カスペルスキー インターネット セキュリティ 2013
カスペルスキー アンチウイルス 2013

KASPERSKY lab

ユーザーガイド

製品バージョン：13.0

カスペルスキー インターネット セキュリティ 2013
カスペルスキー アンチウイルス 2013

ユーザーガイド

まず、はじめよう

1 インストール・アンインストール ▶ 12 ページ

製品の動作環境、インストール方法、はじめて製品を起動したときに必要な確認操作など、製品をお使いいただけるまでの準備について説明します。

2 ライセンス・アクティベーション ▶ 20 ページ

ライセンスの確認や更新、アクティベーションなどについて説明します。

これだけは知っておきたい

3 主な機能と画面構成 ▶ 22 ページ

製品の主な機能、画面構成、各種ウィンドウとツールの概要について説明します。

4 基本的な使い方 ▶ 35 ページ

保護状態の確認、アップデート、スキャン、プロテクションの停止・再開など、基本的な機能の操作方法を説明いたします。

5 脅威への対処 ▶ 50 ページ

ウイルスに感染したり、悪意のある攻撃を受けたりしたときなどの対処方法を説明します。

インターネットを、より安全に

6 インターネットを安全に使用するための機能 ▶ 56 ページ

子供のコンピューター利用制限、個人情報の保護、セキュリティキーボードなど、インターネットをより安全で快適に使用するための機能について説明します。

新機能！「ネット決済保護」を使ってみよう！

※カスペルスキー インターネット セキュリティのみの機能です。

もっと、カスタマイズ

7 プロテクション機能の設定 ▶ 68 ページ

各プロテクション機能の設定方法について説明します。通常は初期設定のままで問題ありませんが、さらにセキュリティを高めたいときなどに変更できます。

8 詳細設定と便利ツール ▶ 93 ページ

コンピューターに詳しいユーザーが管理しやすくしたい場合などに有効な設定方法を説明します。（上級者向け）
また、便利なツールについても説明しています。

9 付録 ▶ 111 ページ

トラブルシューティングや、用語解説を記載しています。

はじめに

Kaspersky Lab の製品をお使いのみなさまへ

このたびは当社製品をお選びいただき、誠にありがとうございます。このガイドがお客様の作業の一助となること、またお客様の疑問にお答えできる内容であることを願っております。

ご注意
この文書は Kaspersky Lab ZAO（以降、「Kaspersky Lab」）の資産です。この文書に対するすべての権利は、ロシア連邦の著作権法および国際条約によって留保されています。この文書またはその一部を不正に複製および配布すると、適用法により民法上、行政上、または刑法上の責任を負うこととなります。

ガイドの複製または配布は、翻訳されたものも含めていかなる形であれ、Kaspersky Lab の書面による同意がないかぎり認められておりません。
このガイドおよびガイドに含まれる画像は、非商用（個人使用）の目的で提供されています。

Kaspersky Lab は、このガイドを予告なく変更する場合があります。最新版については、Kaspersky Lab の Web サイト（http://www.kaspersky.co.jp/docs）をご確認ください。

このガイドに利用されている資料のうち、他社が権利を有するものの内容または品質、妥当性、正確性について、また、そうした資料の使用に関連する潜在的な損害、および実際に発生した損害について、Kaspersky Lab は一切の責任を負いません。

改訂日：2012 年 10 月 11 日
© 2012 Kaspersky Lab ZAO. 無断複写・転載を禁じます。
http://www.kaspersky.co.jp
http://support.kaspersky.co.jp

ソフトウェア使用許諾契約書について

ソフトウェア使用許諾契約書は、ユーザーと Kaspersky Lab との間で締結される拘束力のある契約であり、製品の使用条件を規定しています。製品を使用する前に、使用許諾契約の条件をよくお読みください。
使用許諾契約書の条件は、カスペルスキー製品のインストール時に確認できます。製品をインストールする際に使用許諾契約に同意することにより、使用許諾契約の条件を承諾したと見なされます。本契約書の諸条件に同意されない場合は、本製品のインストールを中止、または使用を中止してください。

ライセンスについて

ライセンスは、ソフトウェア使用許諾契約書に基づいて提供される、製品を使用する期限付きの権利です。ライセンスは、お使いの製品に対して、アクティベーションを実行するための固有のコードが対応づけられています。

ライセンスには、次のサービスを受けられる権利が含まれます。

- 製品を 1 台または複数台のコンピューターで使用する権利
  製品を使用できるデバイスの数は、ライセンスの種類により異なります。
- テクニカルサポートの支援
- ライセンスの有効期間中に Kaspersky Lab またはパートナーから提供されるその他のサービス

サービスの範囲および製品使用条件は、製品のアクティベーションを実行するライセンスの種類によって異なります。
ライセンスの種類は次のとおりです。

- 試用版 – 有効期間に制限がある無料のライセンス
  試用版ライセンスは通常、有効期間が短く設定されています。試用期間が終了すると、製品の機能が使用できなくなります。製品を継続して使用する場合は、製品版ライセンスを購入する必要があります。
- 製品版 – カスペルスキー製品を購入すると提供される、有料ライセンス
  製品版ライセンスの期限が切れても製品をそのまま使用できますが、機能が制限されます（たとえば、アップデートや Kaspersky Security Network の利用はできません）。この状態でも、すべての製品コンポーネントの機能を利用でき、ウイルスなどのマルウェアのスキャンが実行できます。ただし、利用できる定義データベースは、ライセンスの有効期限が切れる前にインストールされたバージョンのみです。カスペルスキー製品のすべての機能を使用するには、製品版ライセンスを更新する必要があります。

