
デフラグ.....	97
デフラグの使用.....	97
スケジューラ.....	97
スケジューラのカスタマイズ.....	98
設定.....	99
ディスクのクリーンアップのカスタマイズ.....	99
レジストリのクリーンアップのカスタマイズ.....	99
履歴のクリーンアップのカスタマイズ.....	100
ツール.....	100
重複ファイルファインダ.....	100
重複ファイルの削除.....	101
スタートアップブースター.....	103
サービスオプティマイザ.....	104
レポート.....	105
自動チューンアップレポート.....	106
ディスクのクリーンアップレポート.....	106
レジストリのクリーンアップレポート.....	106
履歴のクリーンアップレポート.....	107
スケジューラレポート.....	107

安全な削除レポート.....	107
重複ファイルファインダレポート.....	107
スタートアップブースターレポート.....	108
サービスオプティマイザレポート.....	108
復元レポート.....	108
復元.....	109
レポートの復元.....	109
レポートの削除.....	109
9. 技術サポート.....	110
プロダクトキーを紛失した場合の対処法.....	110
サポート.....	110
サポート連絡先.....	112
Quick Heal Technologies の連絡先情報.....	113
10. インデックス.....	114

はじめに

Quick Heal AntiVirus は、簡単にインストールできる使いやすい製品です。インストールの際には各インストール画面をよく読み、指示に従ってください。

前提条件

Quick Heal AntiVirus をシステムにインストールする際は下記のガイドラインに従ってください。

- 複数のアンチウイルスソフトウェア製品が 1 つのシステムにインストールされていると、システムが誤作動を起こす可能性があります。他のアンチウイルスソフトウェアプログラムがシステムにインストールされている場合は、Quick Heal AntiVirus のインストールを続ける前にそれらのプログラムをアンインストールする必要があります。
- Quick Heal AntiVirus のインストールを続ける前に、すべてのプログラムを終了してください。
- システムがウイルスに感染している場合に備えて、データのバックアップを作成しておくことをお勧めします。
- Quick Heal AntiVirus は、管理者権限を使用してインストールしてください。

システム要件

Quick Heal AntiVirus を使用するためには、お使いのシステムが下記の要件を満たしている必要があります。

ただし、下記の要件は最小限のシステム要件です。最高の結果を得るには、下記の要件を上回るシステムをお勧めします。

- アップデートを受け取るためのインターネット接続
- CD/DVD ドライブ

オペレーティングシステムの互換性

オペレーティングシステム	必要要件
Windows 2000 / Windows 2000 Server*	300 MHz Pentium (または互換) プロセッサ メモリ容量 512 MB DVD または CD-ROM ドライブ Service Pack 4 Internet Explorer 6
Windows XP	300 MHz Pentium (または互換) プロセッサ メモリ容量 512 MB DVD または CD-ROM ドライブ Service Pack 2 以降
Windows Server 2003*	300 MHz Pentium (または互換) プロセッサ メモリ容量 512 MB DVD または CD-ROM ドライブ
Windows Vista	1 GHz Pentium (または互換) プロセッサ メモリ容量 512 MB DVD または CD-ROM ドライブ
Windows Server 2008* / Windows Server 2008 R2*	1 GHz Pentium (または互換) プロセッサ メモリ容量 1 GB DVD または CD-ROM ドライブ
Windows 7 / Windows 8 / Windows 8.1	1 GHz Pentium (または互換) プロセッサ 32 ビット版の場合: メモリ容量 512 MB、64 ビット版の場合: メモリ容量 1 GB DVD または CD-ROM ドライブ
Windows Server 2012* / Windows Server 2012 R2*	1 GHz Pentium (または互換) プロセッサ メモリ容量 1 GB DVD または CD-ROM ドライブ

- (*) このオペレーティングシステムに対応しているのは、Quick Heal AntiVirus Server Edition のみです。
- ここに記載される要件は、別途記載がない限り、32 ビット版および 64 ビット版のオペレーティングシステムに適用されます。
- ここに記載される要件は、オペレーティングシステムのすべてのタイプに適用されます。

- Quick Heal AntiVirus Pro、Quick Heal Internet Security Essentials、Quick Heal Internet Security、Quick Heal Total Security は Microsoft Windows Server オペレーティングシステムには対応していません。
- 最新のシステム要件は Quick Heal のウェブサイト www.quickheal.com でご確認ください。

Quick Heal AntiVirus 製品のインストールに必要な空きディスク容量は以下の通りです。

製品	空きディスク容量
Quick Heal Total Security	2.25 GB
Quick Heal Internet Security	2.15 GB
Quick Heal AntiVirus Pro	2.15 GB
Quick Heal AntiVirus Server Edition	2.15 GB
Quick Heal Internet Security Essentials	2.15 GB

電子メールスキャンに対応しているクライアント

電子メールスキャン機能に対応している POP3 電子メールクライアントは下記の通りです。

- Microsoft Outlook Express 5.5 以降
- Microsoft Outlook 2000 以降
- Netscape Messenger 4 以降
- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

電子メールスキャンに対応していないクライアント

電子メールスキャン機能に対応していない POP3 電子メールクライアントとネットワークプロトコルは下記の通りです。

- IMAP
- AOL
- SSL 付きの POP3
- Hotmail や Yahoo! Mail のようなウェブメールメール
- Lotus Notes

SSL 接続は未対応です

電子メール保護は SSL を用いた暗号化電子メール接続には対応していません。

Quick Heal アンチルートキット要件

- 64 ビット版のオペレーティングシステムには対応していません。
- 512 MB 以上のメモリ容量が必要です。

Quick Heal セルフプロテクション

- Microsoft Windows 2000 オペレーティングシステムには対応していません。
- Microsoft Windows XP オペレーティングシステムには、Service Pack 2 以降がインストールされている場合のみ対応しています。
- Microsoft Windows Server 2003 オペレーティングシステムには、Service Pack 1 以降がインストールされている場合のみ対応しています。
- セルフプロテクションのプロセス保護機能は、Microsoft Windows Vista Service Pack 1 以降に対応しています。

Quick Heal PC2Mobile スキャン

- Quick Heal Total Security でのみ利用可能です。
- Microsoft Windows 2000 オペレーティングシステムには対応していません。
- Windows Mobile デバイスには、
 - Windows XP 以前のオペレーティングシステムに Microsoft Active Sync 4.0 以降がインストールされている必要があります。
 - Windows Vista 以降のオペレーティングシステムに Windows Mobile デバイスセンターがインストールされている必要があります。

Quick Heal PCTuner

- Quick Heal Total Security でのみ利用可能です。
- Microsoft Windows 2000 オペレーティングシステムには対応していません。

Quick Heal ブラウザサンドボックス

- Quick Heal AntiVirus Server Edition では利用できません。
- Microsoft Windows 2000、Microsoft Windows XP 64 ビット版オペレーティングシステムには対応していません。

Quick Heal セーフバンキング

- Quick Heal AntiVirus Server Edition では利用できません。
- Microsoft Windows 2000、Microsoft Windows XP 64 ビット版オペレーティングシステムには対応していません。

Quick Heal は、Quick Heal を遠隔管理します

Microsoft Windows 2000 オペレーティングシステムには対応していません。

Quick Heal AntiVirus をインストールする

Quick Heal AntiVirus をインストールするには、以下の手順に従ってください。

1. Quick Heal AntiVirus の CD/DVD を DVD ドライブに挿入してください。

CD/DVD の自動再生機能が作動し、オプションのリスト画面が自動的に表示されます。

CD/DVD が自動的に開始されない場合は、以下の手順に従ってください。

- i. CD/DVD にアクセスできるフォルダに移動します。
 - ii. DVD ドライブを右クリックして **[エクスプローラ]** を選択します。
 - iii. **自動実行ファイル (Autorun.exe)** をダブルクリックします。
2. **[インストール]** をクリックしてインストールを開始してください。

インストールウィザードが、インストール前にシステムのウイルススキャンを行います。インストール前のスキャン中に、アクティブなウイルスがメモリ内で検出された場合、

- インストーラが自動的にブートタイムスキャナを設定し、次の起動時にシステムのスキャンを実施し、ウイルスを駆除します。
- ウイルスを駆除した後、コンピュータが再起動します。インストールを再実行してください。詳細は、[ブートタイムスキャンの実行](#)を参照してください。

システムメモリにウイルスが見つからない場合は、インストールが続行されます。

エンドユーザー使用許諾契約書画面が表示されます。使用許諾契約書はよくお読みください。

3. 使用許諾契約書末尾に **[疑わしいファイルを報告する]** と **[統計を報告する]** という 2 つのオプションがあります。これらのオプションは初期設定で選択されています。疑わしいファイル、統計、またはその両方を報告したくない場合は、これらのオプションからチェックを外してください。
4. 使用許諾契約書の条件に同意する場合は、**[同意する]** をチェックして **[次へ]** をクリックしてください。
インストール先の画面が表示されます。Quick Heal アンチウイルスの初期設定のインストール先が表示されます。インストールに必要なディスク容量も画面に表示されます。
5. 初期設定のインストール先で容量が不足している場合、または別の場所にインストールしたい場合は、**[参照]** をクリックしてインストール先を変更してください。あるいは、**[次へ]** をクリックしてインストールを続行してください。

インストールが開始されます。インストールが完了すると、メッセージが表示されます。

6. [今すぐ登録] をクリックして有効化プロセスを開始するか、[後で登録] をクリックして後で有効化を行ってください。

Quick Heal AntiVirus をアンインストールする

Quick Heal AntiVirus をアンインストールすると、ウイルスの脅威にシステムをさらすこととなります。それでも、以下の方法によって Quick Heal AntiVirus をアンインストールすることができます。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus #] > [Quick Heal AntiVirus をアンインストール] の順に選択します。
 - **Quick Heal を削除し、アップデート定義ファイルを保持する** - このオプションを選択すると、Quick Heal はライセンス情報、ダウンロードしたすべてのアップデート定義、レポート、隔離ファイル、アンチスパムホワイトリスト/ブラックリストを、コンピュータのリポジトリに保存し、再インストール時に使用できるようにします。
 - **Quick Heal を完全に削除** - このオプションを選択すると、Quick Heal はコンピュータから完全に削除されます。
2. オプションの 1 つを選択し、[次へ] をクリックしてアンインストールを続行します。

Quick Heal AntiVirus をパスワードで保護している場合は、認証画面が表示されます。

3. パスワードを入力し、[OK] をクリックします。

アンインストールが開始されます。

アンインストールが完了すると、メッセージが表示されます。

アンインストールした理由等のフィードバックをご提供いただける場合は、[Quick Heal AntiVirus をアンインストールした理由を送信する] をクリックしてください。お客様のフィードバックは当社にとって重要です。製品の品質向上のために活用させていただきます。



参照用にプロダクトキーをメモしてください。[ファイルに保存] をクリックして、お客様のプロダクトキー情報を保存することができます。Quick Heal AntiVirus のアンインストール後は、コンピュータを再起動することをお勧めします。再起動するには [今すぐ再起動] をクリックするか、[後で再起動] をクリックして現在の作業を続け、後で再起動します。



(#) ここに記載される Quick Heal AntiVirus とは次の製品をいずれかを指します。 お客様のコンピュータにインストールされた Quick Heal Internet Security、Quick Heal Total Security、Quick Heal AntiVirus Pro、Quick Heal Internet Security Essentials、Quick Heal AntiVirus Server Edition の各製品。

(*) 機能が Quick Heal アンチスパム機能で使用されるために設定されていることを意味します。

(†) オプションが Quick Heal AntiVirus Server Edition、Quick Heal Internet Security Essentials、Quick Heal Internet Security および Quick Heal Total Security のみで表示されていることを意味します。

登録、再有効化、更新

インストールを行ったら、速やかに登録してください。登録されていない製品は、トライアルバージョンとみなされます。ライセンスを登録するとすべての機能を制限なく使用でき、定期的なアップデートを取得可能で、必要なときに技術サポートを受けることもできます。製品が定期的にアップデートされない場合、最新の脅威からお客様のシステムを守ることができません。

登録

Quick Heal AntiVirus は次のいずれの方法でも登録することができます。

[オンライン登録](#)

[SMS で登録](#)

オンライン登録

インターネットに接続されている場合は、オンラインで製品の登録を行うことができます。Quick Heal AntiVirus をオンラインで登録するには、以下の手順に従ってください。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal AntiVirus を有効化] の順に選択します。
2. 登録ウィザードで 20 桁のプロダクトキーを入力し、[次へ] をクリックします。
登録情報が表示されます。
3. [購入先] および [登録名] テキストボックスに適切な情報を入力し、[次へ] をクリックします。
4. [名前]、[電子メールアドレス]、[連絡先電話番号] を入力します。[国]、[都道府県]、[市町村] を選択します。

お客様の都道府県や市町村がリストにない場合、各ボックスに直接入力してください。

5. [次へ] をクリックして続けます。
お客様の入力情報の確認画面が表示されます。
変更が必要な場合、[戻る] をクリックして前の画面に戻り、必要な変更を行ってください。
6. [次へ] をクリックして続けます。
製品が正常に有効化され、ライセンスの有効期限が表示されます。
7. [終了] をクリックして登録ウィザードを閉じます。



Quick Heal AntiVirus を登録すると、Quick Heal RDM でアカウントを作成するように促されます。これにより、デバイスを遠隔操作で管理できます。Quick Heal RDM でアカウントを作成する方法については、[Quick Heal 1 を遠隔管理](#)を参照してください。

SMS で登録

Quick Heal AntiVirus は、SMS を用いて有効化することもできます。お使いのシステムがインターネットに接続していない場合は、SMS 登録プロセスにより製品を登録することができます。



現時点では SMS を用いた登録機能はインドでのみご利用いただけます。

Quick Heal AntiVirus は以下の方法で SMS 登録機能により製品を登録することができます。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal AntiVirus を有効化] の順に選択します。
2. 登録ウィザードで、[SMS 登録] をクリックします。
SMS 登録画面が表示されます。諸条件をよくお読みください。
3. [次へ] をクリックします。
4. 20 桁の**プロダクトキー**を入力し、[次へ] をクリックします。
登録情報が表示されます。
5. [購入先] および [登録名] テキストボックスに適切な情報を入力し、[次へ] をクリックします。
6. [名前]、[電子メールアドレス]、[連絡先電話番号] を入力します。[国]、[都道府県]、[市町村] を選択します。

お客様の都道府県や市町村がリストにない場合、各ボックスに直接入力してください。

7. [次へ] をクリックして続けます。

お客様の入力情報の確認画面が表示されます。

変更が必要な場合、[戻る] をクリックして前の画面に戻り、必要な変更を行ってください。

8. [次へ] をクリックして続けます。

一意のコードと携帯電話番号が表示されます。

9. このコードを入力し、SMS として表示された番号に送信します。

10. Quick Heal 登録センターで登録が終了すると、英数文字で構成される有効化コードを記載した SMS がお客様の登録済み携帯電話に届きます。この有効化コードを所定のテキストボックスに入力し、[次へ] をクリックします。

製品が正常に有効化され、ライセンスの有効期限が表示されます。

11. [終了] をクリックして登録ウィザードを閉じます。

マルチユーザーパックの登録

マルチユーザーパックの有効化を行う場合は、以下の事項に注意してください。

- マルチユーザーパックのプロダクトキーを登録する場合は、パックに含まれる残りのすべてのプロダクトキーも同時に登録してください。
- 最初に有効化されるプロダクトキーの登録情報が、残りのすべてのプロダクトキーに適用されます。
- 同様に、同じライセンス有効期限がパック内のすべてのプロダクトキーに適用されます。

再有効化

再有効化は、ライセンス有効期限が終了するまで製品を確実にお使いいただくための機能です。再有効化は、お客様がシステムの初期化を行いソフトウェアが消えてしまった場合や、他のコンピュータに Quick Heal AntiVirus をインストールする場合に便利です。そのような場合は、Quick Heal AntiVirus をシステムに再インストールし、再有効化する必要があります。

再有効化プロセスは有効化プロセスと似ていますが、異なるのは、個人情報や再度すべて入力する必要がないという点です。プロダクトキー（および、オフラインでの再有効化の場合はインストール番号）を送信すると、詳細情報が表示されます。これらの情報を確認し、プロセスを完了するだけです。

コンピュータからアンインストールする際に、[\[Quick Heal を削除し、アップデート定義ファイルを保持する\]](#) オプションを利用してライセンスバックアップを保存している場合、再有効化をスタートさせると、Quick Heal 登録ダイアログボックスにプロダクトキーが表示されます。そのプロダクトキーと保存済みのアップデートを使用して、作業を続行できます。別のプロダクトキーを使用することもできます。

プロダクトキー（および、オフラインでの再有効化の場合はインストール番号）を送信すると、ユーザー詳細情報が表示されます。これらの情報を確認し、プロセスを完了できます。



SMS でライセンスを再有効化したい場合は、ユーザー情報を再入力する必要があります。

更新

有効期限終了直後に更新コードを購入して製品ライセンスを更新することもできますが、コンピュータが継続して保護されるように、有効期限終了前の更新をお勧めします。更新コードは、Quick Heal のウェブサイト、お近くの販売業者または代理店で購入することができます。

Quick Heal AntiVirus は、次のいずれの方法でも更新することができます。

[オンライン更新](#)

オンライン更新

お使いのコンピュータがインターネットに接続されている場合、Quick Heal AntiVirus を以下の方法でオンライン更新することができます。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal AntiVirus] の順に選択します。
2. [ヘルプ] メニューをクリックし、[本製品について] > [今すぐ更新] を選択します。

製品ライセンスの有効期限が切れている場合は、Quick Heal ダッシュボードに [今すぐ更新] ボタンが表示されます。ライセンスを更新するには、[今すぐ更新] をクリックします。

登録ウィザードが表示されます。

3. [更新コードを使用して更新します] オプションを選択します。[すでに更新コードを持っています] オプションを選択し、[次へ] をクリックします。

登録情報が表示されます。

4. [購入先]、[電子メールアドレス]、および [連絡先電話番号] テキストボックスが表示され、あらかじめ該当情報が入力されています。必要に応じて連絡先情報を変更し、[次へ] をクリックします。

[現在の有効期限]、[新しい有効期限] 等のライセンス情報が確認のために表示されます。

5. [次へ] をクリックします。

Quick Heal AntiVirus のライセンスが正常に更新されます。

6. [終了] をクリックして、更新プロセスを完了します。



- 更新コードをお持ちでない場合、[更新コードを持っていません。更新コードをオンラインで購入します] オプションを選択し、[今すぐ購入] をクリックします。
- 追加の更新コードを購入された場合、現在の更新を行った 10 日後以降にお使いいただけます。

Quick Heal ダッシュボード

Quick Heal ダッシュボードは Quick Heal AntiVirus のすべての機能のメインインターフェースとして機能します。Quick Heal AntiVirus は初期設定状態でもシステムを保護します。Quick Heal AntiVirus を起動して、現在の保護ステータスを確認したり、手動でシステムをスキャンしたり、レポートを閲覧したり、製品をアップデートしたりできます。

以下のいずれかの方法で Quick Heal AntiVirus を手動で起動することができます。

- [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal AntiVirus] の順に選択します。
- タスクバーの [Quick Heal AntiVirus] アイコンをダブルクリックするか、または [Quick Heal AntiVirus] アイコンを右クリックし、[Quick Heal AntiVirus を開く] を選択します。
- [スタート] > [実行] の順に選択し、スキャナと入力し、Enter キーを押します。

Quick Heal ダッシュボードについて

Quick Heal ダッシュボードは、いくつかのセクションに分かれています。一番上のセクションは Quick Heal メニュー、真ん中のセクションは保護オプション、一番下のセクションは Quick Heal からの最新情報とスキャンオプションです。

一番上のセクション

一番上のセクションには製品メニューがあり、Quick Heal AntiVirus の一般的な設定を行ったり、各種のウイルス感染防止ツールを使用したりできます。システムを診断し、各機能の様々な活動のレポートを閲覧し、ヘルプやライセンス情報にアクセスすることができます。

以下の表ではメニューとその使用法を説明しています。

メニュー	説明
設定	自動アップデート、インターネット設定、レジストリの復元、セルフプロテクション、パスワード保護、レポート設定、ウイルス統計

ツール	レポート、Quick Heal の遠隔管理、初期設定に復元等の機能をカスタマイズできます。
レポート	ウイルスの攻撃を受けた場合のシステム診断、アプリケーションとインターネット閲覧履歴の削除、マルウェアにより改ざんされた Internet Explorer 設定の復元、ウイルス感染したファイルまたは感染が疑われるファイルの隔離、偽装セキュリティツールの削除、USB ドライブからの自動実行マルウェアの感染防止を行います。一部のファイルをウイルス保護の対象から除外することもできます。
ヘルプ	Quick Heal AntiVirus のヘルプツールにアクセスし、製品バージョン、ウイルスデータベース、有効期限、ライセンスに関する情報を閲覧したり、技術サポートを要請したりすることができます。



(*) フィッシング対策のレポートは Quick Heal AntiVirus Pro では利用できません。

(#) PC2Mobile スキャンのレポートは Quick Heal Total Security でのみ利用可能です。

このセクションの詳細は、[Quick Heal メニュー](#)を参照してください。

真ん中のセクション

真ん中のセクションには保護オプションがあり、コンピュータが必要とする様々なセキュリティ機能を設定できます。

以下の表ではオプションとその使用法を説明しています。

オプション	説明
ファイルとフォルダ	悪意のある脅威からファイルとフォルダを保護します。本オプションにより、スキャン設定、ウイルス対策、高度な DNA スキャン、疑わしいバックファイルのブロック、自動偽装セキュリティツールスキャン、スキャンスケジュール、除外ファイルおよびフォルダ、隔離とバックアップの設定ができます。
電子メール	電子メール保護、信頼できる電子メールクライアントの保護、およびスパム対策の設定を行います。
インターネットとネットワーク	インターネットとネットワークの保護環境を設定します。本オプションにより、ファイアウォール保護、ブラウジング保護、マル

ペアレンタルコントロール*	ウェア対策、フィッシング対策#、ブラウザサンドボックス、セーフバンキング、ニュースアラート、不正侵入防御・検知システム (IDS/IPS) を設定できます。 お子様やその他のユーザーのオンライン活動を制御することができます。お子様がインターネットにアクセスして利用できるスケジュールを定義することもできます。
外部ドライブとデバイス	外部ドライブの保護を設定します。本オプションで、自動実行保護、外部ドライブのスキャン、データ盗難対策**、Windows Mobile のスキャン†を設定できます。



(#) フィッシング対策は Quick Heal AntiVirus Pro では利用できません。

† (*) ペアレンタルコントロールは Quick Heal Total Security および Quick Heal Internet Security でのみ利用可能です。

(**) データ盗難対策は Quick Heal Total Security および Quick Heal AntiVirus Server Edition でのみ利用可能です。

(†) Windows Mobile のスキャンは Quick Heal Total Security でのみ利用可能です。

このセクションの詳細は、[Quick Heal 保護センター](#)を参照してください。

一番下のセクション

以下の表ではオプションとその使用法を説明しています。

その他	説明
最新情報	Quick Heal の最新情報を表示しています。[すべて表示する] をクリックすると、すべての最新情報をお読みいただけます。
PCTuner*	ディスクのクリーンアップ、レジストリのクリーンアップ、履歴のクリーンアップ、ファイルファインダの複製、安全な削除、レジストリデフラグ等の機能により、システムをクリーニングしてシステムパフォーマンスを向上させます。
スキャン	システム全体、ユーザーが定義した場所、メモリ、ブートタイム、モバイルスキャン#等、様々なスキャンオプションを提供しています。
マイアカウン ト	このリンクから、Quick Heal リモートデバイスマネジメント (Quick Heal RDM) のウェブポータルに移動できます。製品を Quick Heal RDM に追加して、ポータルから遠隔操作で製品をモニターすることができます。
マイアカウン ト	このリンクから、 Quick Heal リモートデバイスマネジメント (Quick Heal RDM) のウェブポータルに移動できます。製品を Quick Heal RDM に追加して、ポータルから遠隔操作で製品をモニターする