セキュリティ上のすべての脅威からコンピューターを確実に保護するために、ライセンスの有効期限が切れる前に更新することをおすすめします。

アクティベーションコードについて

アクティベーションコードは、カスペルスキーの製品版で提供されるコードです。20 桁の半角英数字で、xxxxx-xxxxx-xxxxx-xxxxx の形式で構成されます。製品のアクティベーションに必要となります。

次のいずれかの購入方法で、アクティベーションコードを入手できます。

- パッケージ版を購入した場合は、パッケージの中に同梱されています。
- ダウンロード版を購入した場合は、注文時に指定されたメールアドレスに送付されます。

製品のアクティベーションを実行した日から、ライセンスの有効期間のカウントが開始されます。複数台で使用できるライセンスを入手した場合、最初の 1 台にアクティベーションを実行した日から、ライセンスの有効期間のカウントが開始されます。

アクティベーションを実行し、製品上でライセンスが有効な状態で、アクティベーションコードを紛失した場合は、マイカスペルスキーアカウントからカスペルスキーのテクニカルサポートサービスにお問い合わせください（113 ページの「ユーザー登録とサポートサービスについて」を参照してください）。

データの提供について

プロテクションレベルを向上させるため、ソフトウェア使用許諾契約書の条項に同意することで、次の情報を Kaspersky Lab に自動的に提供することに同意いただくことになります。

- 処理したファイルのチェックサム（MD5）に関する情報
- URL を評価するために必要な情報
- 製品についてのお知らせの利用状況の統計
- スパムに対する保護に関する統計データ
- カスペルスキー製品のアクティベーションおよび現在使用されているバージョンに関する情報
- 検知された脅威のタイプに関する情報
- 現在使用されているデジタル署名に関する情報、およびそれを検証するのに必要な情報

コンピューターに TPM（信頼するプラットフォームモジュール）が搭載されている場合は、オペレーティングシステムの起動に関する TPM のレポートおよびそれを検証するのに必要な情報を、Kaspersky Lab に提供することに同意していただくことになります。製品のインストール中にエラーが発生した場合は、エラーコード、使用中の配布パッケージ、お使いのコンピューターに関する情報を Kaspersky Lab に自動的に提供することに同意していただくことになります。

Kaspersky Security Network（26 ページの「Kaspersky Security Network への参加」を参照）に参加していただくと、次の情報が Kaspersky Lab に自動的に送信されます。

- コンピューターにインストールされているハードウェアおよびソフトウェアに関する情報
- コンピューターのアンチウイルスのプロテクションステータスや、悪意があると疑わしいオブジェクトや動作のすべて、それらのオブジェクトと動作に関して行われた決定に関する情報
- ダウンロードされ実行されているアプリケーションに関する情報
- インターフェイスエラー、カスペルスキー 製品のインターフェイスの使用に関する情報
- 現在使用中のデータベースのバージョンに関する情報
- アップデートおよび Kaspersky Lab のアップデートサーバーとの接続の統計情報

また、Kaspersky Lab でさらに詳しくチェックするには、悪意のある第三者に悪用される恐れのあるファイル（またはファイルの一部）を送信していただくことが必要になる場合があります。
取得した情報は、既存の法律で定められた要件に基づき、Kaspersky Lab で保護されます。Kaspersky Lab は、取得した情報を、一般的な統計の目的でのみ使用します。一般的な統計情報は、取得した情報をもとに自動生成されます。個人情報や機密情報が含まれることはありません。取得した情報は暗号化された形式で保管され、蓄積された後に消去されます（年に 2 回）。一般的な統計情報は、無期限に保管されます。

情報の入手方法

● **ヘルプを参照する**
Windowsのスタートメニューから、[すべてのプログラム－カスペルスキー インターネット セキュリティ 2013 －カスペルスキー インターネット セキュリティ 2013 ヘルプ］を選択して表示します。また、各ウィンドウの［ヘルプ］をクリックすると、現在表示されている項目と関連する内容のヘルプを直接表示することができます。ヘルプでは、設定や応用操作など、より詳しい説明を参照することができます。

● **サポート情報を参照する**
メインウィンドウの［サポート］をクリックすると、［サポート］ウィンドウが表示されます。お使いの製品のバージョン、定義データベースのリリース日時、オペレーティングシステム、ライセンスの番号などのシステム情報を確認できます。（これらの情報は、サポートセンターにお問い合わせの際、必要になる場合があります。）
また、テクニカルサポートサイトのページを表示することができます。

● **ユーザーガイド（本書）を参照する**
店頭で製品をお買い上げの場合、CD-ROMにユーザーガイドのPDFが含まれています。また、カスペルスキーのWebサイトのダウンロードページから、ユーザーガイドのPDFをダウンロードすることもできます。