サポート	<p>ことができます。</p> <p>サポートメニューで提供されている各種のサポートオプションをご利用いただけます。</p>
Facebook のいいね!	<p>このリンクから、Facebook の Quick Heal ページをいいね! できます。</p> <p>Quick Heal のコーポレート Facebook ページには活発なユーザーコミュニティがあります。また、サイバーセキュリティやウイルスの脅威、警告について定期的に数多くの投稿があります。ダッシュボードの [Facebook のいいね!] リンクをクリックして、Quick Heal の Facebook ページをフォローすることができます。</p> <p>Facebook にログオンしていても Facebook の Quick Heal コミュニティに参加していない場合、Quick Heal ページをいいね! してフォローするように促されます。</p>



(*) PCTuner は Quick Heal Total Security でのみ利用可能です。

(#) モバイルスキャンは Quick Heal Total Security でのみ利用可能です。

このセクションの詳細は、[クイックアクセス機能](#)を参照してください。

右枠メニューオプション

Quick Heal AntiVirus の以下の重要な機能に素早くアクセスできます。タスクバーの [Quick Heal AntiVirus] アイコンを右クリックしてから、オプションを選択します。

右枠メニュー	説明
Quick Heal AntiVirus を開く	Quick Heal AntiVirus を起動します。
アンチマルウェアの起動	Quick Heal アンチマルウェアを起動します。レジストリ、ファイル、フォルダをきわめて高速にスキャンできる内蔵ツールです。スパイウェア、アドウェア、偽装セキュリティツール、ダイアラー、リスクウェア等、システムに潜む脅威を徹底的に検出し、除去できます。
サイレントモードを有効/無効にする	Quick Heal AntiVirus のすべての確認ポップアップ画面と通知機能の有効/無効を切り替えます。
セーフバンキング	セーフバンキングを起動します。セーフバンキングを使用すると、安全に銀行取引を行えます。
セキュアブラウザ	安全にブラウジングするために、既定のブラウザをサンドボックス内で起動できます。
ウイルス対策を有効/無効にする	Quick Heal ウイルス対策の有効/無効を切り替えます。
リモートサポート	リモートサポートを起動します。Quick Heal の技術担当者が

今すぐ更新 メモリスキャン	お客様のシステムにアクセスして問題を解決します。 Quick Heal のウイルスデータベースをアップデートします。 システムのメモリにウイルスが侵入していないかスキャンします。
------------------	-------------------------------------------------------------------------------------------------




このセクションの詳細は、[Quick Heal 保護センター](#)を参照してください。

Quick Heal 保護センター

コンピュータシステムで作業するユーザーは、インターネットや外部ドライブに接続したり、電子メールを送受信したりします。このときシステムは、内部に侵入しようとするウイルスにさらされることとなります。Quick Heal 保護センターに含まれる各機能によって、マルウェア、ウイルス、ワーム、データ盗難のあらゆる脅威から、お客様のシステム、フォルダ、ファイル、データを保護することができます。

機能のすぐ上には、Quick Heal AntiVirus 製品の現在のステータスが表示されます。アンチウイルスがシステム内で脅威を検出すると、色付きアイコンで表示されます。

以下の表ではアイコンとその意味を説明しています。

赤		Quick Heal AntiVirus は最適な設定になく、早急な対応を必要としています。お使いのシステムの安全を守るため、メッセージに記載される処置をただちに実行する必要があります。
黄色		Quick Heal AntiVirus の機能の 1 つに対し、できるだけ早い対応を必要としています。
緑		Quick Heal AntiVirus は最適な設定にあり、安全な状態にあります。

Quick Heal 保護センターには以下の機能があります。

機能	説明
ファイルとフォルダ	スキャン設定、ウイルス対策、高度な DNA スキャン、疑わしいバックアップファイルのブロック、自動偽装セキュリティツールスキャン、スキャンスケジュール、除外ファイルおよびフォルダ、隔離とバックアップが含まれます。
電子メール	電子メール保護、信頼できる電子メールクライアントの保護、スパム対策が含まれます。
インターネットとネットワーク	ファイアウォール保護、ブラウジング保護、マルウェア対策、フィッシング対策、ブラウザサンドボックス、セーフバンキング、

	ニュースアラート、不正侵入防御・検知システム (IDS/IPS) が含まれます。
ペアレンタルコントロール	お子様が好ましくないウェブサイトにはアクセスできないよう制限し、インターネットにアクセスできる時間のスケジュールを設定できます。
外部ドライブとデバイス	自動実行保護、外部ドライブのスキャン、データ盗難対策、Windows Mobile のスキャンが含まれます。

ファイルとフォルダ

この機能では、システム内のファイルとフォルダの保護設定を行えます。

ファイルとフォルダ機能には以下の保護設定が含まれます。

スキャン設定

システムのスキャン開始方法や、ウイルスが検出された場合に実行する処置を定義できます。ただし初期設定は最適な状態に設定されており、お客様のシステムに必要な対策を提供しています。

スキャン設定を行うには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [スキャン設定] をクリックします。
4. [[スキャンモードの選択](#)] から、[自動 (推奨)] を選択して自動的にスキャンをスタートさせるか、[高度なスキャン] を選択して、[より高度なスキャン](#)設定を行います。
5. [[ウイルスが見つかったときに実行する処置を選択する](#)] から適切な処置を選択します。
6. 処置を実行する前にファイルのバックアップを作成する場合は、[処置を実行する前にバックアップを作成する] を選択します。
7. 設定を保存するには、[変更を保存] をクリックします。

スキャンモードの選択

自動 (推奨): 初期設定のスキャンタイプです。お客様のシステムに最適な保護を提供するため、お勧めです。この設定は、初心者ユーザーに最適なオプションです。

高度なスキャン: スキャンオプションのカスタマイズができます。経験があるユーザーに理想的なオプションです。[高度なスキャン] オプションを選択すると、[設定] ボタンが有効になり、高度なスキャン設定ができます。

ウイルスが見つかったときに実行する処置

様々な処置とその説明は以下の通りです。

処置	説明
修復	感染したファイルを修復する場合は、このオプションを選択します。 ファイルのスキャン実行中にウイルスが検出された場合、ファイルを修復します。ファイルを修復できない場合は自動的に隔離します。
削除	感染したファイルを削除する場合は、このオプションを選択します。感染したファイルは通知なしに削除されます。一度削除されると元に戻すことはできません。
スキップ	感染したファイルに対して処置を実行しない場合は、このオプションを選択します。
処置を実行する前にバックアップを作成する	感染ファイルを除去する前にバックアップを作成します。バックアップとして保管されたファイルは隔離メニューから復元できます。

高度なスキャンモードの設定

高度なスキャンモードを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [スキャン設定] をクリックします。
4. [\[スキャンモードの選択\]](#) から [高度なスキャン] を選択します。
[設定] ボタンが有効になります。
5. [設定] をクリックします。
高度なスキャン設定詳細画面が表示されます。
6. [スキャンする項目を選択する] から、実行可能ファイルだけをスキャンする場合は [実行可能ファイルをスキャン] を選択し、すべてのファイルをスキャンする場合は [すべてのファイルをスキャン] を選択します。
[実行可能ファイルをスキャン] オプションは初期設定で選択されています。
[すべてのファイルをスキャン] を行う場合はかなりの時間がかかり、スキャンプロセスによりお使いのシステムが遅くなる場合があります。

7. 以下からスキャン対象を 1 つ選択します。
 - [アーカイブファイルのスキャン](#): zip ファイルや rar ファイル等、アーカイブファイルをスキャンする場合に、このオプションを選択します。
 - [パックファイルのスキャン](#): パックされたファイルをスキャンする場合は、このオプションを選択します。
 - [受信ボックスのスキャン](#): クイックスキャンをする場合は [受信ボックスのクイックスキャン] を選択し、徹底的にスキャンする場合は [受信ボックスの徹底スキャン] を選択します。
8. [OK] をクリックします。
9. [変更を保存] をクリックして設定を保存します。

アーカイブファイルのスキャン

zip ファイル、rar ファイル、chm ファイル等のアーカイブファイルのスキャンルールを詳しく設定します。

アーカイブファイルのスキャンを設定するには、以下の手順に従ってください。

1. [高度なスキャン設定](#)画面で、[アーカイブファイルのスキャン] を選択します。

[設定] ボタンが有効になります。

2. [設定] ボタンをクリックします。

アーカイブファイルのスキャン詳細画面が表示されます。

3. [ウイルスが見つかったときに実行する処置を選択する] から、[削除]、[隔離]、[スキップ] のオプションのうち 1 つを選択します。

4. [アーカイブスキャンレベル] で、ファイルとフォルダに対してスキャンを行いたいレベルを選択します。

初期設定では、スキャンレベルはレベル 2 に設定されています。初期設定のスキャンレベルの数値を上げると、スキャン速度に影響を及ぼすことがあります。

5. [スキャンを行うアーカイブの種類を選択] からアーカイブファイルの種類を選択します。

6. [OK] をクリックして、設定を保存します。

ウイルスが見つかったときに実行する処置

以下の表には様々な処置とその説明を記載しています。

処置	説明
削除	感染したファイルを削除する場合は、このオプションを選択します。感染したファイルは通知なしに削除されます。

隔離	ウイルスが検出された感染アーカイブを隔離したい場合は、このオプションを選択します。
スキップ	感染したファイルに対して処置を実行しない場合は、このオプションを選択します。

スキャンするアーカイブの種類を選択

スキャンプロセス中にスキャンできるアーカイブのリストが表示されます。いくつかの一般的なアーカイブは初期設定で選択されており、必要に応じてカスタマイズすることもできます。

以下の表ではアーカイブのタイプを説明しています。

ボタン	説明
すべて選択	リスト内のアーカイブをすべて選択します。
すべて選択解除	リスト内のアーカイブをすべて選択解除します。

パックファイルのスキャン

パックファイルのスキャンできます。パックファイルとは、たくさんのファイルをまとめたファイル、つまり 1 つのファイルに圧縮してサイズを縮小したファイルです。また、これらのファイルは解凍に他のアプリケーションを必要としません。パックファイルは圧縮と解凍機能を備えています。

パックファイルは他のファイルとともに悪意のあるファイルをパックして、マルウェアを拡散するためのツールとしても利用されます。このようなパックファイルが解凍されると、お客様のコンピュータシステムに被害をもたらす可能性があります。パックファイルのスキャンする場合は、[パックファイルのスキャン] オプションを選択します。

受信ボックスのスキャン

Outlook Express 5.0 以降の受信ボックス (DBX ファイル内) をスキャンできます。KAK、JS.Flea.B 等のウイルスは DBX ファイル内にとどまり、Outlook Express への修正プログラムが適用されない場合に再び出現することがあります。また、UUENCODE/MIME/BinHex (Base 64) でエンコードされた電子メールの添付ファイルもスキャンします。[受信ボックスのスキャン] は初期設定で選択されており、以下の 2 つのオプションが有効になります。

オプション	説明
受信ボックスのクイックスキャン	以前にスキャンしたすべてのメッセージをスキップし、新しいメッセージのみをスキャンします。本オプションは初期設定で選択されています。
受信ボックスの	受信ボックス内のすべてのメールを常時スキャンします。ただし

徹底スキャン	受信ボックスのサイズが大きくなると、スキャンに要する時間も長くなります。
--------	--------------------------------------

ウイルス対策

電子メールの添付ファイル、インターネットからのダウンロード、ファイル転送、ファイル実行等、様々なソースのウイルスがシステムへの侵入を狙っています。ウイルス対策機能によって、ウイルスを継続的に監視できます。重要なのは、前回のスキャンから変更されていないファイルを再スキャンしないという点です。そのため、リソースの使用を抑えられます。

システムを安全に保ち、脅威から守るために、ウイルス対策を常に有効にしておくことをお勧めします。初期設定では、ウイルス対策機能は ON になっています。

ウイルス対策を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [ウイルス対策] を ON にします。
4. [ウイルス対策] をクリックします。
ウイルス対策詳細画面が表示されます。
5. 必要に応じて以下のオプションを設定します。
 - **警告メッセージを表示する** - マルウェア検出等のイベント発生時に警告を表示したい場合は、本オプションを選択します。本オプションは初期設定で選択されています。
 - **ウイルスが見つかったときに実行する処置を選択する** - スキャン中にウイルスが検出されたときに実行する処置を選択します。
 - **処置を実行する前にバックアップを作成する** - 処置を実行する前にファイルをバックアップしたい場合は、本オプションを選択します。バックアップとして保管されたファイルは隔離メニューから復元できます。
 - **脅威が検出されたときの警告音を有効にする** - ウイルスが検出されたときに警告音で通知したい場合は、本オプションを選択します。
6. [変更を保存] をクリックして設定を保存します。

ウイルスが見つかったときに実行する処置

処置	説明
修復	スキャン実行中にウイルスが検出された場合、ファイルを修復します。ファイルを修復できない場合は自動的に隔離します。
削除	ウイルスに感染したファイルを通知なしに削除します。

アクセス拒否	ウイルスに感染したファイルが使用されないよう、アクセスを制限します。
--------	------------------------------------

ウイルス対策を無効にする

システムを安全に保ち、脅威から守るために、ウイルス対策を常に有効にしておくことをお勧めします。ただし、一切利用しないという場合はウイルス対策を無効にできます。ウイルス対策を無効にしても、機能を一時的に利用するオプションが多数用意されており、選択した時間が経過すると自動的に有効になります。

ウイルス対策を無効にするには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [ウイルス対策] を OFF にします。
4. 以下のオプションから 1 つ選択してください。
 - 15 分後に ON にする
 - 30 分後に ON にする
 - 1 時間後に ON にする
 - 次回の再起動後に ON にする
 - 無効のままにする
5. [OK] をクリックして、設定を保存します。

ウイルス対策を無効にすると、ダッシュボードの [ファイルとフォルダ] オプションのアイコンの色が緑から赤に変わり、「システムは安全ではありません」というメッセージが表示されます。

高度な DNA スキャン

DNA スキャンは、システムに潜む悪意のある未知または不明な脅威を検出して除去する、Quick Heal 独自のテクノロジーです。高度な DNA スキャン技術は、きわめて低い誤検出率で疑わしいファイルを捕捉します。さらに、疑わしいファイルを隔離して、システムに被害を及ぼさないようにします。

隔離された疑わしいファイルは、詳細な分析を行うために Quick Heal リサーチラボに送信できます。新しい脅威を監視して、速やかに抑止するために役立てられます。分析が終わると、その脅威は既知の脅威シグネチャデータベースへ追加され、次のアップデートでユーザーに解決策が提供されます。

高度な DNA スキャンを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。

3. [ファイルとフォルダ] 画面で [高度な DNA スキャン] をクリックします。
高度な DNA スキャン詳細画面が表示されます。
4. 必要に応じて以下のいずれかのオプションを選択します。
 - **DNA スキャンを有効にする**: DNA スキャンを有効にする場合は、このオプションを選択します。
 - **挙動検出システムを有効にする**: 挙動検出システムを有効にする場合は、このオプションを選択します。実行中のアプリケーションの挙動が監視されます。[挙動検出レベルの選択] リストから、セキュリティアラートレベル（高、中、低）も選択できます。
 - 高: このセキュリティレベルを選択した場合、Quick Heal AntiVirus は実行中のアプリケーションの挙動を詳細に監視し、アプリケーションに不審な挙動が検出されると警告を發します。警告が増えたり、問題のないファイルでも警告されたりすることがあります。
 - 中: このセキュリティレベルを選択した場合、Quick Heal AntiVirus は実行中のアプリケーションに疑わしい動作を検出すると、警告を送信します。
 - 低: このセキュリティレベルを選択した場合、Quick Heal AntiVirus は実行中のアプリケーションに悪意のある動作を検出したときのみ、警告を送信します。

注意: セキュリティレベルに中または低を選択した場合、**挙動検出システム**はアプリケーションに疑わしい挙動を發見すると、お客様に何らかの処置を促すことなく、バックグラウンドで多数の不明な脅威をブロックします。
 - **ファイルを送信しない**: 疑わしいファイルを Quick Heal リサーチラボに送信したくない場合はこのオプションを選択します。
 - **ファイルを送信する**: 詳細な分析を行うため、Quick Heal リサーチラボに疑わしいファイルを送信する場合は、このオプションを選択します。[ファイル送信時に通知を表示] を選択すれば、ファイルを送信する前にポップアップ画面で送信実行を確認することもできます。



[ファイル送信時に通知を表示] オプションを選択していない場合、Quick Heal は疑わしいファイルを通知せずに送信します。

高度な DNA スキャンは、特性や挙動を調査してファイルを検出します。

特性による検出

毎日、新しい脅威やポリモーフィック型（自身のコードやファイルの情報を変化させる）の脅威が何千も生み出されています。こうした脅威をウイルス定義で検出するには

時間がかかります。高度な DNA スキャンでは、遅延することなくリアルタイムでこうした脅威を検出します。

DNA スキャンが悪意のある新しい脅威をシステム内で発見すると、その疑わしいファイルを隔離し、メッセージとファイル名を表示します。問題のないファイルだと分かった場合は、メッセージボックスのオプションを使って、隔離フォルダからファイルを復元することもできます。

挙動による検出

[**挙動検出システム**] オプションを有効にすると、DNA スキャンはシステム内のアプリケーションの動作を継続的に監視します。アプリケーションの挙動が通常から逸脱した場合や、疑わしい動作をした場合、**挙動検出システム**はそれ以降、システムに被害を与える可能性のある動作を当該アプリケーションに実行させないようにします。

こうしたアプリケーションが検出されると、以下のオプションから適切な処置を実行するように求められます。

- **許可**: アプリケーションの実行を許可する場合は、この処置を実行します。アプリケーションに問題がないと分かっている場合にのみ選択してください。
- **拒否**: アプリケーションの実行をブロックする場合は、この処置を実行します。

疑わしいファイルの送信

疑わしいファイルを自動または手動で送信できます。自動送信では、Quick Heal AntiVirus がアップデートされた際に、DNA スキャンによって疑わしいファイルが新たに隔離されている場合に送信されます。このファイルは暗号化ファイル形式で、Quick Heal リサーチラボへ送信されます。

ただちに送信すべきだと思われる場合は、隔離されたファイルを手動で送信することもできます。以下の方法でファイルを送信できます。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[**ツール**] をクリックします。
3. [クリーニングと復元ツール] から [**隔離ファイルを表示する**] をクリックします。
隔離ダイアログが表示されます。
隔離されたファイルのリストが表示されます。
4. Quick Heal ラボに送信したいファイルを選択し、[**送信**] をクリックします。
5. [**閉じる**] をクリックして隔離ダイアログを閉じます。

疑わしいパックファイルのブロック

疑わしいパックファイルとは、様々な方法で圧縮またはパックされ、さらに暗号化されている悪意のあるプログラムです。これらのファイルが解凍されると、コンピュータシ

システムに深刻な被害を及ぼす可能性があります。本機能によって、このような疑わしいパックファイルを発見してブロックできます。

疑わしいファイルにアクセスされないようにして感染を防ぐために、本オプションは常に有効にしておくことをお勧めします。

疑わしいパックファイルのブロックを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [疑わしいパックファイルのブロック] を ON にします。

疑わしいパックファイルのブロックは初期設定で有効になっています。

自動偽装セキュリティツールスキャン

この機能は、偽装セキュリティツールや偽造アンチウイルスソフトウェアを自動的にスキャンして削除します。本機能を有効にすると、ファイル内に偽装セキュリティツールが潜んでいないかすべてのファイルのスキャンします。

自動偽装セキュリティツールスキャンを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [自動偽装セキュリティツールスキャン] を ON にします。

自動偽装セキュリティツールスキャンは初期設定で有効になっています。

スキャンスケジュール

定期的にスキャンすることで、ウイルスやその他の感染からシステムを守ることができます。スキャンのスケジュール機能によって、システムのスキャンを自動的に開始するスケジュールを定義できます。複数のスキャンスケジュールを定義して、都合に合わせてスキャンを開始できます。

スキャンスケジュールの設定

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で、[スキャンスケジュール] をクリックします。
スキャンスケジュール詳細画面が表示されます。
4. 新しいスキャンスケジュールを設定するには、[新規] をクリックします。

5. [スキャン名] にスキャン名を入力します。
6. [スキャンの頻度] から、お客様の希望に合わせて以下のオプションを選択します。
 - スキャンの頻度：
 - 毎日：毎日システムのスキャンを行う場合は、このオプションを選択します。本オプションは初期設定で選択されています。
 - 毎週：週の特定の曜日にシステムのスキャンを開始する場合は、このオプションを選択します。[毎週] オプションを選択すると、[曜日] ドロップダウンリストが有効になるので、曜日を選択します。
 - スキャン時刻：
 - 最初のブート時に開始：スキャンを行う日の最初の起動時に開始するようにスケジュールします。このオプションを選択した場合、スキャン開始時刻を指定する必要はありません。システムを何時に起動するかにかかわらず、最初にシステムを起動したときにのみスキャンが行われます。
 - 開始時刻指定：一定の時刻にシステムのスキャンを開始したい場合は、このオプションを選択します。このオプションを選択すると、時刻のドロップダウンリストが有効になるので、スキャン時刻を設定します。本オプションは初期設定で選択されています。

また、どのくらいの頻度でスキャンを行うかも、[毎日] と [一定期間ごと] オプションからお選びいただけます。
 - スキャンの優先順位：
 - 高：スキャンを高い優先度で行います。
 - 低：スキャンを低い優先度で行います。本オプションは初期設定で選択されています。
7. [スキャン設定] から、スキャンモードの指定、スキャンの高度な設定、ウイルスが検出されたときに実行する処置、処置を実行する前にファイルのバックアップを作成するかどうかといった設定を行うことができます。初期設定のスキャンで十分にお客様のシステムを安全に保つことができます。
8. [ユーザー名] テキストボックスにユーザー名を、[パスワード] テキストボックスにパスワードを入力します。
9. スキャンが実行されなかった場合に即時スキャンを行う：スケジュールしたスキャンが実行されなかった際にスキャンを開始したい場合は、このオプションを選択します。システムの電源を切っていてスキャンスケジュールが過ぎてしまった場合に役立ちます。後でシステムの電源を入れたときに、自動的に可能な限り早くスキャンスケジュールを開始します。

本オプションは Microsoft Windows Vista 以降のオペレーティングシステムでのみ利用できます。

10. [次へ] をクリックします。

スキャン対象のフォルダを追加するためのスキャンスケジュール設定画面が表示されます。

11. [フォルダを追加] をクリックします。

12. [フォルダの参照] ウィンドウで、スキャンを行うドライブとフォルダを選択します。必要に応じて複数のドライブやフォルダを選択できます。

スキャン対象からサブフォルダを除外する場合は、[サブフォルダを除外] を選択します。[OK] をクリックします。

13. [スキャンスケジュールの設定] 画面で [次へ] をクリックします。

14. スキャンスケジュールの概要が表示されます。確認してから [終了] をクリックして保存し、スキャンスケジュールダイアログを閉じます。

15. [閉じる] をクリックして [スキャンスケジュール] 画面を閉じます。

スキャンスケジュールの編集

必要に応じてスキャンスケジュールを変更できます。スキャンスケジュールを編集するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。

2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。

3. [ファイルとフォルダ] 画面で、[スキャンスケジュール] をクリックします。

スキャンスケジュール詳細画面が表示されます。

4. 編集したいスキャンスケジュールを選択し、[編集] をクリックします。

5. スキャンスケジュールで必要な変更を行い、[次へ] をクリックします。

6. [スキャンスケジュールの設定] 画面で、希望に応じてドライブやフォルダを追加または削除し、[次へ] をクリックします。

7. スキャンスケジュールの変更内容を確認します。

8. [終了] をクリックして、スキャンスケジュールダイアログを閉じます。

9. [閉じる] をクリックして [スキャンスケジュール] 画面を閉じます。

スキャンスケジュールの削除

必要に応じてスキャンスケジュールを削除できます。スキャンスケジュールを削除するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で、[スキャンスケジュール] をクリックします。
スキャンスケジュール詳細画面が表示されます。
4. 削除したいスキャンスケジュールを選択し、[削除] をクリックします。
確認画面が表示されます。
5. [はい] をクリックして、選択したスキャンスケジュールを削除します。
6. [閉じる] をクリックして [スキャンスケジュール] 画面を閉じます。

スキャンスケジュールの設定方法は、[スキャン設定](#)を参照してください。

除外ファイルおよびフォルダ

除外ファイルおよびフォルダ機能では、ファイルとフォルダを指定して、既知のウイルスのスキャン、DNA スキャン、疑わしいパックファイルのスキャン、挙動検出の対象から除外できます。これにより、スキャン済みのファイルや、スキャンする必要がないことが確実に分かっているファイルに対して、不要なスキャンを避けることができます。

以下のスキャンモジュールのスキャン対象からファイルを除外できます。

- スキャナ
- ウイルス対策
- メモリスキャナ
- DNA スキャン

除外ファイルおよびフォルダの設定

除外ファイルおよびフォルダを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で [除外ファイルおよびフォルダ] をクリックします。
除外ファイルおよびフォルダ詳細画面が表示されます。ここで、スキャンの対象から除外されるファイルとフォルダのリストを確認できます。
4. 新しくファイルやフォルダを追加するには、[追加] をクリックします。
新規除外項目画面が表示されます。
5. [項目] テキストボックスにファイルやフォルダのパスを入力します。ファイルやフォルダアイコンをクリックしてパスを選択することもできます。

ファイルやフォルダパスは正しく入力してください。誤ったパスが入力された場合は、メッセージが表示されます。

6. [次から除外する] で、ファイルやフォルダを除外したいモジュールを選択します。既知のウイルス検出、または DNA スキャン、疑わしいパックファイルのスキャン、挙動検出のオプションを選択できます。
7. [OK] をクリックします。
8. [変更を保存] をクリックして設定を保存します。



- 問題のないファイルで既知のウイルス警告が発生する場合は、既知のウイルス検出のスキャンからそのファイルを除外できます。
- 問題のないファイルで DNA スキャン警告が発生する場合は、DNA スキャンからそのファイルを除外できます。

隔離とバックアップ

感染したファイルや疑わしいファイルを安全に分離できます。疑わしいファイルは暗号化形式で隔離し、実行されないようにすることで、感染を防ぎます。

修復前に感染ファイルのコピーが必要な場合は、[スキャン設定] で [処置を実行する前にバックアップを作成する] オプションを選択します。

また、隔離したファイルを隔離フォルダから削除するタイミングを設定することや、必要に応じてファイルのバックアップを保持することもできます。

隔離とバックアップの設定

隔離とバックアップを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ファイルとフォルダ] をクリックします。
3. [ファイルとフォルダ] 画面で、[隔離とバックアップ] をクリックします。
隔離とバックアップ詳細画面が開きます。
4. [一定期間後に隔離/バックアップファイルを削除する] を選択し、隔離フォルダから自動的にファイルを削除する日数を設定します。初期設定では 30 日後が選択されています。
5. 隔離されたファイルを確認するには、[ファイルを表示] をクリックします。隔離ファイルのリストが表示されます。隔離されたファイルに対し、以下の処置を実行できます。
 - 追加：フォルダやドライブから隔離する新しいファイルを手動で追加することができます。

- 削除：隔離ファイルリストからファイルを削除できます。ファイルを削除するには、ファイルを選択して **[削除]** ボタンをクリックします。
- 復元：隔離したファイルを必要に応じて復元できます。ファイルを復元するには、ファイルを選択して **[復元]** ボタンをクリックします。
- すべてを削除：隔離リストからすべての隔離ファイルを削除します。すべてのファイルを削除するには、**[すべてを削除]** ボタンをクリックします。確認メッセージで **[はい]** をクリックして、ファイルをすべて削除します。
- 送信：隔離ファイルを Quick Heal リサーチラボに送信します。ファイルを送信するには、ファイルを選択して **[送信]** ボタンをクリックします。

6. 隔離ダイアログを閉じるには、**[閉じる]** ボタンをクリックします。

電子メール

電子メール機能では、受信するすべての電子メールに対する保護規則を設定できます。電子メールに添付された感染ファイル（マルウェア、スパム、ウイルス）もブロックできます。また、電子メールにマルウェアが検出されたときに実行する処置も設定できます。

[電子メールセキュリティ] には以下の機能が含まれます。

電子メール保護

電子メール保護は初期設定で有効になっています。悪意のある電子メールから受信ボックスを守るために最適な保護が行われています。電子メールを保護するために、電子メール保護機能を常に有効にしておくことをお勧めします。

電子メール保護の設定

電子メール保護を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、**[電子メール]** をクリックします。
3. [電子メール] 画面で、**[電子メール保護]** を ON にします。
電子メール保護は初期設定で有効になっています。
電子メール経由のマルウェアに対する保護が有効になります。
4. 電子メール保護規則をさらに詳しく設定するには、**[電子メール保護]** をクリックします。
5. 電子メールや添付ファイルにウイルスが検出された際にメッセージを表示したい場合は、**[警告メッセージを表示する]** を選択します。



ウイルスに関する警告メッセージには次の情報が記載されています： ウィルス名、送信元電子メールアドレス、件名、添付ファイル名、実行した処置。

6. [ウイルスが見つかったときに実行する処置を選択する] から、[修復] を選択してウイルスが検出された際に電子メールや添付ファイルを修復するか、[削除] を選択して感染した電子メールや添付ファイルを削除することができます。



添付ファイルを修復できない場合は削除します。

7. 処置を実行する前に電子メールのバックアップを作成する場合は、[処置を実行する前にバックアップを作成する] を選択します。
8. [添付ファイル管理設定] から、特定の電子メールの種類や添付ファイルをブロックするオプションを選択します。
9. [変更を保存] をクリックして設定を保存します。

添付ファイル管理設定

<p>複数の拡張子を持つ添付ファイルのブロック</p>	<p>複数の拡張子を持つ電子メールの添付ファイルをブロックします。ワームは通常複数の拡張子を使うため、この機能を使用することでブロックできます。</p>
<p>脆弱性を狙う電子メールのブロック</p>	<p>電子メールクライアントの脆弱性を悪用することのみを目的としている電子メールをブロックします。MIME、IFRAME といった電子メールには通常、脆弱性があります。</p>
<p>添付ファイル管理機能を有効にする</p>	<p>特定の拡張子、またはあらゆる拡張子を持つ電子メールの添付ファイルをブロックします。本オプションを選択すると、以下のオプションが有効となります。</p> <p>すべての添付ファイルのブロック： 電子メールに含まれるすべての種類の添付ファイルをブロックします。</p> <p>ユーザー指定添付ファイルのブロック：</p> <p>特定の拡張子を持つ電子メール添付ファイルをブロックします。本オプションを選択すると、[設定] ボタンが有効になります。さらに詳しく設定するには、[設定] をクリックして以下のオプションを設定します。</p> <ul style="list-style-type: none"> • [ユーザー指定拡張子] から、保持したい拡張子を選択します。これによって、これらの拡張子を持つ電子メール添付ファイルをブロックし、残りの拡張子をすべて削除します。 • ブロックしたい拡張子がリストにない場合、拡張子テキストボックス内に当該拡張子を入力し、[追加] をクリックして、リストに追加します。

-
- [OK] をクリックして変更を保存します。
-

信頼できる電子メールクライアントの保護

電子メールは最も広く使用されているコミュニケーション媒体なので、マルウェアやその他の脅威を運ぶために都合の良い手段として利用されます。ウイルス作成者たちは常に、代表的な電子メールクライアントの脆弱性を利用してウイルスコードを自動的に実行する新しい方法を探しています。また、ワームは独自の SMTP エンジンルーチンを使用して感染を広げます。

信頼できる電子メールクライアントの保護の設定

信頼できる電子メールクライアントの保護を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[電子メール] をクリックします。
3. [電子メール] 画面で [信頼できる電子メールクライアントの保護] を ON にします。
4. 新しい電子メールクライアントを追加するには、[信頼できる電子メールクライアントの保護] をクリックします。

信頼できる電子メールクライアントの保護の詳細画面が開きます。

5. [参照] をクリックし、信頼できる電子メールクライアントを選択します。
6. [追加] をクリックし、電子メールクライアントをリストに追加します。
7. [変更を保存] をクリックして設定を保存します。

スパム対策

スパム対策では、問題のない電子メールと区別して、スパム、フィッシング、アダルトメール等の迷惑メールを除外できます。本機能を常に有効にしておくことをお勧めします。

スパム対策の設定

スパム対策を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[電子メール] をクリックします。
3. [電子メール] 画面で [スパム対策] を ON にします。
4. さらに詳しく設定するには、[スパム対策] をクリックします。

5. [件名にテキストでタグ付けする (推奨)] を選択し、電子メールの件名をスパムとしてタグ付けします。
6. [スパム対策レベル] から対策レベルを設定します。
 - 低 - スпам電子メールの数が少ないか、または明らかにスパム電子メールであると分かるものだけをブロックしたい場合。問題のない電子メールがスパムとして認識される可能性はほとんどありません。
 - 中 (推奨) - 最適なフィルタリングを行います。迷惑メールを多く受信している場合に最適です。ただし、問題のない電子メールの一部がスパムとして認識される可能性があります。初期設定でも選択されている、推奨される対策レベルです。
 - 高 - より厳格なフィルタリング基準を設けていますが、問題のない電子メールもブロックする可能性があるため、理想的な対策レベルではありません。迷惑メールをあまりにも多く受信している場合のみ選択してください。もしくは、別の方法で迷惑メールを阻止することをお勧めします。
7. [電子メールブラックリストを有効にする] を選択し、電子メールアドレスのブラックリストを作成します。ブラックリストに含まれる電子メールアドレスに保護規則が適用されます。
8. [電子メールホワイトリストを有効にする] を選択し、電子メールアドレスのホワイトリストを作成します。ホワイトリストに含まれる電子メールアドレスに保護規則が適用されます。
9. [アンチスパムプラグインを有効にする] を選択して、アンチスパムプラグインに関する保護規則を実施します。
10. [変更を保存] をクリックして設定を保存します。

ブラックリストにおけるスパム対策規則の設定

ブラックリストは、迷惑メールのアドレスのリストです。ブラックリストに含まれる電子メールアドレスから受信した内容はフィルタリングされ、「スパム」とタグ付けされます。

本機能は、お使いのサーバーがオープンメールリレーを使用している場合は特に有効です。オープンメールリレーは不明な送信者からの電子メールを送受信するために使用されます。このメーラーシステムがスパム業者に悪用されることがあります。ブラックリストを使用すれば、電子メールアドレスとドメインによって、迷惑メールや不明な送信者からの電子メールをフィルタリングすることができます。

電子メールアドレスをブラックリストに追加するには、以下の手順に従ってください。

1. スпам対策設定画面で [電子メールブラックリストを有効にする] を選択します。
[カスタマイズ] ボタンが有効になります。
2. [カスタマイズ] をクリックします。

3. ブラックリストのテキストボックスに電子メールアドレスを入力し、[追加] をクリックします。

電子メールアドレスを入力する際、ホワイトリストに入力した電子メールアドレスを入力しないように気を付けてください。誤って入力した場合はメッセージが表示されます。

電子メールアドレスを編集するには、リスト内の電子メールアドレスを選択し、[編集] をクリックします。電子メールアドレスを削除するには、電子メールアドレスを選択し、[削除] をクリックします。

4. [リストのインポート] をクリックしてブラックリストをインポートすることも可能です。

電子メールリストをエクスポート済み、またはアンチスパムデータを保存済みで、それらの電子メールを活用したい場合に非常に便利です。

5. [リストのエクスポート] をクリックしてブラックリストをエクスポートすることも可能です。

リスト内のすべての電子メールアドレスをエクスポートします。後から Quick Heal AntiVirus を再インストールするか、他のシステムにインストールし、同じ電子メールアドレスのリストを使用したい場合に便利です。

6. [OK] をクリックして、設定を保存します。

ホワイトリストに関するスパム対策の設定

ホワイトリストは、信頼できる電子メールアドレスのリストです。ホワイトリストに含まれる電子メールアドレスから受信した内容はスパム対策のフィルタリングポリシーの対象外となり、「スパム」とタグ付けされません。

問題のない電子メールアドレスがスパムとして検出される場合に便利です。あるドメインをブラックリストに登録したものの、そのドメインの特定の電子メールアドレスからの電子メールを受け取りたい場合にも使用できます。

電子メールアドレスをホワイトリストに追加するには、以下の手順に従ってください。

1. スパム対策設定画面で [電子メールホワイトリストを有効にする] を選択します。

[カスタマイズ] ボタンが有効になります。

2. [カスタマイズ] をクリックします。

3. ホワイトリストのテキストボックスに電子メールアドレスを入力し、[追加] をクリックします。

電子メールアドレスを入力する際、ブラックリストに入力した電子メールアドレスを入力しないように気を付けてください。誤って入力した場合はメッセージが表示されます。

電子メールアドレスを編集するには、リスト内の電子メールアドレスを選択し、**[編集]** をクリックします。電子メールアドレスを削除するには、電子メールアドレスを選択し、**[削除]** をクリックします。

4. **[リストのインポート]** をクリックしてホワイトリストをインポートすることも可能です。

電子メールリストをエクスポート済み、またはアンチスパムデータを保存済みで、それらの電子メールを活用したい場合に非常に便利です。

5. **[リストのエクスポート]** をクリックしてホワイトリストをエクスポートすることも可能です。

リスト内のすべての電子メールアドレスをエクスポートします。後から Quick Heal AntiVirus を再インストールするか、他のシステムにインストールし、同じ電子メールアドレスのリストを使用したい場合に便利です。

6. **[OK]** をクリックして、設定を保存します。

ホワイトリストまたはブラックリストにドメインを追加する

ドメインのアドレスをホワイトリストまたはブラックリストに追加するには、以下の手順に従ってください。

1. **[電子メールホワイトリストを有効にする]** か **[電子メールブラックリストを有効にする]** オプションを選択し、**[カスタマイズ]** をクリックします。

2. ドメインを入力し、**[追加]** をクリックします。

ドメインは次の形式で入力してください: *@mytest.com

3. **[OK]** をクリックして変更を保存します。

インターネットとネットワーク

インターネットとネットワークでは、インターネットバンキングやオンラインショッピング、ネットサーフィン等、オンライン活動中に侵入してくる悪意のあるファイルからシステムを守るための保護規則を設定することができます。また、ペアレンタルコントロールを設定してお子様やその他ユーザーのオンライン活動を監視し、見せたくないウェブサイトから守ることもできます。

インターネットとネットワークには以下の機能があります。

ファイアウォール保護

ファイアウォールは、着信および発信ネットワークトラフィックをフィルタリングすることで、侵入者とハッカーからシステムを保護します。コンピュータやシステムに有害と疑われるプログラムがすべてブロックされます。ファイアウォールは、悪意のあるプログラムが外部インターネット接続またはネットワーク内部からシステムに侵入するのを防ぎます。

ファイアウォール保護の設定

ファイアウォール保護を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[インターネットとネットワーク] をクリックします。
3. 切り替えボタンを使用して [ファイアウォール保護] を ON または OFF にできます。
初期設定では、ファイアウォール保護機能は ON になっています。
4. ファイアウォール保護を設定するには、[ファイアウォール保護] エリアのどこかをクリックします。
5. 以下のポリシーに対してファイアウォール保護を設定できます。
 - ファイアウォールのレベル: [低]、[中]、[高]、[すべてブロック] という所定のセキュリティレベルを選択します。
 - トラフィックルール: 着信および発信ネットワークトラフィックのルールを作成します。
 - プログラムルール: インターネットとネットワークにアクセスするプログラムのルールを作成します。
 - ステルスモード: ステルスモードを有効にすると、ネットワーク内のシステムが隠れて他者から見えなくなるため、攻撃を防ぐことができます。

ファイアウォールのセキュリティレベルには以下のものがあります。

- 低: 例外を除くすべての着信および発信接続を許可します。
- 中: 例外を除くすべての着信接続をブロックしますが、すべての発信接続を許可します。
- 高: 例外を除くすべての着信および発信接続をブロックします。
- すべてブロック: すべての着信および発信接続をブロックします。

トラフィックルール

着信および発信ネットワークトラフィックのルールを作成するには、以下の手順に従ってください。

1. [ファイアウォール保護] 画面で、[トラフィックルール] の隣にある [設定] ボタンをクリックします。
2. [トラフィックルールを設定する] ページで、必要に応じて以下を選択します。

- **アラートメッセージを表示する:** 例外ルールに一致する接続にアラートメッセージを表示したい場合、このオプションを選択します。
- **レポートを作成する:** レポートを作成したい場合は、このオプションを選択します。レポートを保存するパスも指定します。
- **例外:** 例外ルールを選択できます。ネットワークトラフィック用の新しい例外ルールを作成することもできます。

3. 設定を保存するには、[OK] をクリックします。

例外ルール

例外ルールを用いて、ネットワークトラフィックを許可またはブロックできます。例外を追加して、IP アドレスおよびポートを介したインバウンドおよびアウトバウンド通信を許可できます。

例外ルールを持ったポリシーを設定するには、以下の手順に従ってください。

1. [例外] で、[追加] をクリックします。
2. [例外の追加/編集] 画面で、[例外名] テキストボックスに名前を入力してプロトコルを選択します。[次へ] をクリックします。
プロトコルには次のものがあります: TCP、UDP、および ICMP。
3. トラフィックの方向を選択して、[次へ] をクリックします。
トラフィックの方向には、インバウンドおよびアウトバウンドがあります。
必要に応じてインバウンドまたはアウトバウンド、またはその両方を選択できます。
4. [IP アドレス] で、IP アドレスまたは IP 範囲を入力して [次へ] をクリックします。
[任意の IP アドレス] を選択すると、すべての IP アドレスがブロックされるため、IP アドレスを入力する必要はありません。
5. [TCP/UDP ポート] で、ポートまたはポート範囲を入力して [次へ] をクリックします。
[すべてのポート] を選択すると、すべてのポートが選択されるため、ポートを入力する必要はありません。
6. [処置] で、[許可] または [拒否] のいずれかを選択します。[終了] をクリックします。

以下の表ではボタンとその機能を説明しています。

ボタン	説明
追加	新しい例外ルールを作成するには、[追加] をクリックします。 [例外の追加/編集] ページで例外ルール名を入力し、TCP、UDP、ICM P からいずれかのプロトコルを選択します。
削除	リストから例外リストを削除できます。ルールを選択して、[削除] をクリックします。
上へ	このボタンを使用すると、選択したルールを上に移動し、優先順位を並び替えることができます。
下へ	このボタンを使用すると、選択したルールを下に移動し、優先順位を並び替えることができます。
デフォルト OK	ルールを初期設定に戻します。 設定を保存します。
キャンセル	設定をキャンセルし、[トラフィックルールを設定する] ダイアログを閉じます。

プログラムルール

プログラムルール機能では、プログラムがインターネットおよびネットワークにアクセスするのを許可またはブロックできます。

プログラムにルールを作成するには、以下の手順に従ってください。

1. [ファイアウォール保護] 画面で、[プログラムルール] の隣にある [設定] ボタンをクリックします。
2. [プログラムルールを設定する] 画面で、[追加] ボタンをクリックしてプログラムを追加します。
実行可能なプログラムのみ追加できます。
3. 追加したプログラムはプログラムリストに記載されます。[アクセス] 欄で、必要に応じてネットワークへのアクセスに [許可] または [拒否] を選択します。
4. 設定を保存するには、[OK] をクリックします。

信頼できるプログラムのみを許可する

信頼できるプログラムとは、確認済みで識別情報が明らかなプログラムです。信頼できないプログラムとは、確認されていない、または疑わしいプログラムです。悪意のあるプログラムは識別情報を隠し、秘密のオペレーションを実行します。こうしたプログラムはネットワークおよびコンピュータに害を及ぼす可能性があります。

[信頼できるプログラムのみを許可する] チェックボックスを選択することで、すべての信頼できないプログラムがインターネットおよびネットワークにアクセスするのを防ぐことができます。

ブラウジング保護

ユーザーが悪意のあるウェブサイトを訪問すると、システムにファイルがインストールされることがあります。こうしたファイルがマルウェアを拡散したり、システムの処理速度を低下させたり、他のファイルを破壊したりします。このような攻撃は、システムに重大な被害を与える可能性があります。

ユーザーがインターネットにアクセスする際に、ブラウジング保護によって悪意のあるウェブサイトブロックします。この機能を有効にすると、アクセスするウェブサイトがスキャンされ、悪意があると判明した場合はブロックされます。

ブラウジング保護の設定

ブラウジング保護を設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[インターネットとネットワーク]** をクリックします。
3. **[インターネットとネットワーク]** 画面で **[ブラウジング保護]** を ON にします。
ブラウジング保護が有効になります。

マルウェア対策

マルウェア対策では、インターネット接続中に、スパイウェア、アドウェア、キーロガー、リスクウェア等の脅威からお使いのシステムを保護できます。

マルウェア対策の設定

マルウェア対策を設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[インターネットとネットワーク]** をクリックします。
3. **[インターネットとネットワーク]** 画面で **[マルウェア対策]** を ON にします。
マルウェア対策が有効になります。

フィッシング対策

フィッシングは詐欺行為であり、通常は電子メールを通して、お客様の個人情報を盗もうとします。通常は、銀行、企業、各種サービス等、大手企業やよく知られたウェブサイトからのメールを装ってメールを送信し、クレジットカード番号、社会保障番号、口座番号、パスワード等の個人情報を入手しようとしています。

フィッシング対策では、フィッシングや詐欺を行うウェブサイトへのアクセスを防止します。ウェブサイトにはアクセス次第、フィッシング行為が行われていないかスキャンし

ます。フィッシング行為が発見された場合はブロックして、フィッシング行為を防止します。

フィッシング対策の設定

フィッシング対策を設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[インターネットとネットワーク]** をクリックします。
3. **[インターネットとネットワーク]** 画面で **[フィッシング対策]** を ON にします。
これでフィッシング対策が有効になります。



フィッシング対策は Quick Heal AntiVirus Pro では利用できません。

ブラウザサンドボックス

インターネットを閲覧する際、どのサイトが信頼できて検証済みか、判断するのは困難です。信頼できるサイトは識別情報を共有し、既知の団体として認証されています。しかし、信頼できないサイトがすべて、偽のサイトやフィッシングサイトではありません。商用ウェブサイト、サプライヤー、ベンダー、サードパーティ、広告、エンターテインメントのウェブサイトが、信頼できないウェブサイトとされている場合があります。

悪意のあるサイトは識別情報を隠し、オペレーションシステムを秘密裏に実行します。こうしたサイトは訪問者の機密認証情報をハッキングしたり、コンピュータを感染させたり、スパムメッセージを拡散したりする場合があります。

ブラウザサンドボックスは、あらゆる悪意のある攻撃からお客様を守ります。この機能によって、すべての信頼できない未確認サイトに対して、厳格なセキュリティポリシーを適用できます。

ブラウザサンドボックスの設定

ブラウザサンドボックスを設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[インターネットとネットワーク]** をクリックします。
3. **[インターネットとネットワーク]** 画面で **[ブラウザサンドボックス]** を ON にします。
4. **[ブラウザサンドボックス]** のセキュリティレベル・ドロップダウンリストから、セキュリティレベルを選択します。