本書での表記

● 本書では、カスペルスキー インターネット セキュリティ 2013とカスペルスキー アンチウイルス 2013をまとめて、「カスペルスキー」と表記します。
● 本書では、Windows 7を使用した場合の操作手順を説明しています。また、Windows 7で表示される画面を使用しています。お使いのOSや環境によっては、実際の操作方法や画面とは異なる場合があります。
● 本書の操作説明では、以下の表記を使用しています。
画面に表示されるウィンドウ名、タブやセクション名、項目名、ウィンドウ内のボタン名、メニューやコマンド名は［　］で囲んで表記します。
例：[設定] ウィンドウで [プロテクション] の [ファイルアンチウイルス] を選択し、[セキュリティレベル] で [設定] をクリックすると、[ファイルアンチウイルス] ウィンドウが表示されます。
階層になっているコマンドメニューは「－」で続けて記載します。
例：[すべてのプログラム－カスペルスキー インターネット セキュリティ 2013 －製品ページ]
関連する機能や詳しい説明が他の箇所で説明されている場合は、「▶」に続けて参照先のページ番号とタイトルを記載しています。
例：▶ P.8 インストール
● 画面は開発中のものです。ご利用中の製品に表示される画面と、画面デザインおよび画面に表示されている文言が若干異なる場合があります。

カスペルスキー アンチウイルスをお使いの方へ

- 本書では、カスペルスキー インターネット セキュリティ 2013 の画面を使用しています。カスペルスキー アンチウイルス 2013 の実際の画面と異なることがあります。
- 「カスペルスキー インターネット セキュリティ」と表記されている箇所は、「カスペルスキー アンチウイルス」と読み替える必要がある場合があります。
- カスペルスキー インターネット セキュリティ 2013の機能の中には、カスペルスキー アンチウイルス 2013 で使用できないものがあります。それらの機能の説明には、注意書きがあります。

  例：※保護者による管理は、カスペルスキー インターネット セキュリティのみの機能です。

目次

はじめに 2
Kaspersky Lab の製品をお使いのみなさまへ 2
ソフトウェア使用許諾契約書について 3
ライセンスについて 3
アクティベーションコードについて 4
データの提供について 5
情報の入手方法 6
本書での表記 6

1 インストール・アンインストール

システム要件 12
インストール 14
インストールする前に 14
インストールする 15
アクティベーションを実行する 17
はじめて起動したときに行うこと 18
アンインストール 19
アンインストールする 19

2 ライセンス・アクティベーション

ライセンス 20
ライセンスを確認する 20
ライセンスを購入する 20
アクティベーション 21
アクティベーションを実行する（ライセンスを更新する） 21

3 主な機能と画面構成

主な機能 22
コンピューターの保護 22
インターネットの保護 24
コンピューターのスキャン 25
定義データベースとプログラムのアップデート 25
検知履歴の確認と処理の実行 26
Kaspersky Security Network への参加 26
各種ツール 27
画面構成 28
メインウィンドウ 28
各種ウィンドウ 31
設定ウィンドウ 31
レポートウィンドウ 31

タスクバーのアイコン 32
アイコンの表示 32
アイコンの操作 33
ガジェット 34

4 基本的な使い方

保護状態の確認 35
保護状態を確認する 35
保護状態の詳細を確認する 35
定義データベースとプログラムのアップデート 36
定義データベースの状態を確認する 36
アップデートを実行する 36
アップデートの実行方法を設定する 38
スキャンの実行・設定 39
スキャンの種類 39
スキャンを実行する 40
スキャンの自動実行を設定する 42
スキャンの対象を設定する 43
セキュリティレベルを設定する 44
脅威の検知時の処理方法を設定する 45
リムーバブルドライブ検出時の動作を設定する 46
スキャン実行用のショートカットアイコンを作成する 46
プロテクション機能の停止・再開 47
プロテクション機能を一時的に停止する・再開する 47
プロテクション機能を完全に停止する 48
カスペルスキーを終了する・起動する 49

5 脅威への対処

通知ウィンドウが表示されたら 50
通知ウィンドウの種類 50
選択できる処理 51
通知方法を変更する 52
処理結果の確認 53
レポートを表示して確認する 53
検知された脅威を処理する 54
レポートを保存する 54
隔離されたオブジェクトを操作する 55

6 インターネットを安全に使用するための機能

保護者によるコンピューター利用の制限 56
保護者による管理を有効にする 56
制限する内容を設定する 57
使用状況を確認する 58

インターネット上の決済処理で使用する情報の保護 59
ネット決済保護機能を利用する 59
ネット決済保護機能を設定する 60
入力情報の漏えいを防止 62
キーボード入力の保護を設定する 62
セキュリティキーボードを起動する 63
セキュリティキーボードを利用する 65
危険なサイトへのリンクを診断 66
危険サイト診断を設定する 66