初心者のユーザーには初期設定が最適かつ理想的です。

5. 必要に応じて、以下を実行します。
- インターネットサーフィン中に機密情報（銀行の取引明細書、写真、重要書類）を保護するには、[ブラウザが機密フォルダにアクセスするのを阻止] を選択し、保護したいフォルダを選択します。

ブラウザサンドボックスで実行中のブラウザおよびその他のアプリケーションは、機密フォルダ内のデータにはアクセスできません。これにより、データの漏えいを防ぎます。

- データが操作されるのを防ぐには、[ブラウザが保護されたデータを変更するのを阻止] を選択し、保護したいフォルダを選択します。

保護されたフォルダ内のデータはアクセス可能ですが、操作または変更はできません。

- 閲覧中、特定のフォルダにコンテンツをダウンロードするには、[特定のフォルダにダウンロードを許可] を選択し、フォルダのパスを指定します。

これにより、後で必要になるコンテンツを特定のフォルダにダウンロードできます。

6. [ブラウザウィンドウの周りに緑のボーダーを表示] を選択すると、ブラウザがブラウザサンドボックス内で実行される際に表示します。

本機能は必須ではないので、お好みにより選択しないことも可能です。

7. サンドボックスキャッシュを消去するには、[削除] をクリックします。

これで一時ファイルを消去できます。

8. [変更を保存] をクリックして設定を保存します。



ブラウザサンドボックスは Quick Heal AntiVirus Server Edition では利用できません。

セーフバンキング

オンラインバンキングで口座を確認したり、料金を支払ったり、株を売買したり、複数の口座間で送金を行ったりできます。ネット上で銀行取引を行うユーザーは、バンキングウェブサイトアクセスして身元認証情報を入力し、必要な取引を実行します。

しかしバンキングウェブサイトアクセスの際、偽のバンキングウェブサイトへ誘導されたり、入力した認証情報を詐欺師に盗まれたりする可能性があり、結果的にお金を失うことになりかねません。

セーフバンキングは、お客様の身元や認証情報が危険にさらされうるあらゆる状況からお客様を守ります。セーフバンキングは、安全な環境内でバンキングセッション全体を起ち上げ、お客様の大切なデータを保護します。

セーフバンキングには以下の機能があります。

- 隔離環境でブラウザを起動し、コンピュータがゼロデイマルウェアに感染するのを防ぎます。
- インターネットの様々な脅威から、お客様のバンキング活動を隔離します。
- あらゆるキー入力記録ツールをブロックし、キーロギングから機密データを守ります。
- 安全な DNS を使用してハッキング攻撃を防ぎます。
- 検証済みの安全なウェブサイト以外へのアクセスを防ぎます。

セーフバンキング環境で作業するには、以下の手順に従ってください。

1. [セーフバンキングの設定](#)
2. [セーフバンキングの起動](#)

セーフバンキングの設定

セーフバンキング機能は初期設定で使用可能です。必要に応じてセーフバンキング機能を設定し、セキュリティを強化することもできます。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[インターネットとネットワーク] をクリックします。
3. [セーフバンキング] をクリックします。
4. 必要に応じて以下のオプションを選択します。
 - **DNS ベースの攻撃から保護する**：このオプションを選択して、お客様のシステムが不正なウェブサイトアクセスするのを防ぎます。
 - **クリップボード共有を許可する**：このオプションを選択してクリップボード共有を許可します。
 - **Windows デスクトップとセーフバンキングデスクトップを切り替えるキーボードショートカット**：このオプションを選択して、セーフバンキングデスクトップから Windows デスクトップに切り替えるショートカットキーを作成します。セーフバンキングは隔離環境で起動するため、このウィンドウからシステムやフォルダにアクセスすることはできません。
5. 設定を保存するには、[変更を保存] をクリックします。

セーフバンキングの起動

セーフバンキング機能は個別にアクセスすることができます。デスクトップに Quick Heal AntiVirus をインストールすると、セーフバンキングもインストールされます。デスクトップにはセーフバンキングのショートカットアイコンが作成されます。

セーフバンキングシールド内でウェブサイトを開始するには、以下の手順に従ってください。

1. [セーフバンキング] のショートカットアイコンをクリックします。または、システムトレイの Quick Heal アイコンを右クリックして、[セーフバンキング] をクリックします。
セーフバンキングが起動します。タスクバーにある対応ブラウザを使用して、好きなウェブサイトを開覧できます。
2. [ブックマークを追加] をクリックして、ウェブサイトをブックマークすることもできます。
3. [ブックマークを追加] ダイアログで、安全モードでアクセスしたいウェブサイトの URL を入力します。[保存] をクリックします。
4. [ブックマークを表示] をクリックし、安全なブラウザで実行したい URL をクリックします。



† セーフバンキングは Quick Heal Total Security および Internet Security でのみ利用可能です。

ニュースアラート

ニュースアラートでは、サイバーセキュリティ、ウイルスの脅威、アラートに関する最新情報や、コンピュータ保護に関するその他の重要な情報を得られます。最新情報は、Quick Heal ダッシュボードからもお読みいただけます。ニュースアラートを希望されない場合は、ニュースアラートを無効にします。

ニュースアラートを無効にする

ニュースアラートを無効にするには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[インターネットとネットワーク] をクリックします。
3. [インターネットとネットワーク] 画面で [ニュースアラート] を OFF にします。

不正侵入防衛・検知システム (IDS/IPS)

不正侵入防衛・検知システム (IDS/IPS) によって規則を設定し、IDS/IPS、ポートスキャン攻撃、分散型サービス拒否 (DDoS) などの、望ましくない侵入および攻撃からコンピュータを保護することができます。

[IDS/IPS] を ON にする

IDS/IPS を ON にするには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[インターネットとネットワーク] をクリックします。
3. [インターネットとネットワーク] 画面で [IDS/IPS] を ON にします。

ペアレンタルコントロール

ペアレンタルコントロールによって、お子様やその他ユーザーのインターネット利用を完全に管理できます。お子様がアクセスしていいウェブサイトと、ブロックすべきウェブサイトをご両親が決められます。カテゴリでウェブサイトを制限することも、ウェブサイトを個々に制限することもできます。お子様がインターネットで時間を浪費しないようにするため、お子様がインターネットにアクセスできる時間を設定することもできます。

ペアレンタルコントロールは、ウェブサイトを種類に応じてカテゴリ分けする機能を備えています。ウェブサイトカテゴリをブロックすると、そのカテゴリに含まれるウェブサイトすべてがブロックされます。ウェブサイトを個々に制限することもできます。

さらに、ブロックしたカテゴリの中で、特定のウェブサイトを許可することもできます。例えば、**ストーリーミングメディア**と**ダウンロード**のウェブサイトカテゴリを制限した場合でも、**YouTube** 等へのアクセスを許可できます。お子様のアクセスを適切なウェブサイトのみ限定し、不適切な内容に触れさせたくないお客様に最適です。

ペアレンタルコントロールの設定前に行うべき重要事項!

ペアレンタルコントロール機能から最善の結果を得るために、以下のオプションを設定することをお勧めします。

ステップ 1

Quick Heal AntiVirus をインストールしたコンピュータに管理者としてログインしていることを確認してください。管理者としてログインしていない場合は、管理者アカウントを作成してから設定することをお勧めします。

制限付きのアカウントを作成するユーザーに、管理者のログイン情報を知られないようにしてください。

ステップ 2

標準アカウント（制限付きユーザー）をお子様やその他ユーザーのために作成します。これにより、システムへのお子様のアクセスが制限されます。

ユーザーごとに別の保護ポリシーを適用することもできます。ポリシーには、制限付きユーザーごとのウェブサイト設定や、インターネットアクセスのタイミングおよびスケジュールを設定できます。

ステップ 3

ペアレンタルコントロールの設定をパスワード保護することで、未承認ユーザーによって Quick Heal AntiVirus がシステムから削除されたり、設定が変更されたりすることを防ぎます。

ペアレンタルコントロールの設定

ペアレンタルコントロールを設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ペアレンタルコントロール] をクリックします。
ペアレンタルコントロール設定詳細画面が表示されます。
3. ブロックしたウェブサイトユーザーがアクセスした際にメッセージを表示したい場合は、[アラートメッセージを表示する] を選択します。
4. [設定が適用されるユーザーを選択する] から、以下のオプションのいずれかを選択します。
 - **すべてのユーザーに適用:** すべてのユーザーに同一の設定を適用する場合は、このオプションを選択します。選択すると、[すべてのユーザー] オプションが下に表示されます。
 - **特定ユーザーに適用:** ユーザーごとに異なる設定を適用する場合は、このオプションを選択します。[特定ユーザーに適用] オプションを選択すると、全ユーザーリストが下に表示されます。
5. ウェブサイトへのユーザーのアクセスを制限したり、インターネットのスケジュールを設定したりするには、[すべてのユーザー] をクリックするか、もしくは [設定が適用されるユーザーを選択する] オプションでの選択に応じて表示されるユーザーをクリックします。
保護規則画面が表示されます。
6. 希望に応じて、以下のいずれか、またはすべてのオプションを設定してください。

- **特定のウェブサイトカテゴリへのアクセスを制限する:** ウェブサイトへのアクセスをカテゴリによって制限します。
 - **特定のウェブサイトへのアクセスを制限する:** 特定のウェブサイトへのアクセスのみを制限します。
 - **インターネットアクセス時間のスケジュールを設定する:** お子様やその他ユーザーのインターネットアクセス時間をスケジュールします。
7. [OK] をクリックします。
 8. [変更を保存] をクリックして設定を保存します。



† ペアレンタルコントロールは Quick Heal Total Security および Quick Heal Internet Security でのみ利用可能です。

特定のウェブサイトカテゴリへのアクセスを制限する

広範なウェブサイトカテゴリが用意されており、ユーザーの希望に応じてアクセスの許可および拒否ができるようになっています。ウェブサイトカテゴリを制限すると、当該カテゴリ下にあるすべてのウェブサイトがブロックされます。あるカテゴリ下にあるすべてのウェブサイトへのアクセスを制限または許可したい場合に便利です。

さらに、あるカテゴリ下のほとんどのウェブサイトへのアクセスは制限したいものの、カテゴリ内の一部サイトへのアクセスは許可したいという場合、対象外リストにサイトを追加することができます。

特定のウェブサイトカテゴリへのアクセスを制限するには、以下の手順に従ってください。

1. [設定が適用されるユーザーを選択する] からユーザーをクリックすると表示される保護規則画面で、[特定のウェブサイトカテゴリへのアクセスを制限する] を選択します。

[カテゴリ] ボタンが有効になります。

2. [カテゴリ] をクリックします。

ウェブサイトカテゴリのリストが表示されます。

3. 希望に応じ、各カテゴリの横にある [許可] または [拒否] ボタンをクリックします。初期設定は初心者ユーザーに最適かつ理想的です。

ブロックの対象となっているウェブサイトカテゴリ下にある特定のウェブサイトを対象から外したい場合は、当該サイトを対象外リストに追加してください。例えば、**ストリーミングメディアとダウンロード**のカテゴリをブロックした場合でも、**YouTube** へのアクセスを許可したい場合、対象外リストに **YouTube** を登録することができます。

- ウェブサイトを対象外とするには、[ウェブカテゴリ] ダイアログで [除外] をクリックします。
- ユーザーにアクセスを認めるウェブサイトの URL を [ブロックしたカテゴリから除外する URL (ウェブサイト) のリスト] テキストボックスに入力し、[追加] をクリックします。

同様に、除外リストからあるウェブサイトを外したい場合は、外したい URL を選択し、[削除] をクリックします。[すべてを削除] をクリックすると除外リストの URL がすべて削除されます。

4. [OK] をクリックして変更を保存します。

特定のウェブサイトへのアクセスを制限する

指定したウェブサイトをブロックできます。特定のウェブサイトを制限したい場合や、対象となるウェブサイトが少ない場合に便利です。

また、ウェブサイトが正しいカテゴリに分類されていない場合や、あるウェブサイトカテゴリを制限したのに一部のサイトがブロック対象から漏れている場合にも便利です。

特定のウェブサイトへのアクセスを制限するには、以下の手順に従ってください。

1. [設定が適用されるユーザーを選択する] からユーザーをクリックすると表示される保護規則画面で、[特定のウェブサイトへのアクセスを制限する] を選択します。
[ブロックリスト] ボタンが有効になります。
2. [ブロックリスト] をクリックします。
3. [追加] ボタンをクリックします。

4. [ウェブサイトを入力] テキストボックスにウェブサイトの URL を入力し、[OK] をクリックします。ウェブサイトのすべてのサブドメインをブロックしたい場合は、[サブドメインもブロックする] を選択します。

例えば、**www.abc.com** とそのサブドメインをブロックすると、**mail.abc.com** や **news.abc.com** 等のサブドメインもブロックされます。

5. [OK] をクリックして、設定を保存します。

インターネットアクセス時間のスケジュールを設定する

お子様がインターネットにアクセスできる時間のスケジュールを設定することにより、お子様のインターネット利用時間を完全に管理できます。お子様がインターネットにアクセスできる曜日や時間のスケジュールを設定することが可能です。

インターネットアクセス時間をスケジュールするには、以下の手順に従ってください。

1. [設定が適用されるユーザーを選択する] からユーザーをクリックすると表示される保護規則画面で、[インターネットアクセス時間のスケジュールを設定する] を選択します。
[設定] ボタンが有効になります。
2. [設定] をクリックします。
インターネットアクセスのスケジュールチャートが表示されます。
3. [ユーザーがインターネットにアクセスできるスケジュールを指定する] から、以下のいずれかのオプションを選択します。
 - インターネットへのアクセスを常に許可する: インターネットアクセスに何ら制限を設けない場合は、このオプションを選択します。
 - スケジュールに従って、インターネットへのアクセスを許可する: インターネットアクセスに制限を設ける場合は、このオプションを選択します。
曜日と時間のスケジュールチャートが有効になります。
 - インターネットアクセスを認める曜日と時間を選択します。
選択されたセルは認められたスケジュールとしてハイライトされます。
4. [OK] をクリックして設定を保存します。

管理者アカウントを作成する

システムでのアプリケーションのインストールおよび削除、設定の変更（ペアレンタルコントロールを含む）が可能になります。お客様だけがシステムを完全に管理できるようになります。

管理者アカウントを作成するには、以下の手順に従ってください。

1. [スタート] > [コントロールパネル] をクリックします。
2. [ユーザーアカウント] をクリックします。
3. お客様のユーザー名の下にアカウントタイプが表示されます。アカウントタイプが管理者になっているか確認します。アカウントタイプが管理者でない場合、管理者アカウントに変更する必要があります。

Quick Heal パスワード保護

パスワード保護機能を有効にすると、Quick Heal AntiVirus の設定を守ることができません。パスワード保護により、お客様の設定が未承認ユーザーによって変更されるのを防ぎます。

パスワード保護を有効にするには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。

2. Quick Heal ダッシュボードで、[設定] をクリックします。
パスワード保護は初期設定で無効になっています。
3. [パスワード保護] を ON にします。
パスワード設定画面が表示されます。
4. [新しいパスワードを入力する] にパスワードを入力し、[新しいパスワードを確認する] にもう一度同じパスワードを入力します。
パスワードを初めて設定する場合は、[古いパスワードを入力する] は無効になっています。
5. [変更を保存] をクリックします。

制限付きユーザーアカウントを作成する

制限付きユーザーアカウントは、ユーザーを自身のアカウントのみに制限して、コンピュータをフルコントロールできないようにします。これにより、ユーザーはセキュリティ権限に影響を与えうる変更を行うことができず、コンピュータは保護されます。

制限付きユーザーアカウントを作成するには、以下の手順に従ってください。

Microsoft Windows XP オペレーティングシステムの場合：

1. [スタート] > [コントロールパネル] > [ユーザーアカウント] の順にクリックします。
2. [ユーザーアカウント] から [新しいアカウントを作成する] をクリックします。
3. [アカウント名] を入力し、[次へ] をクリックします。
4. [制限付き] を選択します。
5. [アカウントの作成] をクリックします。

Microsoft Windows Vista/Windows 7 オペレーティングシステムの場合：

1. [スタート] > [コントロールパネル] > [ユーザーアカウント] の順にクリックします。
2. [ユーザーアカウント] から [別のアカウントの管理] をクリックします。
3. [新しいアカウントの作成] をクリックします。
4. [アカウント名] を入力し、[標準ユーザー] を選択します。
5. [アカウントの作成] をクリックします。

外部ドライブとデバイス

外部デバイスを接続すると、システムはそこからウイルスやマルウェアに侵入されるリスクにさらされます。

CD、DVD、USB ドライブ等、外部デバイスに対する保護規則を設定できます。

自動実行保護

USB デバイスや CD/DVD の自動実行機能は、デバイスがコンピュータに接続されるとただちに実行されます。自動実行マルウェアもデバイスから起動され、コンピュータに重大な被害をもたらすマルウェアを拡散する可能性があります。この機能は、自動実行マルウェアからコンピュータを保護します。

自動実行保護の設定

自動実行保護を設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[外部ドライブとデバイス]** をクリックします。
3. **[外部ドライブとデバイス]** 画面で、**[自動実行保護]** を ON にします。

自動実行保護が有効になります。

外部ドライブのスキャン

USB ドライブは、マルウェアをシステムに転送する可能性のある外部デバイスです。外部ドライブのスキャンでは、USB ドライブがお使いのシステムに接続されるとただちにスキャンを開始します。

外部ドライブのスキャンの設定

外部ドライブのスキャンを設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[外部ドライブとデバイス]** をクリックします。
3. **[外部ドライブとデバイス]** 画面で、**[外部ドライブのスキャン]** を ON にします。

外部ドライブのスキャンが有効になります。

4. さらに詳しい設定を行うには、**[外部ドライブのスキャン]** をクリックします。
5. 以下のオプションから 1 つ選択してください。
 - **ドライブのルートにあるファイルのみをスキャン:** ドライブのルートにあるファイルのみをスキャンする場合に選択します。ルートドライブにあるフォルダ内のファイルはスキャンされません。このスキャンは短時間で済みますが、安全性は低下します。本オプションは初期設定で選択されています。

- **ドライブ全体をスキャン:** USB ドライブ上のすべてのファイルをスキャンする
場合に選択します。スキャンには時間がかかりますが安全です。
6. [変更を保存] をクリックして設定を保存します。



データ盗難対策が有効になっており、[外部ドライブへのすべてのアクセスをブロックする] がオプション選択されている場合、外部ドライブのスキャン機能は実行されません。

データ盗難対策

データ盗難対策機能では、システムと外部デバイス (USB ドライブや CD/DVD デバイス等) 間のデータ転送をブロックできます。システムから外部デバイスへ、または外部デバイスからシステムへ、一切のファイルやデータをコピーできなくなります。データのセキュリティを確保するとともに、有害なファイルが転送される可能性を排除します。

データ盗難対策の設定

データ盗難対策を設定するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[外部ドライブとデバイス] をクリックします。
3. [外部ドライブとデバイス] 画面で、[データ盗難対策] を ON にします。
データ盗難対策が有効になります。
4. [データ盗難対策] をクリックし、以下のオプションのいずれかを実施します。
 - **読み取り専用で外部ドライブへの書き込み不可:** USB ドライブや CD/DVD デバイスからシステムへのデータ転送は可能にしつつ、システムからこれら外部デバイスへの転送は許可しません。本オプションは初期設定で選択されています。
 - **外部ドライブへのすべてのアクセスをブロックする:** システムとすべての外部デバイス間のデータ転送をブロックします。
 - **USB ドライブを承認する:** 承認された USB ドライブや CD/DVD デバイスへのアクセスのみを許可したい場合に選択します。本オプションが選択されているときに外部デバイスをシステムに接続すると、外部デバイスへアクセスするためのパスワードの入力が求められます。そのため、承認された外部デバイスへのアクセスのみが許可されます。

設定で Quick Heal パスワード保護が有効になっているときのみ、本オプションを利用できます。

5. [変更を保存] をクリックして設定を保存します。



データ盗難対策は Quick Heal Total Security および Quick Heal Antivirus Server Edition でのみ利用可能です。

Windows Mobile のスキャン

Windows Mobile のスキャンでは、Windows Mobile 搭載端末をスキャンするために USB ケーブルを使って接続するたびに通知を受けるよう規則を設定できます。

Windows Mobile のスキャンの設定

Windows Mobile のスキャンを設定するには、以下の手順に従ってください。

1. Quick Healantivirus を開きます。
2. Quick Heal ダッシュボードで、[外部ドライブとデバイス] をクリックします。
3. [外部ドライブとデバイス] 画面で [Windows Mobile のスキャン] を ON にします。
Windows Mobile のスキャンが有効になります。



Windows Mobile のスキャンは Quick Heal Total Security でのみ利用可能です。

クイックアクセス機能

クイックアクセス機能により、スキャンオプションや PCTuner 等、重要な機能へのクイックアクセスが可能になります。また、Quick Heal の最新情報も表示します。

デスクトップにある Quick Heal セキュアブラウザのショートカットアイコンから、既定のブラウザをサンドボックス内で起動し、安全にブラウジングすることができます。ブラウザサンドボックスを無効にしても、安全なブラウジングが可能です。

スキャン

Quick Heal ダッシュボードには、お客様の都合に合わせてシステムをスキャンできるように、様々なオプションが用意されています。

システム全体、ドライブ、ネットワークドライブ、USB ドライブ、フォルダまたはファイル、特定の場所やドライブ、メモリスキャン、ブートタイムスキャン等、各種スキャンを起動することができます。通常、手動スキャンは初期設定で十分ですが、ご希望に応じてオプションを調整できます。

システム全体のスキャンの実行

システム全体のスキャンでは、コンピュータ上のすべてのブートレコード、ドライブ、フォルダ、ファイル、脆弱性の包括的なスキャンを行うことができます（マップしたネットワークドライブは除きます）。

システム全体のスキャンを開始するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードから、**[スキャン]** > **[システム全体のスキャン]** を選択します。

スキャンが開始されます。

スキャンが完了すると、**[レポート]** でスキャンレポートを閲覧できます。



[システム全体のスキャン] を実行すると、バックグラウンドでは脆弱性スキャンも実行されます。

カスタムスキャンの実行

カスタムスキャンでは、システム上の特定のドライブとフォルダをスキャンすることができます。特定の項目だけをスキャンし、システム全体のスキャンをしたくない場合に便利です。

特定のフォルダをスキャンするには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[スキャン] > [カスタムスキャン] を選択します。
3. スキャンする項目を追加済みの場合は、[カスタムスキャン] 画面にスキャン項目リストが表示されます。まだ項目を追加していない場合や、新しい項目をスキャンしたい場合は、[追加] をクリックしてスキャン項目を追加します。
 - [フォルダの参照] リストから、スキャンを行うフォルダを選択します。
複数のフォルダをスキャン対象として追加できます。選択したフォルダのサブフォルダもすべてスキャンされます。サブフォルダは、必要に応じてスキャン対象から除外できます。サブフォルダを除外するには、[サブフォルダを除外] オプションを選択してから [OK] をクリックします。
4. スキャン項目リストから項目を選択し、[スキャン開始] をクリックします。
スキャンが開始されます。
スキャンが完了すると、レポートメニューでスキャンレポートを閲覧できます。

メモリスキャンの実行

メモリスキャンを実行するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[スキャン] > [メモリスキャン] を選択します。
スキャンが開始されます。
スキャンが完了すると、[レポート] でスキャンレポートを閲覧できます。

スキャン中に以下のフィールドが表示されます。

スキャンされたファイル	スキャンされたファイルの合計数が表示されます。
アーカイブ/バックファイル	スキャンされたアーカイブファイルまたはバックファイル数が表示されます。

検出された脅威	検出された脅威数が表示されます。
DNA スキャン警告	DNA スキャンにより検出されたファイル数が表示されます。
ブート/パーティションウイルス	ブート/パーティションウイルスの数が表示されます。
修復されたファイル	修復された悪意あるファイル数が表示されます。
隔離されたファイル	隔離された悪意あるファイル数が表示されます。
削除されたファイル	削除された悪意あるファイル数が表示されます。
I/O エラー	スキャン中に発生した I/O エラー数が表示されます。
スキャンステータス	実行中のスキャン状況が表示されます。

ブートタイムスキャンの実行

ブートタイムスキャンは、重度に感染したシステムをクリーニングするのに大変便利です。一部のウイルスは、システムの実行中はアクティブになっており、除去することができません。ブートタイムスキャンではそのようなウイルスを除去できます。本スキャンは、Windows NT ブートシェルを用いて次に再起動するときに実行されます。

ブートタイムスキャンを設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[スキャン]** > **[ブートタイムスキャン]** を選択します。
ブートタイムスキャンには以下のオプションがあります。
 - クイックスキャン: システムで事前に定義された、ウイルスのリスクの高い場所のみをスキャンします。
 - システム全体のスキャン: システム全体をスキャンします。時間が長くかかる場合があります。
3. **[はい]** をクリックします。
4. ただちにスキャンを行うためにシステムを再起動するには、**[はい]** をクリックします。後でシステムのスキャンを行うには、**[いいえ]** をクリックします。

注意: ブートタイムスキャンに時間がかかっている場合、または誤って開始した場合は、**[ESC]** キーを押して中止できます。

モバイルスキャンの実行

PC2Mobile スキャン機能は、幅広い携帯電話の機種をスキャンできます。携帯端末をスキャンする前に、以下の条件をご確認ください。

- モバイルスキャン機能は、Microsoft Windows XP、Windows Vista、Windows 7、Windows 8、Windows 8.1 の各 OS に対応しています。
- Windows Mobile 搭載端末 (Windows Mobile バージョン 3.0 以前からバージョン 7.0) では、Windows XP (32 ビット) 用の Microsoft Active Sync 4.5 以降と、Windows Vista、Windows 7、Windows 8、Windows 8.1 オペレーティングシステム用の Windows Mobile デバイスセンターが必要です。
- コンピュータに PCSuite とデバイスドライバをインストールします。デバイスが PCSuite に接続したら、PCSuite を終了します。
Samsung 社製携帯電話には Kies (PCSuite)、Nokia 社製携帯電話には Nokia PCSuite 等、適切な PCSuite をインストールすることをお勧めします。
- Bluetooth 接続をするためには、適切なドライバがインストールされた Bluetooth デバイスがシステムに搭載されている必要があります。
Bluetooth デバイスについては、Microsoft、Broadcom および Widcomm ドライバのみがサポートされています。また、より良い結果を得るために、Microsoft の Bluetooth デバイス用ドライバをインストールすることをお勧めします。
- 携帯端末とコンピュータを Bluetooth およびケーブル接続するためには、一部の携帯電話機種では Quick Heal コネクタをインストールしておく必要があります。
ご使用の携帯端末にインストールする際には、Quick Heal モバイル接続ウィザードが便利です。
- Android 端末をスキャンするには、端末が USB ケーブルで接続され、[USB デバッグ] と [スリープを無効化] オプションが有効になっている必要があります。

PC2Mobile スキャンで携帯端末をスキャンする

PC2Mobile スキャンでは、次の手順で携帯端末をスキャンできます。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[スキャン] をクリックし、次に [モバイルスキャン] を選択します。
3. ケーブルまたは Bluetooth で携帯電話と PC を接続します。
4. [携帯端末を検索] ボタンをクリックします。
5. [検索を開始] ボタンをクリックします。

接続されている携帯電話の機種が検索されます。

6. リストから携帯端末を選択します。[スキャンを開始] をクリックします。

Total Security モバイル接続ウィザードは、選択した機種がコンピュータに接続されているかどうかを確認します。その機種が接続済みとして検出されなかった場合、スキャンは開始されません。

その機種が接続済みとして検出されると、[コネクタのインストール] ボタンが使用できるようになります。携帯端末とコンピュータ間の通信に使用するコネクタ

一を携帯端末にインストールする必要があります。携帯端末にコネクタがインストール済みの場合は、実行されていることを確認してください。

7. お使いの携帯電話に Quick Heal コネクタをインストールする必要がある場合、コネクタのインストールを促すメッセージが表示されます。Quick Heal コネクタをインストールするには、[コネクタのインストール] をクリックします。
8. Android 端末の場合、コネクタがインストールされて携帯端末のスキャンが開始されます。[モバイルスキャン] ウィンドウを閉じるには、[閉じる] をクリックします。

スキャンが完了すると、レポートメニューでスキャンレポートを閲覧できます。



モバイルスキャン機能は Quick Heal Total Security でのみ利用可能です。

Quick Heal PCTuner

Quick Heal Total Security に内蔵された Quick Heal PCTuner は、コンピュータシステムのクリーニングに役立つツールです。インターネットの履歴を削除することで、コンピュータのパフォーマンスを向上させるとともに、お客様のプライバシーを守ります。PCTuner を定期的を使用することにより、システムの最適なパフォーマンスを確保できます。

PCTuner に関する詳細は [Quick Heal PCTuner ダッシュボード](#)を参照してください。

最新情報

[最新情報] セクションは、サイバーセキュリティ、ウイルスの脅威、アラートに関する最新情報や、コンピュータ保護に関するその他の重要な情報を表示します。最新情報を入手するには、ライセンス認証された製品をお使いになっている必要があります。

Quick Heal メニュー

Quick Heal メニューでは、一般設定を調整して、アップデートを自動的に受け取れるようにしたり、Quick Heal AntiVirus の設定をパスワード保護して無許可の人物が変更できないようにしたりできます。プロキシサポートの設定や、リストからレポートを自動的に削除する規則の設定もできます。

設定

設定では様々な保護規則を適用して、Quick Heal からリリースされるアップデートを取得したり、設定をパスワード保護したりできます。あらゆるインシデントについて生成されるレポートを削除する規則も設定できます。ただし初期設定は最適な状態に設定されており、お客様のシステムに完全なセキュリティを提供しています。設定の変更は、どうしても必要なときにのみ行うことをお勧めします。

設定には以下の機能があります。

インポートとエクスポート設定

Quick Heal AntiVirus の各種機能の設定をインポートおよびエクスポートできます。再インストールが必要な場合や、複数のコンピュータを同じ設定にしたい場合に、現在使用しているコンピュータに設定された内容をエクスポートするだけで、対象のコンピュータに簡単にインポートできます。初期設定とお客様の設定の両方をエクスポートできます。

Quick Heal AntiVirus 設定のインポートとエクスポート

Quick Heal AntiVirus の設定をインポートまたはエクスポートするには、以下の手順に従ってください。

1. **Quick Healantivirus** を開きます。
2. Quick Heal ダッシュボードで、**[設定]** をクリックします。
3. 設定画面で **[インポート/エクスポート]** タブをクリックします。

4. インポート/エクスポート設定ダイアログで、以下のいずれかのオプションを選択します。
 - **設定をファイルにエクスポート**: 現在の設定を .dat ファイルにエクスポートできます。
 - **設定をファイルからインポート**: 設定を .dat ファイルからインポートできます。

設定のインポート中に、「**設定されている設定がすべて上書きされます。**」という警告が表示されます。インポートを承諾するには、**[はい]** をクリックします。
5. エクスポートまたはインポートが成功すると、メッセージが表示されます。**[OK]** をクリックしてインポート/エクスポートダイアログを閉じます。



- 設定は、同一系統の製品の同一バージョンからしかインポートできません。例えば、Quick Heal AntiVirus Pro version 16.00 の設定をインポートできるのは、Quick Heal AntiVirus Pro version 16.00 のみです。
- 以下の機能の設定はエクスポートまたはインポートできません。
 - スケジュールスキャン
 - ブラウザサンドボックス
 - パスワード保護

自動アップデート

この機能を利用して、最新のウイルス定義を自動アップデートすることができます。これにより、システムは最新のマルウェアから保護されます。アップデートを定期的に受け取れるように、自動アップデートを常に有効にしておくことをお勧めします。自動アップデートは初期設定で無効になっています。

自動アップデートの設定

自動アップデートの設定を行うには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[設定]** をクリックします。
3. 設定画面で、**[自動アップデート]** を ON にします。
自動アップデートが有効化されます。
4. **[自動アップデート]** をクリックします。

5. Quick Heal AntiVirus のアップデートについて通知を受け取りたい場合は、[アップデート通知ウィンドウを表示する] を選択します。本オプションは初期設定で ON になっています。
6. 以下のオプションからアップデートモードを選択します。
 - インターネットからダウンロード - お使いのシステムにインターネットからアップデートをダウンロードします。
 - 指定したパスからアップデートファイルを選択 - ローカルフォルダやネットワークフォルダからアップデートを選択します。
 - 指定した場所にアップデートファイルをコピー - ローカルフォルダやネットワークフォルダにアップデートのコピーを保存します。
 - Quick Heal AntiVirus の最新バージョンの確認
 - アップグレードが利用可能になったら通知: 新しいアップグレードが利用可能になったときに通知を受けたい場合を選択します。
 - アップグレードを自動的にダウンロード: 新しいアップグレードが利用可能になったときに自動的にシステムへダウンロードしたい場合を選択します。ダウンロード後に手動でインストールして、現在のバージョンをアップグレードする必要があります。
7. [変更を保存] をクリックして設定を保存します。

インターネット設定

インターネット設定では、インターネット接続を使用するために、プロキシのサポートの有効化、プロキシのタイプの設定、IP アドレスとポートの設定ができます。ネットワークでプロキシサーバーをお使いの場合、または Socks バージョン 4 および 5 のネットワークをお使いの場合には、プロキシと SOCKS V4 および SOCKS V5 サーバーの IP アドレス（またはドメイン名）とポートを入力する必要があります。インターネット設定を行う場合、ユーザー名とパスワードの資格情報を入力する必要があります。

Quick Heal AntiVirus の以下のモジュールでは、この変更が必要です。

- 登録ウィザード
- クイックアップデート
- メッセンジャー

インターネット設定

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で [インターネット設定] をクリックします。
4. [プロキシ設定を有効にする] を選択します。

プロキシのタイプ、サーバー、ポート、ユーザー認証情報のテキストボックスが有効になります。

5. [タイプ] リストで、HTTP、SOCKS V4、SOCKS V5 から希望のプロキシタイプを選択します。
6. [サーバー] テキストボックスに、プロキシサーバーの IP アドレスまたはドメインを入力します。
7. [ポート] テキストボックスに、プロキシサーバーのポート番号を入力します。
ポート番号は、HTTP では 80、SOCKS V4 と SOCKS V5 では 1080 に初期設定されています。
8. ユーザー名とパスワードの資格情報を入力します。
9. [変更を保存] をクリックして設定を保存します。

レジストリの復元

レジストリは、Microsoft Windows オペレーティングシステムの設定やオプションを保存するために使用するデータベースです。すべてのハードウェア、ソフトウェア、ユーザー、システムの情報と設定が含まれています。

ユーザーがコントロールパネル、ファイルの関連付け、システムポリシーを変更したり、新しいソフトウェアをインストールしたりすると、その変更が反映されてレジストリに保存されます。マルウェアは一般的にシステムのレジストリを標的とし、オペレーティングシステムやその他のアプリケーションの特定の機能を制限します。マルウェアによって都合良く動作するようにシステムレジストリを変更することがあり、システムに問題を生じさせます。

Quick Heal のレジストリの復元機能は、マルウェアによって変更された重要なシステムレジストリエリアとその他のエリアを復元します。システムレジストリの修復も行います。

レジストリの復元の設定

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で、[レジストリの復元] をクリックします。
4. [重要なシステムレジストリエリアの復元] を選択し、スキャン中に重要なシステムレジストリを復元します。一般的にマルウェアは、特定のタスクを自動的に実行するか、システムアプリケーションによる検出や変更を回避するために、重要なシステムレジストリエリアを改ざんします。例えば、タスクマネージャを無効化したり、レジストリエディタを無効化したりします。

5. [悪意あるレジストリへのエントリを修復する] を選択し、マルウェア関連のエントリがないかシステムレジストリをスキャンします。マルウェアとその関連ファイルはスキャン中に自動的に修復されます。

セルフプロテクション

マルウェア対策の設定をした Quick Heal AntiVirus のファイル、フォルダ、設定、レジストリエントリが何らかの方法で変更または改ざんされないよう、Quick Heal AntiVirus を保護できます。Quick Heal AntiVirus のプロセスとサービスも保護します。セルフプロテクションを常に有効にしておくことをお勧めします。本オプションは初期設定で ON になっています。

セルフプロテクションの設定

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で [セルフプロテクション] を ON にします。

セルフプロテクションは初期設定で有効になっています。

パスワード保護

未承認の人物が Quick Heal AntiVirus の設定を変更しないよう制限し、セキュリティが侵害されないようにします。パスワード保護を常に有効にしておくことをお勧めします。

セーフモード保護

Windows をセーフモードで実行すると、コンピュータは基本的なファイルとドライバのみで起動し、Quick Heal AntiVirus のセキュリティ機能は初期設定で無効になっています。未承認ユーザーがこの状況を利用してデータを盗んだり、Quick Heal AntiVirus の各種機能の設定を変更したりする可能性があります。

未承認ユーザーによるシステムへのアクセスを防ぐために、セーフモード保護を設定できます。設定すると、セーフモードを使用する際にはパスワードの入力が必要になります。

パスワード保護の設定

パスワード保護を設定するには、次の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で [パスワード保護] を ON にします。

パスワード保護設定画面が表示されます。

4. パスワードを初めて設定する場合は [パスワードを入力] に新しいパスワードを入力し、さらに同じパスワードを [パスワードを確認] に入力します。

パスワードを初めて設定する場合は、[古いパスワードを入力する] は無効になっています。

5. [変更を保存] をクリックします。

レポート設定

Quick Heal AntiVirus 製品のすべての活動についてレポートが生成されます。これらのレポートにより、コンピュータがスキャン済みかどうか、マルウェアが検出されなかったか、ブロックしたウェブサイトへのアクセスがあったか等、あらゆる活動の状況を確認できます。

レポートはレポートリストに追加され続けます。規則を設定し、こうしたレポートを自動的に削除する時期を決めることができます。レポート削除の初期設定は 30 日です。必要な場合は、レポートを保持することもできます。

レポート設定を行う

レポート設定を行うには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で [レポート設定] をクリックします。
レポート設定画面が表示されます。
4. [一定期間後にレポートを削除する] を選択し、レポートを自動的に削除する日数を設定します。
[一定期間後にレポートを削除する] を無効にするとレポートは削除されません。
5. [変更を保存] をクリックして設定を適用します。

ウイルス統計レポート

スキャン中に生成されたウイルス検出の統計レポートを Quick Heal リサーチセンターへ自動的に送信できます。

ウイルス統計レポートの設定

ウイルス統計レポートを設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[設定] をクリックします。
3. 設定画面で [ウイルス統計レポート] を ON にします。

ウイルス統計レポートが有効になります。

Quick Heal を遠隔管理

Quick Heal RDM 経由でデバイス上の Quick Heal AntiVirus を管理するには、常に [Quick Heal を遠隔管理] オプションを有効にしておくことが重要です。デバイスを制御したくない場合は、ウェブポータルからこのオプションを無効にすることもできます。

[Quick Heal を遠隔管理] を有効にするには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[**設定**] をクリックします。
3. [**Quick Heal を遠隔管理**] を ON にします。

デバイスを追加していない場合は [Quick Heal 製品を追加する] ページが表示されます。このページにはデバイスを追加する方法の説明と [Quick Heal RDM ポータル](#) へのリンクが表示されます。

Quick Heal リモートデバイスマネジメント

Quick Heal リモートデバイスマネジメント (Quick Heal RDM) はクラウドベースのウェブポータルで、コンピュータ、ノートパソコン、タブレット、スマートフォンなどのデバイスを遠隔で管理・制御できる総合的なモニタリング機能を提供します。

Quick Heal RDM を利用して、デバイスのセキュリティステータス、ライセンス履歴、ライセンス情報を確認したり、ライセンスを更新したりできます。

Quick Heal RDM を活用するには、以下の手順に従ってください。

1. [Quick Heal RDM ウェブポータルでアカウントを作成する](#)
2. [Quick Heal RDM ウェブポータルにデバイスを追加する](#)

Quick Heal RDM ウェブポータルでアカウントを作成する

Quick Heal RDM ポータルでアカウントを作成する前に、有効なプロダクトキーでデバイス上の Quick Heal AntiVirus を有効化する必要があります。Quick Heal AntiVirus を有効化する方法については、「[Quick Heal の登録](#)」を参照してください。

1. デバイスに Quick Heal AntiVirus が登録されると、[Quick Heal RDM サインアップ] 画面が表示されます。サインアップの案内を受け取るには、電子メールアドレスを入力し、[次へ] をクリックします。

Quick Heal RDM アカウントを有効化する方法を説明した電子メールが、お客様の電子メールアドレスに送信されます。

3. 電子メールをチェックして、[有効化] ボタンをクリックするか、記載されているリンクをブラウザにコピーします。

Quick Heal RDM ポータルのパスワード設定ページにリダイレクトされます。

4. パスワードを設定して、**[保存]** をクリックします。

Quick Heal RDM ポータルでアカウントが正常に作成されます。デバイスを管理するには、まず Quick Heal RDM ポータルにデバイスを追加する必要があります。

Quick Heal RDM ウェブポータルでサインアップする

ウェブポータルからも直接 Quick Heal RDM でアカウントを作成することができます。

Quick Heal RDM にサインアップするには、以下の手順に従ってください。

1. 次のウェブサイトです Quick Heal RDM にアクセスします: <https://mydevice.quickheal.com>
2. 右上にある **[サインアップ]** ボタンをクリックします。
3. ユーザー名または電子メールアドレス、有効な携帯番号、プロダクトキーを入力します。
4. 正しい認証コードを入力します。

使用許諾契約書とプライバシーポリシーをよく読みます。

5. **[Quick Heal 使用許諾契約書とプライバシーポリシーに同意する]** オプションを選択します。
6. **[サインアップ]** をクリックします。

Quick Heal RDM アカウントを有効化する方法を説明した電子メールが、お客様の電子メールアドレスに送信されます。

7. 電子メールをチェックして、**[有効化]** ボタンをクリックするか、リンクをブラウザにコピーします。

Quick Heal RDM のパスワード設定ページにリダイレクトされます。

8. パスワードを設定して、**[保存]** をクリックします。

Quick Heal RDM ポータルでアカウントが正常に作成されます。デバイスを管理するには、まず Quick Heal RDM ポータルにデバイスを追加する必要があります。

Google アカウントを利用して Quick Heal RDM ウェブポータルでサインアップする

既存の Google アカウントを利用して、Quick Heal RDM ポータルでアカウントを作成することもできます。

Google アカウントでサインアップするには、以下の手順に従ってください。

1. [Google でサインイン] ボタンをクリックします。
2. 既存の Google アカウントのユーザー名とパスワードを入力します。
サービス契約書とプライバシーポリシーをよく読みます。
3. [同意する] をクリックします。
4. [新規アカウントの作成] ページに、有効な携帯番号とプロダクトキーを入力します。
5. 正しい認証コードを入力します。
使用許諾契約書とプライバシーポリシーをよく読みます。
6. [Quick Heal 使用許諾契約書とプライバシーポリシーに同意する] オプションを選択します。
7. [サインアップ] をクリックします。

Quick Heal RDM ポータルでアカウントが正常に作成されます。この時点から、既存の Google アカウントを使用して Quick Heal RDM アカウントにログオンして、デバイスを管理できます。

Quick Heal RDM に最初にログオンすると、[デバイスの追加] ページを設定する必要があります。デバイスの追加方法は、「Quick Heal RDM にデバイスを追加する」を参照してください。

Quick Heal RDM ウェブポータルにデバイスを追加する

デバイスをリモート管理するには、デバイスを Quick Heal RDM に追加する必要があります。アカウント作成後 Quick Heal RDM ポータルに最初にログオンすると、デバイスを追加するように促されます。

デバイスを追加するには、以下の手順に従ってください。

1. 次のウェブサイトで Quick Heal RDM ポータルにアクセスします: <https://mydevice.quickheal.com>
2. Quick Heal RDM ポータルにログオンします。
[デバイスの追加] ページが表示されます。
3. デバイスの名前を入力し、プロダクトキーを入力します。
好きな名前をデバイスに付けることができます。
4. [追加] をクリックします。
ワンタイムパスワード (OTP) が生成されます。ワンタイムパスワード (OTP) を取得するには、デスクトップアプリケーションに移動して以下の手順を実行します。
 - i. デスクトップで Quick Heal AntiVirus を開き、[設定] をクリックします。
 - ii. [Quick Heal を遠隔管理] を ON にします。

検証が行われ、Quick Heal リモートデバイスウィザードにワンタイムパスワード (OTP) が表示されます。

5. このワンタイムパスワード (OTP) を Quick Heal RDM ウェブポータルに入力し、**[送信]** をクリックします。
これで、デバイスの追加は完了です。
6. ポータルでワンタイムパスワード (OTP) の検証が完了したら、デスクトップの Quick Heal リモートデバイスウィザードで **[次へ]** をクリックします。
7. ウィザードを閉じるには、**[OK]** をクリックします。

初期設定に復元

お客様がカスタマイズした設定を初期設定に戻すことができます。初期設定を変更したものの、十分な保護が行われない場合や、保護が不十分になったと思われる場合にきわめて有用です。システムは初期設定に復元することができます。

初期設定に復元

初期設定を復元するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[設定]** をクリックします。
設定詳細画面が表示されます。
3. **[初期設定の復元]** で **[すべてを初期設定にする]** ボタンをクリックします。
Quick Heal AntiVirus が初期設定に戻ります。

ツール

ツールでは、システムをクリーニングして元の設定に復元する、特定のドライブへのアクセスを防止する、システムを診断する等、様々な操作を実行できます。

ツールには以下の機能があります。

ハイジャック復元

Internet Explorer の初期設定を変更した場合や、マルウェア、スパイウェア、あるいは正規アプリケーションにより設定が変更された場合、ハイジャック復元機能を使用することで初期設定を復元することができます。

Internet Explorer ブラウザの初期設定を復元する他、レジストリエディタやタスクマネージャ等、重要なオペレーティングシステムの設定も復元できます。

ハイジャック復元の使用

ハイジャック復元を使用するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [クリーニングと復元ツール] から、[ハイジャック復元] をクリックします。
4. [ハイジャック復元] 画面で [すべてをチェック] を選択して、リストにあるすべてのブラウザ設定を選択します。
5. [初期設定ホストファイルの復元] を選択して、初期設定ホストファイルを復元します。
6. [重要なシステム設定の復元] を選択して、重要なシステム設定を復元します。
7. 設定の復元を開始するには [今すぐ復元] をクリックします。

初期設定ホストファイルの復元

初期設定ホストファイルには、以下のオプションが含まれています。

IP アドレス	ホストの IP アドレスを入力します。
ホスト名	ホスト名を入力します。
追加	[追加] をクリックし、ホスト情報をリストに追加します。
編集	リストにあるホストを選択し、[編集] をクリックして変更を行います。
削除	リストにあるホストを選択し、[削除] をクリックしてホストを削除します。
OK	[OK] をクリックし、ホストファイルの設定を保存して [ホスト詳細] ウィンドウを終了します。
閉じる	[閉じる] をクリックし、設定を保存せずに [ホスト詳細] ウィンドウを終了します。

重要なシステム設定の復元

この機能には以下のオプションがあります。

すべてをチェック	リストのすべてのシステム設定を復元します。
OK	変更した設定をすべて保存し、[重要なシステム設定] ウィンドウを終了します。
閉じる	設定を保存せずに、[重要なシステム設定] ウィンドウを終了します。