7 プロテクション機能の設定

全般的なプロテクション設定 68
プロテクションの有効・無効を切り替える 68
脅威の処理方法を変更する 69
パスワードを設定して操作を制限する 69
検知時の処理方法を設定する 70
ファイルアンチウイルス（ファイルからの感染を検知） 72
セキュリティレベルを設定する 72
メールアンチウイルス（メールからの感染を検知） 74
セキュリティレベルを設定する 74
ウェブアンチウイルス（Web ページからの感染を検知） 76
セキュリティレベルを設定する 76
メッセンジャーアンチウイルス
（インスタントメッセージングからの感染を検知） 78
スキャン方法を設定する 78
アプリケーションコントロール（アプリケーションの動作を監視） 79
アプリケーションに設定されたステータスを確認・変更する 79
保護するデータを確認・変更する（プライバシープロテクション） 82
システムウォッチャー（システムプロセスを監視） 83
検知時の処理方法を設定する 83
不正な動作を元に戻す設定をする 84
ぜい弱性への攻撃をブロックする 85
ファイアウォール（ネットワークからのアクセスを監視） 86
ネットワークに設定されたステータスを確認・変更する 86
ネットワークルールを変更する 87
ネットワーク攻撃防御（ネットワークからの攻撃をブロック） 88
攻撃元からの接続をブロックする時間を設定する 88
アンチスパム（迷惑メールを識別） 89
セキュリティレベルを設定する 89
アンチバナー（バナー広告を非表示） 91
スキャン方法を設定する 91
ブロックまたは許可するサイトを登録する 92

8 詳細設定と便利ツール

検知する対象の設定.....93
検知する脅威を設定する.....93
信頼する対象の設定.....94
信頼するオブジェクトを追加する.....94
信頼するアプリケーションを追加する.....95
ネットワークに関する機能の設定.....97
監視するネットワークポートを設定する.....97
暗号化された接続のスキャンを有効にする.....98
プロキシサーバーを設定する.....99
ネットワークの接続状況を確認する（ネットワークモニター）.....100
パフォーマンスに関する機能の設定.....101
特別な駆除機能を有効にする.....101
スキャンやアップデートを自動的に延期する.....101
全画面使用時に設定を自動的に切り替える（ゲームモード）.....102
設定のエクスポート・インポートと初期化.....103
設定をエクスポートする.....103
設定をインポートする.....103
設定を初期化する.....104
便利ツールの活用.....105
起動できなくなったシステムの感染を検知・駆除する（レスキューディスク）.....105
Windows の設定を検査する（Windows 設定診断）.....107
ユーザーの操作履歴を消去する（プライバシークリーナー）.....108
Internet Explorer の設定を検査する（Internet Explorer 設定診断）.....109
変更・削除した内容を元に戻す.....110

9 付録

トラブルシューティング.....111
用語解説.....112
ユーザー登録とサポートサービスについて.....113
ユーザー登録.....113
サポートサービスをご利用になる前に.....113
マイカスペルスキーアカウントによるテクニカルサポート.....114
ライセンスに関するお問い合わせ.....115
ご購入後の技術的なお問い合わせ.....115
KASPERSKY LAB ZAO.....116
索引.....118

システム要件

カスペルスキー インターネット セキュリティ 2013 ／カスペルスキー アンチウイルス 2013（以下、まとめてカスペルスキー）の動作に必要な環境は次のとおりです。
インストール前にご確認ください。

OS *1	Windows 8（日本語版） Windows 7（日本語版） Windows Vista（日本語版） Windows XP（Service Pack 2 以上）（日本語版） ※それぞれ、32 ビット版・64 ビット版に対応しています。
CPU	Intel Pentium 1 GHz 32 ビット（x86）／ 64 ビット（x64）以上のプロセッサ（または同等の互換プロセッサ）
メモリ	Windows 8：64 ビット版は 2 GB 以上、32 ビット版は 1 GB 以上 Windows 7：64 ビット版は 2 GB 以上、32 ビット版は 1 GB 以上 Windows Vista：64 ビット版は 2 GB 以上、32 ビット版は 1 GB 以上 Windows XP：512 MB 以上 ※必要メモリ容量を搭載していても、常駐プログラムやサービスの数によっては、メモリ不足のエラーが発生します。こうした場合は、常駐プログラムやサービスを停止し空きメモリを確保してください。安定した動作をさせるにはメモリの増設をおすすめします。
ハードディスク必要容量	480 MB 以上（システムドライブ上の 380 MB を含む） ※お使いのハードディスクのフォーマット形式や確保容量などにより、必要容量は異なります。 ※定義データベースのサイズやレポートの作成状況により、必要容量は変動します。 ※レポートや隔離で使用する容量は、プログラムの設定で変更できます。
ディスプレイ	1024 × 576 以上、High Color 以上
サウンド	PCM 音源が再生できる環境を推奨
その他	• CD-ROM 対応のドライブ（CD-ROM からインストールする場合） • インターネット接続環境（製品のアクティベーション、定義データベースおよびソフトウェアモジュールのアップデートに使用） • Microsoft Internet Explorer 8.0 以上 • Microsoft Windows インストーラー 3.0

*1 Windows 7 の対応エディションは、Starter / Home Premium / Professional / Ultimate です。
Windows Vistaの対応エディションは、Home Basic / Home Premium / Business / Ultimate / Enterpriseです。
Windows XPの対応エディションは、Home Edition / Professional / Professional x64 Editionです。