[ハイジャック復元] 画面にあるボタンは以下の通りです。

今すぐ復元	選択した設定の復元を開始できます。
取り消す	現在の画面で行った設定を取り消すことができます。 [取り消す] ボタンをクリックすると、[取り消しを行う] ウィンドウが開きます。初期設定に復元された設定のリストが表示されます。設定を選択するか、[すべてをチェック] を選んですべての設定を選択します。
閉じる	[OK] をクリックして既存の設定に戻します。 設定を保存せずに [ハイジャック復元] ウィンドウを終了します。

追跡クリーナ

ほとんどのプログラムは最近開いたファイルの一覧を内部形式で保存しており、再び素早く開けるようになっています。しかし、複数のユーザーがシステムを利用している場合は、プライバシーの問題が生じます。追跡クリーナは、このような最近使用した (MRU) プログラムの記録をすべて削除し、プライバシーを守ります。

追跡クリーナの使用

追跡クリーナを使用するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [クリーニングと復元ツール] から、[追跡クリーナ] をクリックします。
[追跡クリーナ] 画面が表示されます。最近開いたすべてのプログラムの一覧が表示されます。
4. 記録を削除したいプログラムを選択するか、[すべてをチェック] を選択して一覧のプログラムをすべて選択します。
5. クリーニングを開始するには、[クリーニングを開始する] をクリックします。
6. [追跡クリーナ] ウィンドウを閉じるには、[閉じる] をクリックします。

アンチルートキット

アンチルートキットでは、システム内で活動するルートキットを能動的に検出し、除去します。本プログラムは実行中のプロセスや Windows レジストリ、ファイル、フォルダ等をスキャンして疑わしい行動を特定し、ウイルス定義を使用せずにルートキットを検出します。現在出回っているほとんどのルートキットを検出することはもちろん、今後の出現が予測されるルートキットも検出し、除去できます。

Quick Heal アンチルートキットはオペレーティングシステムについて知識のある人物が使用するか、Quick Heal 技術サポートエンジニアの助けを借りて使用することをお勧めします。本プログラムを誤って使用すると、システムが不安定になる恐れがあります。

Quick Heal アンチルートキットの使用

アンチルートキットを使用するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [クリーニングと復元ツール] から、[アンチルートキット] をクリックします。
アンチルートキットを起動する前に他のすべてのアプリケーションを終了することを勧めるメッセージが表示されます。
4. [アンチルートキット] 画面の左側フレームで、[スキャン開始] ボタンをクリックします。

Quick Heal アンチルートキットは、お使いのシステムで実行中のプロセス、Windows レジストリ、ファイルおよびフォルダにおける疑わしい行動のスキャンを開始します。

スキャンが終了すると、3 つのタブを持つ結果画面が表示されます。

5. 表示された脅威ごとに適切な処置を選択します。例えば、ルートキットのプロセスを終了し、ルートキットのレジストリエントリや、ファイルおよびフォルダの名前を変えることができます。

処置の実行後にシステムを再起動すると、ルートキット除去が実行されます。

<p>スキャンの中止 閉じる</p>	<p>実行中のスキャンを中止することができます。 [アンチルートキット] ウィンドウを閉じます。スキャン実行中に [アンチルートキット] ウィンドウを閉じようとする、スキャンを中止するか確認するメッセージが表示されます。</p>
<p>エラー報告の送信</p>	<p>システム内の感染やその他予期しない状況により Quick Heal アンチルートキットのスキャンが中断してしまふことがあります。この場合、お使いのシステムを再スキャンし、分析のため、エラー報告を Quick Heal チームに送信するように促されます。</p>

[アンチルートキット] 画面の設定機能を用いて、どの項目をスキャンするか選択できます。

Quick Heal アンチルートキットの設定

1. [Quick Heal アンチルートキット] を開きます。
2. [Quick Heal アンチルートキット] 画面で、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. アンチルートキットでは初期設定として自動スキャンが選択されており、システム内の必要な箇所をスキャンするようになっています。

自動スキャン	<p>自動スキャンはアンチルートキットで初期設定として選択されています。自動スキャンでは、Quick Heal アンチルートキットが事前設定したシステム内のエリアをスキャンします。例えば</p> <ul style="list-style-type: none"> • 隠しプロセス • 隠しレジストリエントリ • 隠しファイルおよびフォルダ • 実行可能 ADS
カスタムスキャン	<p>アンチルートキットのスキャン設定を以下のオプションに対してカスタマイズできます。</p> <p>隠しプロセスの検出 - システムにおける隠しプロセスの実行をスキャンします。</p> <p>隠しレジストリ項目の検出 - Windows レジストリの隠し項目をスキャンします。</p> <p>隠しファイルおよびフォルダの検出 - システム内や実行可能 ADS（代替データストリーム）内の隠しファイルやフォルダをスキャンします。以下のオプションから選択できます。</p> <ul style="list-style-type: none"> • オペレーティングシステムがインストールされているドライブのスキャン • すべての固定ドライブのスキャン • ADS（代替データストリーム）内の実行可能 ADS のスキャン
レポートファイルパス	<p>Quick Heal アンチルートキットは実行された場所にスキャンレポートファイルを作成しますが、別の場所を指定することもできます。</p>

代替データストリーム（ADS）の概要

ADS によって、隠されていない通常ファイルとリンク付けられた隠しファイルにデータを保管できます。ストリームは大きさに制限はなく、いくつでも 1 つの通常ファイルにリンク付けることができます。ADS がセキュリティリスクである理由は、ストリームがほぼ完全に隠されていることです。

トロイの木馬やウイルスの作成者がマルウェアを拡散するために、ストリームを利用してウイルス源を隠す可能性があります。

スキャン結果およびルートキットの除去

1. [Quick Heal アンチルートキット] を開きます。
2. [Quick Heal アンチルートキット] 画面の左側のフレームで、[スキャン開始] ボタンをクリックします。
3. Quick Heal アンチルートキットは、お使いのシステムで実行中のプロセス、Windows レジストリ、ファイルおよびフォルダにおける疑わしい行動のスキャンを開始します。

スキャンが終了すると、3 つのタブを持つ結果画面が表示されます。

適切な処置を実行します。システムを再起動すると、ルートキット除去が実行されます。

スキャン結果画面に表示されるタブ

<p>プロセス</p> <p>隠しプロセスの終了</p>	<p>スキャン終了後、Quick Heal アンチルートキットは隠しプロセスを検出し、リストを表示します。[プロセス] タブを選択して終了させることはできますが、プロセスリストに、内容が分かっている信頼できるプロセスが含まれていないことを確かめてください。</p> <p>Quick Heal アンチルートキットはスキャン済みの総プロセス数や検出された隠しプロセス数の概要も表示します。</p> <p>終了させるプロセスリストを選択後、[終了] ボタンをクリックします。プロセスが正常に終了すると、PID (プロセス識別子) フィールドが [該当なし] を表示し、プロセス名に [終了済み] が追加されます。すべての終了されたプロセスは再起動後に名前が変更されます。</p>
<p>レジストリ</p>	<p>プロセススキャン同様、Quick Heal アンチルートキットは隠しレジストリキーのリストを表示します。キー</p>

隠しレジストリキーの名前の変更	<p>を選択して名前を変更することはできますが、名前の変更を行うキーのリストに、内容が分かっている信頼できるレジストリキーが含まれていないことを確かめてください。</p> <p>Quick Heal アンチルートキットはスキャン済みの総レジストリ数や検出された隠しレジストリ数の概要も表示します。</p> <p>名前を変更するキーのリストを選択後、[名前の変更] ボタンをクリックします。オペレーション名を変更すると再起動が必要となるため、キー名の先頭に「Rename Queued」が付加されます。</p>
-----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>ファイルとフォルダ</p> <p>隠しファイルおよびフォルダの名前の変更</p>	<p>同様に、Quick Heal アンチルートキットは隠しファイルおよびフォルダのリストを表示します。[ファイルとフォルダ] タブを選択して名前を変更することはできますが、ファイルとフォルダの一覧に、内容が分かっている信頼できるファイルが含まれていないことを確かめてください。</p> <p>Quick Heal アンチルートキットは、実行可能な代替データストリームの一覧も表示します。</p> <p>また、Quick Heal アンチルートキットはスキャン済みの総ファイル数や検出された隠しファイル数の概要も表示します。</p> <p>名前を変更するファイルおよびフォルダのリストを選択後、[名前の変更] ボタンをクリックします。オペレーション名を変更すると再起動が必要となるため、ファイル名とフォルダ名の先頭に「Rename Queued」が付加されます。</p>
---------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Quick Heal 緊急ディスクを用いたルートキットの除去

ときとして、ルートキットが除去されず、Quick Heal アンチルートキットスキャン中に再度検出されることがあります。このような場合は、Quick Heal 緊急ディスクを用いて適切に除去することもできます。この方法で除去するためには、Quick Heal 緊急ディスクを作成し、そこからお使いのシステムを起動します。

Quick Heal 緊急ディスクを作成し、これを用いてお使いのシステムをクリーニングするには、以下の手順に従ってください。

ステップ 1

Quick Heal 緊急ディスクを作成するには、「緊急ディスクの作成」 p - 76 に記載された手順に従ってください。

ステップ 2

1. [Quick Heal アンチルートキット] を開きます。
2. [Quick Heal アンチルートキット] 画面の左側のフレームで、[スキャン開始] ボタンをクリックします。

Quick Heal アンチルートキットは、お使いのシステムで実行中のプロセス、Windows レジストリ、ファイルおよびフォルダにおける疑わしい行動のスキャンを開始します。

スキャンが終了すると、3 つのタブを持つ結果画面が表示されます。

3. 表示された各脅威に対して適切な処置を実行します。例えばルートキットプロセスを終了したり、ルートキットのレジストリエントリやファイルの名前を変更したりすることができます。

ステップ 3

1. Quick Heal 緊急ディスクを用いてシステムを起動します。
2. Quick Heal 緊急ディスクはお使いのシステムを自動的にスキャンし、ルートキットを除去します。

緊急ディスクの作成

Windows コンピュータシステムを起動し、NTFS パーティションを含むすべてのドライブのスキャン、クリーニングを行える、専用の緊急ブート可能ディスクを作成できます。このディスクを用いて、Windows 内では除去できないウイルス感染源ファイルによって重度に感染したシステムをクリーニングできます。

緊急ディスクは、お使いのシステム上で Quick Heal AntiVirus が使用する最新のウイルスシグネチャパターンファイルで作成されます。

緊急ディスクを作成するには、以下の手順に従ってください。

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [クリーニングと復元ツール] から [緊急ディスクを作成する] をクリックします。
4. [緊急ディスクを作成する] 画面でリンクをクリックし、緊急ツールに必要なパッケージをダウンロードします。

5. ダウンロードしたパッケージをお使いのシステム上（例：c:\¥my documents¥qhempkg）で解凍します。
6. 解凍したパッケージパスを指定し、[次へ] をクリックします。
7. 緊急ディスクを作成するには、画面に表示されたオプションから 1 つを選択します。例えば、[緊急 USB ディスクを作成する] または [緊急 CD/DVD を作成する] を選択します。
8. 緊急ディスクに変換するディスクドライブを選択して [次へ] をクリックします。緊急ディスクが正常に作成されたことを示すメッセージが表示されます。

緊急ディスクを作成する際に覚えておくこと

- ご使用のシステム上に解凍したパッケージのコピーを保管しておくことをお勧めします。
- Windows XP および Windows 2003 オペレーティングシステムでは、**イメージング API バージョン 2.0 のパッチ**をインストールする必要があります。
- USB デバイスや書き換え可能な CD/DVD を使用する際にはデバイスが初期化されるため、バックアップを作成しておいてください。
- USB か CD/DVD からシステムを起動するには、BIOS でブートシーケンスを設定する必要があります。
- スキャン終了後、コンピュータを再起動する前に、緊急 USB ディスクまたは CD/DVD を取り外す必要があります。取り外さないまま再起動すると、ブートシェルで再び起動します。

緊急ディスクの使用

1. CD/DVD または USB ドライブに**緊急ディスク**を挿入します。
2. システムを再起動します。
3. 緊急ディスクは、自動的にすべてのドライブのスキャンを開始します。感染が見つかった場合は、自動的に駆除します。
4. システムを再起動します。

アンチマルウェアの起動

Quick Heal アンチマルウェアは、新型の先端マルウェアスキャンエンジンで、レジストリやファイル、フォルダを高速でスキャンし、スパイウェア、アドウェア、偽装セキュリティツール、ダイアラー、リスクウェア等、システム内に潜む脅威を徹底的に検出して除去します。

Quick Heal アンチマルウェアの開始

Quick Heal アンチマルウェアは、以下の方法で開始できます。


- [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal アンチマルウェア] の順に選択します。
- Windows システムトレイ上の [ウイルス対策] アイコンを右クリックして、[アンチマルウェアを起動] を選択します。
- Quick Heal AntiVirus を開き [ツール] をクリックします。[クリーニングと復元ツール] から [アンチマルウェアを起動] をクリックします。

Quick Heal アンチマルウェアの使用

[Quick Heal アンチマルウェア] 画面で [今すぐスキャン] をクリックし、マルウェアのスキャンを開始します。スキャン中、Quick Heal アンチマルウェアはマルウェアに感染したファイル、フォルダ、レジストリエントリを表示します。スキャンが完了すると、悪意のあるファイル、フォルダ、およびレジストリエントリ内で検出されたすべてのマルウェアのリストが表示されます。

表示されたリストから、ファイル、フォルダ、またはレジストリエントリを除外することができます。除外項目がすべて正規アプリケーションであり、悪意のあるアプリケーションでないことを確認してください。

マルウェアが検出された場合、以下の処置を行うことができます。

クリーニング	システムからマルウェアとその関連ファイルを除去します。特定のファイル、フォルダ、またはレジストリエントリをリストから除外すると、次回以降これらの項目をスキャン対象から外すかどうか問われます。以降のスキャン対象から外す場合は [はい]、今回だけ対象から外す場合は [いいえ] をクリックします。
スキップ	システムに潜むマルウェアに対して何の処置も行いません。
スキャンの中止	スキャンを中止します。
システム復元ポイントをクリーニング前に設定する	システムのクリーニングを始める前に、システム復元ポイントを作成します。Windows システム復元機能を用いて、Quick Heal アンチマルウェアによるクリーニングを行う前の状態に戻すことができます。  [システム復元ポイントをクリーニング前に設定する] 機能は、Windows 2000 オペレーティングシステムではお使いいただけません。
詳細	Quick Heal のウェブサイトが開きます。

隔離ファイルの表示

この機能によって、感染したファイルや疑わしいファイルを安全に隔離できます。ファイルが隔離されると、Quick Heal AntiVirus がファイルを暗号化して隔離ディレクト

リ内に保持します。暗号化形式で保持することで、これらのファイルが実行されることを防ぐため、安全です。隔離機能は、感染したファイルを修復する前にもコピーを取ります。処置を実行する前にファイルのバックアップを作成することもできます。

隔離ファイルの起動

1. Quick Heal AntiVirus を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [クリーニングと復元ツール] から [隔離ファイルを表示する] をクリックします。
すべての隔離ファイルのリストが表示されます。

隔離ダイアログでは以下のタスクも実行できます。

追加	ファイルを手動で隔離します。
削除	隔離ファイルを削除します。
復元	隔離ファイルを元の場所に戻します。
すべてを削除	隔離ファイルをすべて削除します。
送信	隔離ファイルを Quick Heal のリサーチラボに送信し、さらなる分析にかけることが可能です。送信したいファイルを選択し、[送信] をクリックします。

隔離ファイルを Quick Heal リサーチラボに送信する際に、お客様の電子メールアドレスと、ファイルを送信する理由の入力を求められます。理由には、以下のものがあります。

疑わしいファイル	特定のファイルがシステム内の疑わしい行動の原因だと思われる場合に選択します。
修復できないファイル	システム内に潜む悪意のあるファイルを Quick Heal がスキャン中に検出したが、ファイルの感染を修復できない場合に選択します。
誤検出	悪意がなく、お客様がご使用になっており、機能について熟知しているデータファイルが、悪意あるファイルとして Quick Heal AntiVirus に検出された場合に選択します。

USB ドライブの保護

外部ドライブがシステムに接続されると、自動実行機能が自動的に起動し、そのドライブにあるすべてのプログラムも起動します。ドライブには自動実行マルウェアも書き込まれている可能性があり、そのマルウェアはドライブが接続されるとすぐに起動し、シ

システムに拡散します。USB ドライブの保護機能は、自動実行マルウェアから USB デバイスを保護します。

USB ドライブの保護を設定するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [防止ツール] から [USB ドライブの保護] をクリックします。
4. [リムーバブルドライブの選択] 一覧に、お使いのシステムにプラグインされたすべてのリムーバブルドライブが一覧表示されます。ドライブを選択し、[リムーバブルドライブの保護] ボタンをクリックします。

ドライブは別のシステムで使用された場合でも自動実行マルウェアから保護されません。



Quick Heal は USB ドライブの自動実行機能を無効にしておくことをお勧めしておりますが、USB ドライブの自動実行機能を有効にする場合は、ここで記載された手順に従ってください。

System Explorer

このツールは、実行プロセス、インストール済み BHO、Internet Explorer にインストールされているツールバー、インストール済み ActiveX、ホスト、LSP、スタートアッププログラム、Internet Explorer の設定、アクティブなネットワーク接続といった、お使いのコンピュータに関するすべての重要な情報を提供します。このツールは、新しいマルウェアやリスクウェアに関してシステムを診断します。

System Explorer を使用するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [診断ツール] から [System Explorer] をクリックします。

Windows スパイ

Windows スパイでは、アプリケーションまたはプロセスについて詳細な情報を見つけることができます。ときとして、スパイウェアやその他マルウェアがダイアログボックスやメッセージを頻出させているにもかかわらず、それがどこに潜んでいるのか場所の特定ができないことがあります。こうした状況でもこのツールを用いれば、対象を画面上のダイアログやウィンドウまでドラッグすることによりアプリケーションの詳細を確認

することができるようになります。本ツールはダイアログやウィンドウの以下の情報を表示します。

- アプリケーション名
- オリジナルファイル名
- 会社名
- ファイルの詳細
- ファイルのバージョン
- 内部名
- 製品名
- 製品のバージョン
- 著作権情報
- コメント

Windows スパイの使用

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [診断ツール] から [**Windows スパイ**] をクリックします。
4. アプリケーション上にマウスポインタをドラッグします。
ウィンドウが開き、上記の情報が表示されます。
5. アプリケーションやウィンドウを終了したい場合は、[プロセスを終了する] をクリックします。

ファイル拡張子の除外

ファイル拡張子の除外では、ウイルス対策のためにファイルタイプや拡張子の除外リストを作成できます。悪意のある挙動の影響を受けやすいファイルだけにウイルス対策を集中させることができます。

ウイルス対策の除外リストの作成

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、[ツール] をクリックします。
ツール詳細画面が表示されます。
3. [診断ツール] から [**ファイル拡張子を除外する**] をクリックします。
4. ウイルス対策スキャンの対象から外す必要のあるファイル拡張子を入力し、[追加] をクリックします。
5. 追加された拡張子が誤っていた場合、追加した拡張子をリストから選択し、[削除] をクリックして削除します。

6. [OK] をクリックしてリストを保存します。

レポート

Quick Heal AntiVirus は、ウイルススキャン、アップデートの情報、機能の設定変更等、すべての重要な活動についての詳細なレポートを作成し、管理します。

レポートの閲覧が可能な Quick Heal AntiVirus の機能は以下に挙げる通りです。

- スキャナ
- ウイルス対策
- 電子メール保護
- スキャンスケジューラ
- 挙動検出
- クイックアップデート
- メモリスキャン
- フィッシング対策
- レジストリの復元
- ブートタイムスキャナ
- アンチマルウェアスキャン
- ファイアウォール保護
- ペアレンタルコントロール
- IDS & IPS
- ブラウジング保護
- PC2Mobile スキャン
- 脆弱性スキャン

レポートの閲覧

各機能のレポートと統計を閲覧するには、以下の手順に従ってください。

1. Quick Heal antivirus を開きます。
2. Quick Heal ダッシュボードで、[レポート] をクリックします。
レポートリストが表示されます。
3. [レポートリスト] からレポートの閲覧機能をクリックします。

レポート詳細リストが右側のフレームに表示されます。各機能に関するレポート内容には、レポート作成日時や作成理由が記載されます。

ボタン	処置
詳細	リスト内で選択したレコードについての詳細なレポートを表示します。
すべて削除	リスト内のレコードをすべて削除します。
削除	リスト内で選択したレコードを削除します。
閉じる	[レポート] 画面を閉じます。

機能についてレポートの詳細を確認できます。右側のフレームでレポートをクリックすると、詳細な情報が表示されます。レポート詳細画面には以下のオプションがあります。

ボタン	処置
前へ	リストで前にあるレコードの詳細レポートを表示します。 選択したレコードがリスト上で最初のレコードの場合、このボタンは使用できません。
次へ	リストで次にあるレコードの詳細レポートを表示します。選択したレコードがリスト上で最後のレコードの場合、このボタンは使用できません。
印刷	詳細レポートを印刷します。
名前を付けて保存	詳細レポートがテキスト形式 (.txt) でシステム内に保存されます。
閉じる	レポート詳細画面を閉じます。

レポートに関する詳細は、[レポート](#)を参照してください。

ヘルプ

ヘルプ機能では、Quick Heal AntiVirus 機能の使用方法や設定方法、Quick Heal 技術サポートチームからサポートを受ける方法、製品のアップデート方法を知りたいときや、製品のライセンス情報を確認したいときに、ヘルプトピックを参照できます。

ヘルプには以下のオプションがあります。

- **ヘルプ**: 内蔵されているヘルプトピックにアクセスできます。Quick Heal ダッシュボードで、[ヘルプ] > [ヘルプ] を選択します。製品の機能とその利用法に関する説明が記載されている画面が表示されます。(あるいは、F1 キーを押すか、ダイアログの [ヘルプ] ボタンをクリックしてもこのヘルプページが表示されます)
- **システム情報の送信**: お客様のシステムの情報を分析のために Quick Heal に送信します。
システム情報の送信の方法については[システム情報](#)を参照してください。
- **サポート**: 製品やその機能に関する問題に直面したときは、いつでも Quick Heal Technologies (P) Ltd. のカスタマーサービス部門からサポートを受けることができます。サポートには次のオプションがあります: ウェブサポート (FAQ へアクセス)、電子メールサポート、電話サポート、ライブチャットサポート。お客様は、お使いのシステムの情報を Quick Heal に送信し、技術担当者のリモートアクセスによる問題解決を要請することができます。
サポートに関する詳細は、[サポート](#)を参照してください。
- **製品について**: [製品について] セクションには、以下に関する情報が収録されています。
 - Quick Heal のバージョン

- ライセンス情報
- ライセンスの有効期限
- 今すぐアップデートのオプション

さらに [製品について] セクションでは、以下のボタンもお使いいただけます。

<p>今すぐ更新 ライセンス情報</p>	<p>現在購入済みのライセンスを更新できます。</p> <p>このセクションでは、ライセンス情報およびエンドユーザー使用許諾契約書 (EULA) が入手できます。</p> <p>ライセンス情報のアップデート: この機能は、すでにあるライセンス情報を Quick Heal 有効化サーバーと同期する際に役立ちます。既存のサブスクリプションを更新したいのに方法が分からない、または更新時に問題が発生する場合は、お手元のプロダクトキーや更新用コードを Quick Heal サポートチームにお電話でお伝えください。</p> <p>Quick Heal サポートチームがお手元のソフトウェアを更新します。お客様は以下の手順を実行する必要があります。</p> <ol style="list-style-type: none"> 1. インターネットに接続します。 2. [ライセンス情報のアップデート] をクリックします。 3. [続行する] をクリックして、購入済みのライセンスをアップデートします。 <p>ライセンス情報の印刷: [ライセンス情報の印刷] をクリックして、お手持ちの購入済みライセンス情報を印刷します。</p>
<p>今すぐ更新</p>	<p>Quick Heal のウイルスデータベースをアップデートできます。</p>