ネットブックのハードウェア要件

- ○ CPU：Intel Atom 1.6 GHz 以上、または同等の互換プロセッサ
- ○ ビデオカード：Intel GMA950 ビデオメモリ 64 MB 以上、または同等の互換ビデオカード
- ○ ディスプレイ：10.1 インチ以上、1024 × 576 以上の画面解像度

注意事項

- ● 本製品のご使用前にソフトウェア使用許諾契約書にご同意いただく必要があります。
- ● 最新の動作環境につきましては、下記のサイトをご覧ください。
  - ○ カスペルスキー インターネット セキュリティ
    http://www.kaspersky.co.jp/internet-security
  - ○ カスペルスキー アンチウイルス
    http://www.kaspersky.co.jp/anti-virus

プラグイン

● **メールアンチウイルス**
次のメールソフトがインストールされている場合、専用プラグインがアドオンされます。
○ Microsoft Outlook 2010 / 2007 / 2003

● **アンチスパム**
次のメールソフトがインストールされている場合、専用プラグインがアドオンされます。
○ Microsoft Outlook 2010 / 2007 / 2003
○ Microsoft Outlook Express 6
○ Windows メール
○ Thunderbird 3.0 以上
※アンチスパムは、カスペルスキー インターネット セキュリティのみの機能です。

● **危険サイト診断（ウェブアンチウイルス）**
次のブラウザーがインストールされている場合、各ブラウザー用のアドオンとしてプラグインが追加されます。
○ Microsoft Internet Explorer 8、9、10
○ Mozilla Firefox 9.x ～ 12.x
○ Google Chrome 15.x ～ 17.x

メール・Web の保護対象範囲

● **メール送受信の保護**
SMTP、POP3、IMAP、NNTP のプロトコルを使用するメール送受信をスキャンします。
※暗号化されたメールには対応しておりません

● **Web ブラウジングの保護**
HTTP トラフィックを監視し、Web ブラウザーで脅威を検知します。
SSL/TLS プロトコルで暗号化された接続をスキャンするには、証明書をインストールします。
※証明書をインストールしても、一部の Web サイトは閲覧できない可能性があります。
※お使いのブラウザーによっては、手動で証明書をインストールする必要があります。

Windows 8 使用時の制限事項

● Windows 8 スタイルでの Microsoft Internet Explorer 10 の使用時、および Microsoft Internet Explorer 10 の拡張保護モードを有効にした状態での使用時には、次の機能は使用できません。
○ セキュリティキーボード
○ 入力情報の漏えい防止
○ ネット決済保護
○ 危険サイト診断

インストール

インストールする前に

インストールする前に、以下の点を確認してください。

□ **管理者アカウントのユーザー情報を準備する**
Windows 7 / Vista の場合は、カスペルスキーを使用するユーザーでログオンします。ログオンしたユーザーが管理者アカウントではない場合、インストールの途中で管理者アカウントのユーザー名とパスワードを入力する必要があります。
Windows XP の場合は、Administrators グループに所属しているユーザーや「コンピュータの管理者」のユーザーでログオンします。

□ **他のセキュリティ対策ソフトをアンインストールする**
すでに他のセキュリティ対策ソフトがインストールされている場合は、インストールを開始する前にアンインストールしてください。アンインストールの方法は、インストールされているセキュリティ対策ソフトのマニュアルをご覧ください。

□ **起動しているアプリケーションをすべて終了する**

□ **アクティベーションコードを用意する**
インストールの直後に、ライセンスを認証するためのアクティベーションを実行します。このとき、有効なアクティベーションコードを入力する必要があります。

アクティベーションコード

パッケージに同梱されているか、ダウンロード版購入時のメールに記載されている 20 桁の英数字です。xxxxx-xxxxx-xxxxx-xxxxx の形式で記載されています。

□ **インターネットに接続可能な状態にする**
アクティベーションやインストール後のアップデートなどには、インターネットへの接続が必要です。

□ **マイカスペルスキーアカウント登録用のメールアドレスを用意する**
アクティベーションの途中で、マイカスペルスキーアカウントに登録します。その際に、マイカスペルスキーアカウント用のメールアドレスが必要になります。

マイカスペルスキーアカウント

マイカスペルスキーアカウントは、テクニカルサポートサイトにある各ユーザー固有のエリアです。詳しくは、113 ページの「ユーザー登録とサポートサービスについて」を参照ください。

お知らせ　ライセンスの種類と複数のコンピューターへのインストール

ライセンスの種類によっては、カスペルスキーを複数のコンピューターにインストールして使用できます。

メインウィンドウの［ライセンス］をクリックすると、現在のライセンス情報が確認できます。

インストールする

インストールを実行します。インストールは、画面の指示に従って進めます。

1. **コンピューターに本製品の CD-ROM をセットします。**

本製品をダウンロードで入手した場合

手順 1 の代わりに、ダウンロードしたファイルを実行します。ファイルが解凍され、インストール開始画面が表示されます。手順 4 へ進みます。

2. **［autorun.exe の実行］をクリックします。**
3. **［ここをクリックしてインストール］をクリックします。**
4. **［ソフトウェア使用許諾契約書］をクリックして、ソフトウェア使用許諾説明書の内容を確認します。**
5. **Kaspersky Security Network（KSN）に参加する場合は、［Kaspersky Security Network（KSN）に参加して、コンピューターの保護を最適化します］をオンにします。**

Kaspersky Security Network（KSN）について

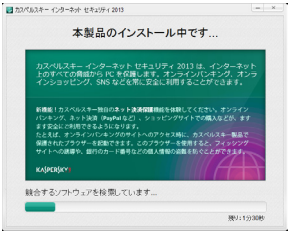
KSN は、新しい脅威へいち早く対応できるようにする、クラウドを利用したオンラインサービスです。［KSN 声明］をクリックすると、KSN についての説明が表示されます。詳しくは、26 ページの「Kaspersky Security Network への参加」を参照してください。
なお、KSN はいかなる個人情報も収集・転送することはありません。

6. **［インストール］をクリックします。**

インストールが実行されます。

［ユーザーアカウント制御］画面が表示される場合があります

お使いの環境によっては、インストールの実行中に［ユーザーアカウント制御］画面が表示される場合があります。その場合、［はい］または［許可］をクリックしてください。



コンピューターの再起動を求める画面が表示される場合があります

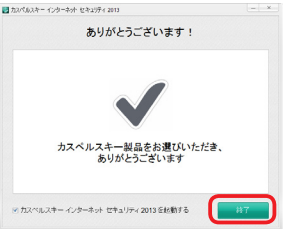
お使いの環境によっては、インストールの実行中にコンピューターの再起動を求める画面が表示される場合があります。その場合、［終了］をクリックしコンピューターを再起動してからインストールを続行してください。

ご注意　共存できないソフトウェアがインストールされている場合

共存できない他のセキュリティ対策ソフトがインストールされている場合、その製品名が表示されます。インストールを続けるには共存できないソフトをアンインストールする必要があります。

7. インストールが終了し、［ありがとうございます！］画面が表示されたら、［カスペルスキー インターネット セキュリティ 2013 を起動する］をオンにして、［終了］をクリックします。

カスペルスキーが起動します。最初の起動は、しばらく時間がかかります。
起動すると、［アクティベーション方法の選択］画面が表示されます。
次ページの「アクティベーションを実行する」へ進みます。

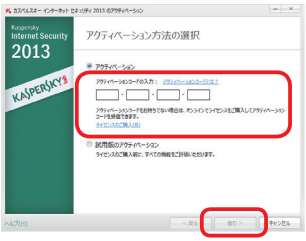


アクティベーションを実行する

インストールが終了したら、ライセンスのアクティベーション（有効化）を実行します。アクティベーション後は、カスペルスキーのすべての機能が使用可能になります。
インストールの終了後、［アクティベーション方法の選択］画面が表示されたら、次の手順を実行します。

有効期限が切れていないライセンスが保存されている場合（アンインストール時にライセンスデータの保存を選択した場合など）、［アクティベーション方法の選択］画面は表示されず、自動的にアクティベーションが実行されます。カスペルスキーのメインウィンドウが起動したら、アクティベーションが完了した状態になっています。あらためてアクティベーションを実行する必要はありません。

1. 有効なアクティベーションコードを［アクティベーションコードの入力］に入力します。



アクティベーションコード

パッケージに同梱されているか、ダウンロード版購入時のメールに記載されている 20 桁の英数字です。xxxxx-xxxxx-xxxxx-xxxxx の形式で記載されています。

2. ［進む］をクリックします。

アクティベーションコードの確認が実行されます。

アクティベーションコードが確認されると、マイカスペルスキーアカウントへの登録画面が表示されます。

3. マイカスペルスキーアカウントにまだご登録されていない場合は、有効なメールアドレスを使用して、登録の手続きをしてから、［進む］をクリックします。

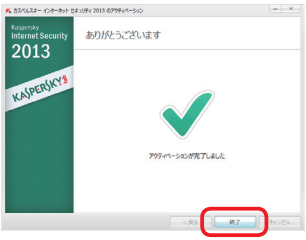
※表示されない場合もあります。

マイカスペルスキーアカウント

マイカスペルスキーアカウントは、テクニカルサポートサイトにある各ユーザー固有のエリアです。詳しくは、113 ページの「ユーザー登録とサポートサービスについて」を参照ください。

4. 正常にアクティベーションが完了すると［ありがとうございます］画面が表示されるので、［終了］をクリックします。

カスペルスキーのメインウィンドウが表示されます。



はじめて起動したときに行うこと

インストール後、カスペルスキーはそのままお使いになれます。正常に起動したら、コンピューターとネットワークをより適切に保護するために、できるだけ早く以下の作業を行うことをおすすめします。

● **ライセンスの状態を確認する**

ライセンスが正常に適用されているか、［ライセンス］画面を確認してください。

▶ P.20 ライセンスを確認する

インストール後にアクティベーションを実行しなかったなどで、ライセンスが適用されていない場合は、アクティベーションを実行してください。

▶ P.21 アクティベーション

● **現在の保護状態を確認する**

問題なくコンピューターが保護されているか、メインウィンドウの表示から確認してください。

▶ P.35 保護状態の確認

● **定義データベースとプログラムをアップデートする**

ウイルスや不正アクセスなどの脅威からコンピューターを保護するためには、定義データベースとプログラムを常に最新の状態に保つことが必要です。
定義データベースとプログラムは、自動アップデートするよう設定されています。コンピューターのスキャン前に、アップデートが実行済みであることを確認してください。