システム情報

Quick Heal システム情報は、以下の場合に Windows システムの重要な情報を集めるために必要となるツールです。

<p>新しいマルウェアを検出する</p>	<p>本ツールは実行中のプロセス、レジストリ、システムファイル (Config.Sys や、Autoexec.bat 等) から新しいマルウェアを検出するための情報を集めます。</p>
<p>Quick Heal の情報を入手する</p>	<p>インストールされている Quick Heal AntiVirus のバージョンや、その環境設定、隔離ファイルがある場合は隔離ファイルに関する情報を集めます。</p>

システム情報ファイルの送信

本ツールは C:\¥ に INFO.QHC ファイルを作成し、自動的に sysinfo@quickheal.com へ送信します。



INFO.QHC ファイルには、重要なシステム詳細情報とお客様のシステムにインストールされている Quick Heal AntiVirus のバージョン詳細情報がテキスト形式とバイナリ形式で記述されています。ファイルの自動実行（レジストリ、Autoexec.bat、System.ini、Win.ini による）や、実行中のプロセスと対応のライブラリの情報も含まれています。これらの情報を用いて、システム内の新たなマルウェアの有無や、Quick Heal AntiVirus が正しく機能しているかの分析を行います。上述の情報を用いて、より良い、そしてご満足いただけるサービスをお客様に提供しています。このツールは、パスワード等の個人を特定できる情報を収集するものではなく、この情報を第三者と共有または第三者に開示することはありません。当社はお客様のプライバシーを尊重しています。

システム情報の生成

システム情報を生成するには、以下の手順に従ってください。

1. Quick Heal ダッシュボードで、[ヘルプ] > [システム情報の送信] を選択します。
システム情報ウィザードが表示されます。
2. [次へ] をクリックして続けます。
3. システム情報を送信する理由を選択します。システム内に新たなマルウェアの存在が疑われる場合は、[私のシステムが新たなマルウェアに感染したことを疑っています] を選択し、Quick Heal AntiVirus 使用中に問題に直面した場合は、[Quick Heal 使用中に問題が発生しました] を選択します。[コメント] テキストボックスにコメントを入力し、電子メールアドレスも入力します。
4. [終了] をクリックします。
5. システム情報（INFO.QHC）が生成され、Quick Heal 技術サポートに送信されます。

Quick Heal のアップデートとウイルスの除去

Quick Heal AntiVirus のアップデートは、Quick Heal のウェブサイト上で定期的にリリースされます。アップデートには、新しく発見されたウイルスの検出や削除に関する情報が含まれています。新たなウイルスからお使いのシステムを守るために、Quick Heal AntiVirus を定期的にアップデートする必要があります。

Quick Heal AntiVirus の初期設定では、お客様による作業なしに、インターネットから自動でアップデートを取得するように設定されています。ただし、アップデートを定期的に取得するには、システムがインターネットに接続されている必要があります。

アップデートはローカルまたはネットワークパスから適用できますが、当該パスに最新の定義が揃っている必要があります。Quick Heal AntiVirus がインストールされているコンピュータがインターネットに接続されていない場合に便利です。

Quick Heal AntiVirus のアップデートに関する重要事項は以下の通りです。

- Quick Heal AntiVirus のアップデートはすべて、定義ファイルアップデートやエンジンアップデートを含んだ完全なアップデートとなっています。
- Quick Heal AntiVirus のセキュリティアップデートはすべて、必要に応じてお客様のバージョンのアップグレードも行い、これによりお客様のシステムを守るための新しい機能や技術が利用できるようになっております。
- Quick Heal のアップデートは 1 つの作業で完了するアップグレードです。

以下のいずれかの方法により、必要に応じて、手動で Quick Heal AntiVirus をアップデートすることもできます。

インターネットから Quick Heal をアップデートする

[今すぐアップデート] では、ご都合に合わせていつでも手動で Quick Heal AntiVirus をアップデートできます。Quick Heal AntiVirus の初期設定では、インターネットから自動でアップデートされるように設定されています。アップデートを定期的に入手するために、お使いのシステムがインターネットに接続されている必要があります。本機能はあらゆる種類のインターネット接続に対応しています（ダイヤルアップ、ISDN、ケーブル等）。

Quick Heal AntiVirus をアップデートするには、以下の手順に従ってください。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [クイックアップデート] の順に選択します。
2. 手順に従い、[次へ] ボタンをクリックします。
3. [Quick Heal AntiVirus インターネットセンターからダウンロード] を選択します。
4. インターネット接続がアクティブであることを確認し、[次へ] をクリックし、アップデート処理を開始します。
5. クイックアップデートは Quick Heal のウェブサイト接続し、お客様の Quick Heal AntiVirus に適したアップグレードファイルをダウンロードし、その後お客様の Quick Heal に適用することで、最新のファイルにアップデートします。

Quick Heal を定義ファイルを用いてアップデートする

アップデート定義ファイルを持っている場合、インターネットに接続せずに Quick Heal AntiVirus をアップデートできます。これは複数のシステムがネットワークに接続している環境で便利です。Quick Heal AntiVirus を使用しているネットワーク内のすべてのコンピュータにアップデートファイルをダウンロードする必要はありません。Quick Heal のウェブサイト <http://www.quickheal.com/update> から最新の定義ファイルをダウンロードできます。

定義ファイルを使用して Quick Heal AntiVirus をアップデートするには、以下の手順に従ってください。

1. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [クイックアップデート] の順に選択します。
2. 手順に従い、[次へ] ボタンをクリックします。
3. [指定されたパスから選択] を選択します。
4. [ファイル] をクリックして定義ファイルがある場所を指定します。アップデートファイルを選択します。
5. [次へ] をクリックします。

クイックアップデートは指定されたパスから定義ファイルを入手し、インストールされたバージョンへの互換性を確認後に、お客様の Quick Heal AntiVirus をアップグレードします。

ネットワーク環境のアップデートガイドライン

Quick Heal AntiVirus はネットワークを通して簡単にアップデートできるよう設定可能です。最高の結果を得るため、以下のガイドラインに従うことをお勧めしています。

1. マスターアップデート機としてコンピュータ 1 台（サーバー等）をセットアップします。ここでは、サーバー名を「サーバー」とします。
2. ご希望の場所に **Quick Heal UPD** フォルダを作成します。（例：**C:¥QHUPD**）読み取り専用共有権限を本フォルダに割り当てます。
3. [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal AntiVirus] の順に選択します。
4. ダッシュボードで、[設定] > [自動アップデート] を選択します。
5. [指定した場所にアップデートファイルをコピー] を選択します。
6. [参照] をクリックし、**Quick Heal UPD** フォルダの場所を指定します。[OK] をクリックします。
7. [変更を保存] をクリックして設定を保存します。
8. ネットワーク内のすべてのユーザーコンピュータで、**Quick Heal AntiVirus** を起動します。
9. [設定] から [自動アップデート] ページにアクセスします。
10. [指定したパスからアップデートファイル入手] を選択します。
11. [参照] をクリックします。
12. ネットワークコンピュータから [サーバー¥QHUPD] フォルダの場所を指定します。または、[¥¥サーバー¥QHUPD] をパスとして入力することもできます。
13. [変更を保存] をクリックして設定を保存します。

ウイルスの除去

Quick Heal AntiVirus は、以下の場合にウイルス感染の警告を表示します。

- 手動スキャン中にウイルスが検出された場合。
- Quick Heal のウイルス対策/電子メール保護によってウイルスが検出された場合

スキャン実行中に検出されたウイルスの削除

Quick Heal AntiVirus の初期設定は適切に設定されており、システムを保護するのに最適な状態となっています。スキャン中にウイルスが検出されると、Quick Heal AntiVirus はウイルス感染の修復を試みます。感染したファイルを修復できなかった場合は、そのファイルを隔離します。スキャナの初期設定をカスタマイズしている場合、ウイルスが検出されたときには適切な処置を実行してください。

スキャンオプション

スキャン中、必要に応じて以下の処置を実行できます。

[処置] タブ	ファイルに対する処置を表示します。
フォルダをスキップ	現在処理中のフォルダをスキャン対象から外すことができます。スキャン対象が別の場所に移動します。疑わしい項目を含まないフォルダをスキャン中に使用すると便利です。
ファイルをスキップ	現在処理中のファイルをスキャン対象から外すことができます。大量のアーカイブファイルをスキャン中に使用すると便利です。
停止	スキャンプロセスを停止します。
閉じる	スキャンプロセスを終了します。
終了後に PC をシャットダウン	スキャン終了後にシステムをシャットダウンできます。スキャンが完了しない限り作動しません。

メモリ内で検出されたウイルスの除去

「メモリでアクティブなウイルス」とは、ウイルスがアクティブで別のファイルや（ネットワークに接続されている場合）コンピュータに拡散し、悪意のある活動を行っている状態を指します。

メモリスキャン中にウイルスが検出されると、次回起動時にブートタイムスキャンが実行されるよう自動的にスケジュールが設定されます。ブートタイムスキャンはデスクトップがロードを完了する前でも NTFS パーティションを含むすべてのドライブをスキャンしてクリーニングします。最も代表的なルートキットやスパイウェア、特殊な目的を持ったトロイの木馬やロガーも検出して除去します。

一部のマルウェアの除去には再起動が必要

一部のマルウェアは、explorer.exe、Iexplore.exe、svchost.exe といったシステムで実行中のプロセスに自らの DLL をドロップおよび注入します。これらは無効にしたり除去したりできません。メモリスキャン中に検出されると、次回起動時に削除されるよう自動的に設定されます。こうした場合、Quick Heal AntiVirus のメモリスキャンでは詳細情報と推奨される処置を提示します。

ブート/パーティションウイルスの除去

Quick Heal AntiVirus のメモリスキャナがブートウイルスかパーティションウイルスをシステム内に発見すると、安全な起動ディスクを使用してシステムを再起動することを推奨します。Quick Heal 緊急ディスクを使用し、ウイルスをスキャンして除去できます。

ウイルス対策によるウイルス発見アラートへの対応

Quick Heal AntiVirus のウイルス対策は、お客様が作業をしている間もバックグラウンドでシステムのウイルスを継続的にスキャンしています。初期設定では、感染したフ

Quick Heal のアップデートとウイルスの除去

ファイルを自動的に修復します。また、ウイルス対策による処置が実行された後、プロンプトが表示されます。

Quick Heal PCTuner

Quick Heal PCTuner は、Quick Heal Total Security に内蔵されたツールです。インターネットの履歴を削除することで、コンピュータのパフォーマンスを最高水準で維持するとともに、お客様のプライバシーを守ります。PCTuner を定期的を使用することにより、システムの最適なパフォーマンスを確保できます。



PCTuner は Quick Heal Total Security でのみ利用可能です。

Quick Heal PCTuner ダッシュボード

Quick Heal PCTuner ダッシュボードは、PCTuner アプリケーションを開いたときに表示される初期設定のインターフェースです。ダッシュボードには、これまでに取られた処置とその時点で保留になっている処置についての情報が表示されます。

PCTuner にアクセスするには、以下の手順に従ってください。

- [スタート] > [プログラム] > [Quick Heal AntiVirus] > [Quick Heal PCTuner] の順に選択します。

Quick Heal PCTuner のメインウィンドウが表示されます。

Quick Heal PCTuner では以下の機能を利用できます。

メニュー	機能
ダッシュボード	実行中のスキャンのステータスが表示されます。
チューンアップ	不要なファイル、無効なレジストリ、閲覧履歴等のシステムクラッターをクリーンアップします。
ツール	ハードディスクからファイルを安全に削除するためのツールが含まれます。
レポート	実行された様々なチューンアップ活動に関するレポートを提供します。
復元	チューンアップ中に削除された項目を復元します。

バージョン情報	ソフトウェアに関する情報やサポート情報を提供します。
ヘルプ	ヘルプトピックを確認できます。F1 キーを押してヘルプトピックを表示することもできます。

各機能の項目のリストは以下の通りです。



メニュー	メニュー項目
ダッシュボード	ステータス
チューンアップ	自動チューンアップ ディスクのクリーンアップ レジストリのクリーンアップ 履歴のクリーンアップ デフラグ スケジューラ 設定
ツール	重複ファイルファインダ 安全な削除 スタートアップブースター サービスオプティマイザ
レポート	自動チューンアップ ディスクのクリーンアップ レジストリのクリーンアップ 履歴のクリーンアップ スケジューラ 安全な削除 重複ファイルファインダ スタートアップブースター サービスオプティマイザ
復元	復元 ディスク/レジストリ スタートアップブースター
バージョン情報	情報

ステータス

PCTuner による特定のチューンアップ活動に関して、システムの最新の状況をステータスメーターで表示します。チューンアップ活動には以下の機能があります。

- ディスクのクリーンアップ
- レジストリのクリーンアップ
- 履歴のクリーンアップ
- デフラグ

すべてのチューンアップ活動を定期的に行っている場合に限り、ステータスメーターのポインタが深緑色を指します。ステータス機能は、以下の形式でもチューンアップ活動のステータスを表示します。

チューンアップ活動	チューンアップ活動の名前（ディスクのクリーンアップ、レジストリのクリーンアップ、履歴のクリーンアップ、デフラグ）。
前回実行日	各チューンアップ活動の前回実行日。一回も実行されていないチューンアップ活動は「未実行」と表示されます。 3 番目の欄には各チューンアップ活動に対して記号が表示されます。  は、該当するチューンアップ活動が未実行であるか、過去 15 日間実行されていないことを示します。  は、該当するチューンアップ活動が過去 15 日以内に実行されたことを示します。
[今すぐチューンアップ] ボタン	スキャンをカスタマイズする場合は、高度な設定モードを選択します。経験があるユーザーのみに理想的なオプションです。本オプションを選択すると、「設定」ボタンが有効になります。



デフラグのスケジュールを設定すると、「次回起動時にデフラグが実行されるように設定されました」というメッセージが表示されます。

チューンアップ

不要なファイル、無効なレジストリ、閲覧履歴等のシステムクラッターをクリーンアップします。チューンアップには以下のオプションがあります。

自動チューンアップ

自動チューンアップは、ディスクのクリーンアップ、レジストリのクリーンアップ、履歴のクリーンアップ、デフラグを実行します。初心者ユーザーや、クリーンアップ活動を個別に実行する時間を節約したいユーザーに理想的なオプションです。復元できるのは、ディスクのクリーンアップやレジストリのクリーンアップにより削除された項目のみです。

自動チューンアップのカスタマイズ

自動チューンアップを実行する前に、必要に応じて自動チューンアップをカスタマイズします。自動チューンアップをカスタマイズするには、以下の手順に従ってください。

1. [チューンアップ] > [設定] の順に選択します。

[チューンアップ設定] 画面が表示されます。この画面には 3 つのタブ、[ディスク設定]、[レジストリ設定]、[履歴設定] があります。各タブには項目のリストがあり、チェックボックスが付いています。各タブの初期設定は、すべての項目が選択されています。

2. 自動チューンアップをスキップする必要がある項目は、チェックボックスのチェックマークを外してください。初心者ユーザーの場合は、すべての項目を選択したままにすることをお勧めします。

[削除する前にバックアップを作成] は初期設定で選択されています。本オプションが選択されていない場合は、バックアップが作成されなまますべての項目を削除します。本オプションは、選択したままにしておくことをお勧めします。

3. [適用] をクリックして設定を保存します。
4. または、[閉じる] をクリックして設定を保存せずに終了します。

自動チューンアップの実行

自動チューンアップを実行するには、以下の手順に従ってください。

1. [チューンアップ] > [自動チューンアップ] の順に選択します。
2. 前のセクションに記載されている自動クリーンアップのカスタマイズを行う場合は、[設定] をクリックします。
3. [スタート] をクリックして、自動チューンアップを開始します。
4. 自動チューンアップを中止する場合は [中止] をクリックします。自動チューンアップが完了したら、[閉じる] をクリックします。

ディスクのクリーンアップ

ハードディスクドライブから無効なファイルや不要なファイルを見つけて削除します。これらのファイルは、ハードディスクの空き容量を占有するとともに、システム速度を大幅に低下させます。これらのファイルを削除することによって、空き容量を確保し、システムパフォーマンスを向上させます。一時ファイル、インターネットキャッシュファイル、不適切なショートカットファイル、無効な名称のファイル、空のフォルダも削除します。

ディスクのクリーンアップの実行

ディスクのクリーンアップを実行するには、以下の手順に従ってください。

1. [チューンアップ] > [ディスクのクリーンアップ] の順に選択してください。
2. [設定] をクリックすると、ディスクのクリーンアップのカスタマイズを行うことができます。
3. [スタート] をクリックします。
ファイル保管場所と削除対象カテゴリのリストが表示されます。
4. [停止] をクリックして、リストに追加されたエントリを中断することができます。
各ファイル保管場所の先頭にチェックボックスが表示されます。すべてのファイル保管場所が初期設定で選択されています。
5. ディスクのクリーンアップをスキップする必要がある場所は、チェックボックスのチェックマークを外してください。
以下の情報を表示するその他 4 つのフィールドがあります。
 - **検出されたファイル:** ディスクのクリーンアップによって検出されたファイルの合計数。
 - **合計サイズ:** ディスクのクリーンアップによって検出されたファイルの合計サイズ。
 - **選択されたファイル:** 削除の対象として選択されたファイルの数。
 - **選択されたファイルのサイズ:** 削除の対象として選択されたファイルのサイズ。
6. [ファイルを削除] をクリックしてファイルを削除します。
7. [閉じる] をクリックしてディスクのクリーンアップを終了します。

レジストリのクリーンアップ

適切に実行されなかったアンインストールや存在しないフォント等によって表示される、無効であるかまたは古くなったレジストリエントリをシステムから削除します。ときには、アンインストール実行中にレジストリエントリが削除されないことがあります。その結果、システムパフォーマンスが遅くなることがあります。レジストリのクリーンアップは、このような無効なレジストリエントリを削除し、システムパフォーマンスを向上させます。

レジストリのクリーンアップの実行

レジストリのクリーンアップを実行するには、以下の手順に従ってください。

1. [チューンアップ] > [レジストリのクリーンアップ] の順に選択してください。
2. [設定] をクリックすると、前のセクションに記載されているレジストリのクリーンアップのカスタマイズを行うことができます。
3. [スタート] をクリックします。

レジストリエントリとそのパスのリストが表示されます。

4. [停止] をクリックして、リストに追加されたエントリを中断することができます。各レジストリエントリの先頭にチェックボックスが表示されます。すべてのレジストリエントリが初期設定で選択されています。
5. レジストリのクリーンアップをスキップする必要があるレジストリエントリは、チェックボックスのチェックマークを外してください。
6. 以下の情報を表示するその他 2 つのフィールドがあります。
 - **検出された項目:**レジストリのクリーンアップによって検出されたレジストリエントリの合計数。
 - **選択された項目:**削除の対象として選択されたレジストリエントリの合計数。
7. [エントリを削除] をクリックしてファイルを削除します。
8. [閉じる] をクリックしてレジストリのクリーンアップを終了します。

履歴のクリーンアップ

様々なアプリケーションの MRU (最近使用した) リストやインターネット閲覧履歴を削除します。安全に履歴を削除し、クッキー、キャッシュ、自動入力フォーム、パスワードを削除します。ユーザーのプライバシーが侵害されないようにするには、自動入力エントリや保存されたパスワード等の履歴を削除する必要があります。Microsoft Office の各種アプリケーション、Adobe Acrobat Reader、Media Player、WinZip、WinRAR 等の一般的によく使用されているアプリケーションの履歴、ブラウザクッキー等の履歴、保存されたパスワード等も削除します。

履歴のクリーンアップの実行

履歴のクリーンアップを実行するには、以下の手順に従ってください。

1. [チューンアップ] > [履歴のクリーンアップ] の順に選択してください。
2. [設定] をクリックすると、前のセクションに記載されている履歴のクリーンアップのカスタマイズを行うことができます。
3. [スタート] をクリックします。
履歴が含まれるアプリケーションのリストが表示されます。
4. [停止] をクリックして、リストに追加されたエントリを中断することができます。各対象アプリケーションの先頭にチェックボックスが表示されます。すべての対象アプリケーションが、初期設定で選択されています。
5. 履歴のクリーンアップをスキップする必要があるアプリケーションは、チェックボックスのチェックマークを外してください。
6. 以下の情報を表示するその他 2 つのフィールドがあります。

- 検出された項目の合計: 検出された履歴を含むアプリケーションの合計数。
 - 選択された項目: 削除の対象として選択された履歴を含むアプリケーションの合計数。
7. [項目を削除] をクリックして、リストに掲載されているアプリケーションから履歴を削除します。
 8. [閉じる] をクリックして履歴のクリーンアップを終了します。

デフラグ

システムのパフォーマンスを向上させるために、ページファイルやレジストリハイブ等の重要なファイルのデフラグを行います。ファイルはフラグメント（断片）としてばらばらな場所に保管されることが多いため、システムパフォーマンスの低下につながりません。デフラグはフラグメント数を減らし、すべてのフラグメントを 1 つの連続した塊にまとめることでシステムパフォーマンスの向上を実現します。

デフラグの使用

ページファイルやレジストリハイブのデフラグを行うには、以下の手順に従ってください。

1. [チューンアップ] > [デフラグ] を選択します。
次の 2 つのオプションが表示されます。[デフラグを有効にする] と [デフラグをキャンセルする] が表示されます。[デフラグをキャンセルする] は初期設定で選択されています。
2. [次回起動時にデフラグを実行する] を選択して次回起動時にデフラグを実行するか、または [起動するたびにデフラグを実行する] を選択してシステムを起動するたびにデフラグを行います。
3. [システムページングファイル（仮想メモリ）のデフラグ] と [Windows レジストリのデフラグ] は初期設定では選択されていません。これらのいずれかまたは両方を選択して、デフラグを実行することができます。これらのオプションは、選択したままにしておくことをお勧めします。
4. [適用] をクリックして設定を保存するか、または、[閉じる] をクリックして設定を保存せずに終了します。

スケジューラ

必要に応じて、チューンアップ活動を定期的に行うようスケジュールを設定することができます。ディスクのクリーンアップ、レジストリのクリーンアップ、履歴のクリーンアップ、デフラグを実行するために、チューンアップのスケジュールを設定します。タスクを作成し、そのスケジュールを設定することもできます。タスクは、作成時に指

定した時間に、バックグラウンドで実行されます。実行されたタスクの詳細は、スケジューラレポートで確認することができます。

スケジューラのカスタマイズ

スケジューラをカスタマイズして、チューンアップを都合の良い時間に実行することができます。ただし、デフラグのスケジュールを設定できるのは、次回の起動時のみです。スケジューラをカスタマイズするには、以下の手順に従ってください。

1. [チューンアップ] > [スケジューラ] の順に選択します。

タスクのリストが、タスク名、実行頻度、活動、バックアップ、最も古いバックアップの削除等の詳細とともに表示されます。
2. チューンアップのスケジュールを設定する際に、以下の 3 つのオプションを選択することができます。
 - i. **新規** - 新しいタスクを設定します
 - ii. **編集** - 既存タスクを編集します
 - iii. **削除** - すでにスケジュールが設定されているタスクを削除します
3. 新しいチューンアップスケジュールを設定するには、[新規] をクリックします。