▶ P.36 定義データベースとプログラムのアップデート

● **コンピューターの完全スキャンを行う**

カスペルスキーをインストールする前に、すでにコンピューターがウイルスや不正アクセスの脅威にさらされている可能性もあります。確実にコンピューターを保護するために、定義データベースとプログラムのアップデート後、すぐにコンピューターの完全スキャンを実行してください。

▶ P.39 スキャンの実行・設定

はじめて完全スキャンを実行すると、終了までに時間がかかる場合があります。スキャンの設定を変更することで、スキャン時間を短縮できます。

▶ P.44 セキュリティレベルを設定する

アンインストール

カスペルスキーを使用しなくなった場合には、プログラムをアンインストールできます。

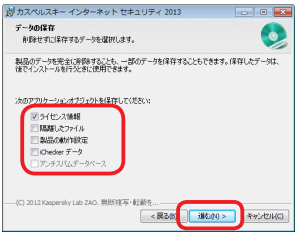
アンインストールする

1. タスクバーの通知領域にあるカスペルスキーのアイコン を右クリックして、［終了］を選択します。

2. Windows の［スタート］ボタンをクリックし、［すべてのプログラム－カスペルスキー インターネット セキュリティ 2013 －カスペルスキー インターネット セキュリティ 2013 の削除］を選択します。

3. インストールウィザードが起動したら、［進む］をクリックします。

4. 削除せずに保存するデータを選択します。
あとで再インストールする可能性があるときなどのために、必要なデータをコンピューター内に残しておくことができます。
すべてのデータを削除する場合は、すべてのチェックボックスをオフにします。



5. ［進む］をクリックします。

6. ［削除］をクリックします。

［ユーザーアカウント制御］画面が表示される場合があります

お使いの環境によっては、アンインストールの実行中に［ユーザーアカウント制御］画面が表示される場合があります。その場合、［はい］または［許可］をクリックしてください。

7. アンインストールが完了し、再起動を促すメッセージが表示されたら、［はい］をクリックします。

ライセンス

ライセンスは、カスペルスキーの全機能を利用するために必要な使用権です。ライセンスには有効期間があり、更新することで有効期間を延長できます。ライセンスの状態や有効期限は、画面上でいつでも確認できます。ライセンスの情報は、サポートセンターへお問い合わせの際に必要になる場合があります。

ライセンスを確認する

ライセンスの有効期間中は、メインウィンドウに有効な残日数が表示されます。
また、［ライセンス］画面では、詳しいライセンス情報が確認できます。

1. **メインウィンドウ右下の［ライセンス］をクリックします。**

   ［ライセンス］画面が表示されます。
   ライセンスの状態、種類、アクティベーション日、有効期限、残り日数などが確認できます。

   ▶ P.20 ライセンスを購入する
   ▶ P.21 アクティベーション

> ライセンスの期限が切れた場合や、インストール時にアクティベーションを行わなかった場合は、メインウィンドウ右下には［ライセンス］ではなく、［アクティベーションコードの入力］と表示されます。

ライセンスを購入する

ライセンスの有効期限が切れると、カスペルスキーのアップデート機能が使用できなくなります。そのため、最新のウイルスに対応できなくなり、感染の危険性が高くなります。有効期限が間近になったら、期限が切れる前にライセンスを購入しておくことをおすすめします。新しいライセンスは、［ライセンス］画面から購入できます。

1. **メインウィンドウ右下の［ライセンス］をクリックします。**

   ※ライセンスの有効期限が切れている場合や、アクティベーションを一度も実行していない場合は、メインウィンドウ右下に［アクティベーションコードの入力］と表示されます。

2. **［ライセンスのご購入］をクリックします。**

   ブラウザーが起動し、ライセンスの購入ページが表示されます。

3. **ライセンスの購入ページに表示される手順に従ってライセンスを購入し、新しいアクティベーションコードを入手します。**

   ※アクティベーションコードは 20 桁の英数字です。

ライセンスの購入後は、アクティベーションを実行します。

▶ P.21 アクティベーション

アクティベーション

アクティベーションとは、ライセンスを有効化することです。アクティベーションコードを入力して、アクティベーションを実行することでライセンスが有効になります。インストール後にアクティベーションを実行しなかった場合や追加でライセンスを購入した場合は、アクティベーションを実行します。
アクティベーションは、インターネットに接続可能な環境で実行してください。

アクティベーションを実行する（ライセンスを更新する）

ご注意　現在のライセンスの有効期限が 2 週間以内であることを確認してください。

有効な製品版のライセンスが 2 週間以上期限が残っている場合、新しいライセンスでアクティベーションを実行すると、ライセンスが上書きされ、現在残っている有効期間がなくなります。
有効期限が 2 週間以内の場合、現在の残りの有効期間に、新しいライセンスの有効期間が足されます。たとえば、1 週間残っているときに 1 年間のライセンスで新たにアクティベーションを行うと、その日から 1 年と 1 週間有効になります。