チューンアップスケジュール設定画面が表示されます。
4. [タスク名]、[実行頻度]、[開始時刻] のボックスに情報を入力します。

各チューンアップ活動の先頭にチェックボックスが表示されます。すべての項目が、初期設定で選択されています。
5. スケジューラ機能をスキップする必要のある項目は、チェックボックスのチェックマークを外してください。
6. [クリーンアップする前にバックアップを作成] は初期設定で選択されています。本オプションが選択されていない場合は、バックアップが作成されないままクリーンアップが実行されます。本オプションは、選択したままにしておくことをお勧めします。バックアップが上限を超える場合は、[バックアップの上限を超える場合は最も古いバックアップを削除する] 機能によって最も古いバックアップが削除されます。
7. ユーザー名とパスワードを入力してください。
8. [適用] をクリックして新しい設定を保存するか、または、[閉じる] をクリックして設定を保存せずに終了します。



[バックアップの上限を超える場合は最も古いバックアップを削除する] を選択しないままにしておく、バックアップの上限を超える場合にスケジューラが機能しません。

設定

必要に応じて、ディスクのクリーンアップの設定、レジストリのクリーンアップの設定、履歴のクリーンアップの設定をカスタマイズすることができます。

ディスクのクリーンアップのカスタマイズ

必要に応じて実行するようディスクのクリーンアップを事前にカスタマイズできます。ディスクのクリーンアップをカスタマイズするには、以下の手順に従ってください。

1. **[チューンアップ]** > **[設定]** の順に選択します。
[チューンアップ設定] 画面が表示されます。
2. **[ディスク設定]** をクリックします。
各項目の先頭にチェックボックスが表示されます。すべての項目が、初期設定で選択されています。
3. ディスクのクリーンアップをスキップする必要がある項目は、チェックボックスのチェックマークを外してください。
4. **[項目を削除する前にバックアップを作成]** は初期設定で選択されています。本オプションが選択されていない場合は、バックアップが作成されなまますべての項目を削除します。本オプションは、選択したままにしておくことをお勧めします。
5. **[適用]** をクリックして新しい設定を保存するか、または、**[閉じる]** をクリックして設定を保存せずに終了します。

レジストリのクリーンアップのカスタマイズ

必要に応じて実行するようレジストリのクリーンアップを事前にカスタマイズできます。レジストリのクリーンアップをカスタマイズするには、以下の手順に従ってください。

1. **[チューンアップ]** > **[設定]** の順に選択します。
[チューンアップ設定] 画面が表示されます。
2. **[レジストリ設定]** をクリックします。
各項目の先頭にチェックボックスが表示されます。すべての項目が、初期設定で選択されています。
3. レジストリのクリーンアップをスキップする必要がある項目は、チェックボックスのチェックマークを外してください。
4. **[項目を削除する前にバックアップを作成]** は初期設定で選択されています。本オプションが選択されていない場合は、バックアップが作成されなまますべての項目を削除します。本オプションは、選択したままにしておくことをお勧めします。

5. [適用] をクリックして新しい設定を保存するか、または、[閉じる] をクリックして設定を保存せずに終了します。

履歴のクリーンアップのカスタマイズ

必要に応じて実行するよう履歴のクリーンアップを事前にカスタマイズできます。履歴のクリーンアップをカスタマイズするには、以下の手順に従ってください。

1. [チューンアップ] > [設定] の順に選択します。
[チューンアップ設定] 画面が表示されます。
2. [履歴設定] をクリックします。
各項目の先頭にチェックボックスが表示されます。すべての項目が、初期設定で選択されています。
3. 履歴のクリーンアップをスキップする必要がある項目があれば、チェックマークを外します。
4. [項目を削除する前にバックアップを作成] が選択されています。本オプションが選択されていない場合は、バックアップが作成されないまますべての項目を削除します。本オプションは、選択したままにしておくことをお勧めします。
5. [適用] をクリックして新しい設定を保存するか、または、[閉じる] をクリックして設定を保存せずに終了します。

ツール

システムから重複ファイルを削除します。ファイルが恒久的に削除され、復元用ソフトウェアを使用しても復元できない安全な削除を行います。ツールメニューには以下のオプションがあります。

重複ファイルファインダ

様々な定義済みファイルカテゴリから重複するファイルを削除します。ユーザーが指定した場所で重複ファイルを検索します。重複ファイルのスキャンを省略するフォルダ除外リストを指定することもできます。重複ファイルは、お客様の希望に合わせて、ワンパス、ツーパスまたは DoD 削除方式を用いて削除されます。初期設定ではワンパス削除方式が選択されています。

重複ファイルファインダの実行中にスキャンされる定義済みファイルカテゴリは以下の通りです。

ファイルカテゴリ	拡張子
画像/写真ファイル	.pcx, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wm p, .png, .tif
クリエイティブア	.ai, .eps, .pcx, .psd, .tiff, .wpg, .bmp, .gif, .

ネットワークファイル	.jpg, .jpeg, .wmp, .png, .cdr, .pdf, .tif
動画ファイル	.avi, .rm, .vob, .mov, .qt, .mpeg, .mpg, .mpe, .mpa, .dat
音声ファイル	.wmv, .wma, .mp4, .mp3
テキストファイル	.txt, .asci, .xml
ドキュメントファイル	.pdf, .doc, .rtf, .wri, .sam, .dox, .xls, .ppt, .docx, .xlsx, .pptx, .wk3, .wk4, .vsd, .vsdx, .wpg, .123, .wpd
電子メールファイル	.eml

重複ファイルの削除

重複ファイルの削除を行うには、以下の手順に従ってください。

1. [ツール] > [重複ファイルファインダ] の順に選択します。
2. 重複ファイルファインダ設定を変更するには、[オプション] をクリックします。
[Quick Heal 重複ファイルファインダオプション] ウィンドウが表示されます。
3. [重複カテゴリタイプを選択してください] リストで、スキップする必要のあるカテゴリがあれば、チェックマークを外します。
除外フォルダリストで、重複ファイルファインダの対象外とする除外リストを追加できます。
4. [フォルダを追加] ボタンをクリックして除外する場所を追加します。追加した場所が正しくなかった場合は、その場所を選択してから [クリア] をクリックします。追加した除外場所をすべて削除するには、[すべてクリア] をクリックします。
[安全な削除を使う] オプションが有効になります。初期設定では [ワンパス削除方式 - 迅速なデータ破壊] 削除方式が選択されています。すべての削除方式が選択可能です。様々な削除方式について知るには、「削除方法」を参照してください。
5. [適用] をクリックして設定の変更を保存するか、または [閉じる] をクリックして、変更された設定を保存せずに終了します。
6. [パスを追加] をクリックして、重複ファイルを検索するためのパスを追加します。
[フォルダを参照] ウィンドウが表示されます。
7. 必要なフォルダをブラウジングします。フォルダ内のサブフォルダをスキヤンの対象から除外したい場合は、[サブフォルダを除外] を選択します。[サブフォルダを除外] オプションは初期設定で選択されていません。

8. 必要なパスを選択したら、[OK] をクリックします。追加したパスが正しくない場合は、そのパスを選択してから [クリア] をクリックしてパスを削除します。[すべてクリア] をクリックするとすべての追加されたパスがリストから削除されます。
9. [検索を開始] をクリックします。
10. 元ファイルの場所と重複ファイルの場所のリストが表示されます。スキャンの情報は以下のフィールドに表示されます。
 - **検索の進行状況:** 検索の進行状況を表示します。
 - **スキャンされたフォルダ:** スキャンされたフォルダの数が表示されます。
 - **スキャンされたファイル:** スキャンされたファイルの数が表示されます。
 - **検出された重複:** 重複が発見されたファイルの数が表示されます。
 - **無駄になっていたスペース:** 重複ファイルによって占められていたスペースを表示します。
11. [すべてをチェック] をクリックして、拡張された元ファイルに含まれるすべての重複ファイルを選択します。
12. [削除] をクリックして、すべての重複ファイルを削除します。
13. [閉じる] をクリックして、ツールメニューを終了します。

安全な削除

安全な削除は、不要なファイルやフォルダを完全に削除するために使用されます。秘密情報を削除する場合、安全な削除を用いてデータを削除することにより、いかなる手段を用いても復元するのが不可能となります。Windows の削除機能を用いて削除されたデータは、データへのリンクがハードドライブのクラスター内に残存するため、復元ソフトウェアを用いることにより復元可能です。Quick Heal PCTuner の安全な削除機能は、ハードドライブから直接ファイルやフォルダを削除するため、復元ソフトウェアを使用しても復元することができません。

削除方法

Quick Heal PCTuner で利用できる 3 つのファイル削除方法を以下に示します。

ワンパス - 迅速なデータ破壊	ワンパス削除方式は、ランダムな文字を使用してデータを上書きします。この削除方式は、迅速で安全です。削除されたデータを回復することはできません。大半のユーザーにとっては、これが最適なオプションです。ワンパス削除方式は初期設定で選択されています。
ツーパス - より安全な駆除	ツーパス削除方式は、2 倍のランダムな文字を使用してデータを上書きします。この削除方式では、さらにセキュリティが向上します。削除されたデータは、ど

DoD - 標準データ破壊	<p>のような復元ソフトウェアでも復元できません。</p> <p>DoD 削除方式は国防省覚書に従って、ランダムな文字を使用した暗号化方式によってデータを上書きします。削除されたデータは、どのような復元ソフトウェアでも復元できません。</p>
---------------	---------------------------------------------------------------------------------------------------------------------------

安全な削除の使用

安全な削除を使用してファイルやフォルダを削除するには、以下の手順に従ってください。

1. [ツール] > [安全な削除] の順に選択します。
2. [オプション] ボタンをクリックします。
[安全な削除方法の選択] ウィンドウが表示されます。
3. 削除方法を選択して [承諾] ボタンをクリックします。[安全な右クリック削除を有効にする (コンテキストメニュー)] を選択すると、[安全な削除] を右クリックするだけでデータを削除できます。
4. [ファイルの追加] ボタンをクリックして、削除するファイルを指定します。
5. [フォルダを追加] ボタンをクリックして、削除するフォルダとサブフォルダを指定します。
6. 削除するファイルの選択が正しくない場合は、ファイルを選択して [クリア] をクリックします。[すべてクリア] をクリックして、すべての選択を取り消します。
7. [続ける] をクリックします。
8. ウィンドウが表示され、削除すると復元できなくなりますというメッセージが表示されます。このウィンドウを使って、削除方法を変更することもできます。この段階で削除方法を変更する場合は、[オプション] をクリックします。[はい] をクリックして削除を続行します。
選択したファイルは削除され、削除の概要画面が表示されます。
9. [レポートの表示] ボタンをクリックして削除プロセスのレポートを表示するか、または [閉じる] をクリックしてツールメニューを終了します。

スタートアップブースター

不要なスタートアッププログラムをシステムから削除するツールです。レジストリランやスタートアップからすべての不要なアプリケーションを削除し、システムのスタートアップ速度を向上させます。

スタートアップブースターの使用

スタートアップブースターを使用するには、以下の手順に従ってください。

1. [ツール] > [スタートアップブースター] の順に選択します。
2. [検索を開始] をクリックします。

スタートアップ中に自動的にローディングを行うアプリケーションがリストに表示されます。各アプリケーションの先頭にチェックボックスが表示されます。初期設定で選択されているアプリケーションはありません。
3. システム起動時に毎回読み込まれることのないよう、削除する必要のあるアプリケーションを選択します。
4. [削除] をクリックしてリストからアプリケーションを削除するか、または [閉じる] をクリックして終了します。

サービスオプティマイザ

お客様がお使いのコンピュータには、起動時に実行されて CPU やメモリを使用する不要なサービスが数多く存在し、システムパフォーマンスの低下につながっている可能性があります。サービスオプティマイザは、お客様がお使いのシステムを分析し、関連するサービスに対するお客様の回答に基づいて、起動時に実行されないよう安全に無効化できるサービスを提示します。

Quick Heal PCTuner のサービスオプティマイザで利用できるサービスを以下に示します。

- ネットワーク関連サービス
- システム関連サービス
- パフォーマンス関連サービス
- セキュリティ関連サービス

サービスオプティマイザの使用

サービスオプティマイザを使用するには、以下の手順に従ってください。

1. [ツール] > [サービスオプティマイザ] の順に選択します。

サービスは、カテゴリ別に以下の 4 つのタブが示す 4 つのセクションに分類されます:[ネットワーク]、[システム]、[パフォーマンス]、[セキュリティ]
2. サービスを選択してから、各セクションの質問に関連する回答を選択してください。

サービスオプティマイザを開くときはいつも、[適用] ボタンが選択できない状態になっています。しかし、回答を変更する（例えば、[はい] または [いいえ] のいずれかを選択する）と、[適用] ボタンが有効になります。
3. [適用] をクリックしてサービスを最適化するか、または、[閉じる] をクリックして保存せずに終了します。

4. いずれかのサービスを最適化すると、[サービス最適化の概要]が表示されます。
[レポートを表示]をクリックして詳細なレポートを表示するか、または[閉じる]
をクリックして終了します。



- サービスに関連する回答が変更を必要としない場合は、メッセージが表示されます。
- [初期設定] ボタンをクリックすると、すべての最適化されたサービスが元の状態に戻ります。

レポート

レポートメニューには、Quick Heal PCTuner が実行する様々な活動のレポートが含まれます。このメニューには、いくつかのメニュー項目があります。各メニュー項目は特定の活動のレポートに対応しています

レポートメニューのメニュー項目は以下の通りです。

各メニュー項目には、それぞれ 4 つのボタンがあります。以下に示す各メニュー項目での処置は、すべてのメニュー項目に共通です：

ボタン	処置
詳細	リスト内で選択したレコードについての詳細なレポートを表示します。
すべて削除	リスト内のレコードをすべて削除します。
削除	リスト内で選択したレコードを削除します。
閉じる	レポートメニューを終了します。

メニュー項目の [詳細] ボタンをクリックすると [レポート] ウィンドウが開きます。この画面には、さらに 5 つのボタンが表示されます。それらのボタンに関連付けられている処置は、すべてのメニュー項目に共通です。

ボタン	処置
前へ	リストで前にあるレコードの詳細レポートを表示します。
次へ	リストで次にあるレコードの詳細レポートを表示します。
印刷	詳細レポートを印刷します。

名前を付けて保存	詳細レポートがテキスト形式でシステム内に保存され
----------	--------------------------

閉じる	ます。 [レポート] ウィンドウを閉じます。
-----	---------------------------

自動チューンアップレポート

このシステムで実行された**自動チューンアップ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。自動チューンアップレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [自動チューンアップ] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

ディスクのクリーンアップレポート

このシステムで実行された**ディスクのクリーンアップ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。ディスクのクリーンアップレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [ディスクのクリーンアップ] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

レジストリのクリーンアップレポート

このシステムで実行された**レジストリのクリーンアップ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。レジストリのクリーンアップレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [レジストリのクリーンアップ] の順に選択してください。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

履歴のクリーンアップレポート

このシステムで実行された**履歴のクリーンアップ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。履歴のクリーンアップレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [履歴のクリーンアップ] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

スケジューラレポート

このシステムで実行された**スケジュールされたタスク**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。スケジューラレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [スケジューラ] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

安全な削除レポート

このシステムで実行された**安全な削除**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。安全な削除レポートを表示するには、以下の手順に従ってください。

1. [レポート] > [安全な削除] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。

[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

重複ファイルファインダレポート

このシステムで実行された**重複ファイルファインダ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。重複ファイルファインダレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [重複ファイルファインダ] の順に選択します。

2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。
[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

スタートアップブースターレポート

このシステムで実行された**スタートアップブースター**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。スタートアップブースターレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [スタートアップブースター] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。
[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

サービスオプティマイザレポート

このシステムで実行された**サービスオプティマイザ**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。サービスオプティマイザレポートを表示するには、以下の手順に従ってください。

1. [レポート] > [サービスオプティマイザ] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。
[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

復元レポート

このシステムで実行された**復元**の実行結果に関するレコードのリストと、詳細なレポートが表示されます。復元レポートを表示するには、以下の手順に従ってください。

1. [レポート] > [復元] の順に選択します。
2. リストから、必要なレコードを選択します。
3. [詳細] ボタンをクリックします。
[レポート] ウィンドウが開き、選択したレコードに関する詳細レポートが表示されます。

復元

ディスクのクリーンアップ、レジストリのクリーンアップ、スタートアップブースターのいずれかによって削除された項目を元の場所に復元します。ただし、履歴のクリーンアップによって削除された項目は復元されません。



ディスクのクリーンアップ、レジストリのクリーンアップで **[バックアップを作成せずに項目を削除]** が選択されている場合、バックアップは作成されません。自動チューンアップの場合は、バックアップを作成して必要なときにファイルを復元できるように、**[ファイルを削除する前にバックアップを作成]** を選択することをお勧めします。

復元を実行できるチューンアップ活動のリストが、復元ポイントエリアに掲載されます。復元ポイントエリアで実行できる処置は以下の通りです。

レポートの復元

復元を行うには、以下の手順に従ってください。

1. 必要な復元ポイントを選択します。
2. **[復元]** ボタンをクリックします。
3. メッセージボックスに以下のメッセージが表示されます:**バックアップを復元しますか?** バックアップを復元する場合は **[はい]** を、しない場合は **[いいえ]** をクリックしてください。
4. 前のステップで **[はい]** をクリックした場合はバックアップが復元され、**[選択されたバックアップが正常に復元されました]** というメッセージが表示されます。 **[OK]** をクリックして復元プロセスを完了します。

レポートの削除

リスト内の復元ポイントを削除するには、以下の手順に従ってください。

1. 必要な復元ポイントを選択します。
2. **[削除]** ボタンをクリックします。
3. 以下のメッセージが表示されます:**復元ポイントを削除しますか?** 復元ポイントを削除する場合は **[OK]** を、削除せずに終了する場合は **[キャンセル]** をクリックします。

技術サポート

Quick Heal では、登録済みユーザーを対象に広範な技術サポートを提供しています。メールやお電話の際には、Quick Heal のサポート担当者から効率的なサポートを受けられるように、必要な詳細をすべてお手元にご用意いただくことをお勧めします。

プロダクトキーを紛失した場合の対処法

プロダクトキーは Quick Heal AntiVirus におけるお客様の ID の役割を果たしています。プロダクトキーを紛失した場合は、再発行いたしますので Quick Heal 技術サポートまでご連絡ください。プロダクトキーの再発行には、若干の手数料が発生します。

サポート

サポートオプションは、お客様が問題に直面した際の様々な解決策を提示する包括的なオンラインサポートを提供しています。サポートオプションには FAQ（よくある質問）セクションがあり、よくある質問に対する回答を見つけることができます。FAQ で解決策が見つからない場合は、質問を電子メールで送信するか、直接電話で問い合わせることができます。

サポートには以下のオプションがあります。

ウェブサポート

ウェブサポートでは、質問を送信したり、FAQ（よくある質問）を確認したりできます。他のサポート手段をご利用になる前に、一度 FAQ の回答をご確認いただくことをお勧めします。これにより、ご自身で問題を解決できる場合があります。

ウェブサポートを利用するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal メニューバーから、**[ヘルプ]** > **[サポート]** をクリックします。
3. **[サポート]** 画面で **[FAQ を見る]** をクリックしよくある質問を表示するか、**[フォーラムに参加する]** から質問を送信します。

電子メールサポート

電子メールサポートでは、お客様の質問に関して電子メールを送信でき、Quick Heal のサポート担当者が適切な解決策をお客様に提供します。

電子メールサポートを利用するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal メニューバーから、**[ヘルプ]** > **[サポート]** をクリックします。
3. **[サポート]** 画面の **[電子メールサポート]** から **[チケットを送信する]** をクリックし、質問を送信します。

[チケットを送信する] ボタンをクリックすると、質問を送信できる当社のサポートウェブページが開きます。

電話サポート

電話によるサポートでは、Quick Heal 技術担当者から素早くサポートを得るために電話でご連絡いただくことができます。

電話でのサポートを希望される場合は、次の番号にお電話ください：03-5050-1377

リモートサポート

Quick Heal 技術サポートチームは、場合によってリモートサポートも提供しています。このサポートモジュールは、インターネットを通してお客様のコンピュータシステムに簡単に接続し、遠隔操作で技術サポートを行います。これにより、当社の技術担当者がお客様の問題を効果的にサポートすることができます。

リモートサポートを利用するには、以下の手順に従ってください。

1. **Quick Heal AntiVirus** を開きます。
2. Quick Heal ダッシュボードで、**[ヘルプ]** > **[サポート]** をクリックします。
3. **[リモートサポート]** ボタンをクリックします。

[リモートサポートの同意] 画面が開きます。同意内容をよくお読みください。

4. **[同意する]** をクリックします。
5. Quick Heal リモートサポートエージェントで利用できる **ID** を Quick Heal のサポート担当者に提供します。

Quick Heal のサポート担当者は、問題を解決するためにお客様のシステムにリモートアクセスします。

ライブチャットサポート

この機能を利用すると、問題を解決するために Quick Heal 技術担当者とチャットすることができます。

サポート連絡先

Quick Heal では、登録済みユーザーを対象に広範な技術サポートを提供しています。お電話の際には、Quick Heal のサポート担当者から効率的なサポートが受けられるよう、必要な詳細をすべてお手元にご用意いただくことをお勧めします。

電話対応の受付時間

Quick Heal Technologies (P) Ltd. 技術サポートへは、午前 10 時 30 分 - 午後 6 時 30 分 (JST) の間に電話をおかけください。

連絡先電話番号

インド国内の Quick Heal ユーザーは、03-5050-1377 に電話をおかけください。

南インドのお客様は、地域サポート +919043121212 (マラヤナム語、タミル語、テルグ語、カンナダ語) をご利用いただけます。

インド国外でのサポート

オンラインで質問を提出したり、オンラインチャットを利用したりするには、

http://www.quickheal.com/contact_support をご覧ください (24 時間 365 日対応)。

各国での電話番号を調べるには、http://www.quickheal.com/int_techsupp にアクセスします。

お客様の国内の販売店を調べるには、<http://www.quickheal.com/locate-dealer> にアクセスします。

電話サポートに必要なお客様情報

- 製品が入っていた箱に同梱されているプロダクトキー。オンラインで購入された場合は、注文確認電子メールに記載されています。
- お使いのコンピュータシステムに関する情報: 製品機種、プロセッサの種類、メモリ容量、ハードドライブの大きさ、空き領域、その他関連情報 (周辺機器など)。
- オペレーティングシステム: 名称、バージョン番号、言語。
- インストールされたアンチウイルスソフトウェアやウイルスデータベースのバージョン。
- お使いのシステムにインストールされたソフトウェア。
- ネットワーク接続の有無。接続されている場合は、システム管理者にまずご連絡ください。管理者が問題を解決できない場合は、管理者が Quick Heal 技術サポートまでご連絡ください。
- その他の情報: 最初に問題が発生したのはいつですか?問題が発生したとき、どのような操作をしていましたか?

技術サポート担当者にお伝えいただく内容

サポート担当者はいただいた情報をもとに解決策を導き出すため、最大限の情報をできる限り具体的にお伝えいただく必要があります。

Quick Heal Technologies の連絡先情報

本社

Quick Heal Technologies (P) Ltd.

603, Mayfair Towers II,

Wakdewadi, Shivajinagar,

Pune 411005, Maharashtra

電子メール:info@quickheal.com

詳細については、次の URL を参照してください: www.quickheal.co.jp.

インデックス

D

DNA スキャン, 24

ウ

ウイルスの除去, 88
ウイルス対策, 23

ス

スキャン
外部ドライブ, 52
スキャンスケジュール, 27
スキャン設定, 19
スパム対策, 34

デ

データ盗難対策, 53

パ

パスワード保護, 64

フ

フィッシング対策, 41

ブ

ブラウザサンドボックス, 42
ブラウジング保護, 41

ペ

ペアレンタルコントロール, 46

更

更新
オンライン, 11

登

登録
SMS, 9
オンライン, 8
マルチユーザーパック, 10

隔

隔離とバックアップ, 31

電

電子メール保護, 32