1. メインウィンドウ右下の［ライセンス］をクリックします。

※ライセンスの有効期限が切れている場合や、アクティベーションを一度も実行していない場合は、メインウィンドウ右下に［アクティベーションコードの入力］と表示されます。

2. ［アクティベーションコードの入力］をクリックします。

3. ［アクティベーションコードの入力］画面が表示されたら、入力欄にアクティベーションコードを入力し、［進む］をクリックします。

アクティベーションコード

20 桁の英数字です。パッケージに同梱されているか、ダウンロード版購入時のメールに記載されています。有効期限が切れた場合は、ライセンスを購入すると、新しいアクティベーションコードが入手できます。
▶ P.20 ライセンスを購入する

4. 正常にアクティベーションが完了すると［ありがとうございます］画面が表示されるので、［終了］をクリックします。

［ライセンス］画面に戻ります。
ライセンスの種類や有効期限を確認できます。

主な機能

カスペルスキーは、多彩な手法を使い、コンピューターのデータを保護します。ウイルスの検知・駆除、ネットワーク経由の不正アクセス防止だけでなく、スパム（迷惑メール）やフィッシング、悪意のあるソフトウェアなど、インターネットの新たな脅威にも対応しています。

ここでは、カスペルスキーの主な機能について説明します。

コンピューターの保護

カスペルスキーのプロテクション（保護）機能はウイルスなどの脅威を常時監視し、検知した場合はすぐに対応してコンピューターを保護します。
インストール直後から、プロテクション機能は開始されています。保護の方法や精度を変更することもできます。各設定の変更は、［設定］ウィンドウから行います。
▶ P.31 設定ウィンドウ

カスペルスキーのプロテクション機能には、次の種類があります。

ウイルス対策

● **ファイルアンチウイルス**　▶ 72 ページ
ファイルに含まれるウイルスを常時監視します。USB メモリなどのリムーバブルドライブにも対応します。ウイルスを検知したら、駆除または削除します。

● **メールアンチウイルス**　▶ 74 ページ
送受信するメールのデータに、ウイルスが含まれていないかスキャンします。安全なメールやデータだけを取り扱うことができます。

● **ウェブアンチウイルス**　▶ 76 ページ
HTTP のトラフィックや HTML ファイルに埋め込まれているスクリプトを監視し、ウイルスの侵入を防ぎます。また、フィッシングサイトなどを判断して、危険なサイトへのアクセスをブロックし、脅威を未然に防ぎます。

フィッシングサイト
クレジットカード番号や銀行口座へのログインパスワードを入力させて盗むために、実在する金融機関などを装った偽のサイトのことをいいます。

● **メッセンジャーアンチウイルス**　▶ 78 ページ
インスタントメッセージングによる送受信データに、ウイルスが含まれていないかスキャンします。また、やりとりするデータにフィッシングサイトなどの危険なサイトへの URL が含まれていないかどうかもチェックします。

アプリケーション監視

● **アプリケーションコントロール** ▶ 79 ページ
悪意のあるアプリケーションがシステムファイルやレジストリなどの重要なデータに、不正にアクセスするのを防ぎます。
※アプリケーションコントロールは、カスペルスキー インターネット セキュリティのみの機能です。

● **システムウォッチャー** ▶ 83 ページ
システム内のアプリケーションの動作を監視し、記録します。もし、アプリケーションの不正な動作があった場合、記録に基づいて不正な動作を元に戻すことができます。また、収集した情報を他のプロテクション機能に提供します。

ネットワーク監視

● **ファイアウォール** ▶ 86 ページ
インターネットや LAN の利用時に、ネットワーク経由での不正なアクセスを防ぎます。コンピューターへ送られてくるデータと外に出て行くデータを監視して、不正なデータの出入りをブロックします。
※ファイアウォールは、カスペルスキー インターネット セキュリティのみの機能です。

● **ネットワーク攻撃防御** ▶ 88 ページ
ネットワークから侵入して大量のパケットを送信したり、インストールされているソフトウェアの情報を盗もうとしたりする攻撃を監視します。不正侵入を検知すると、ただちにネットワークをブロックし、警告を表示します。
※ネットワーク攻撃防御は、カスペルスキー インターネット セキュリティのみの機能です。

迷惑行為対策

● **アンチスパム** ▶ 89 ページ
不特定多数に向けられたダイレクトメールや迷惑メールのことをスパムといいます。スパムと思われるメールを識別して、メールの見出しにスパムの目印を付加したり、自動削除や指定したフォルダーへの移動などを選択したりできます。また、やりとりするデータに危険なサイトへの URL が含まれていないかどうかもチェックします。
※アンチスパムは、カスペルスキー インターネット セキュリティのみの機能です。

● **アンチバナー** ▶ 91 ページ
ブラウザーで Web サイトを閲覧中に表示されるポップアップ広告や、アプリケーションのメニュー部分などに勝手に追加されるバナー広告をスキャンして、表示をブロックします。
※アンチバナーは、カスペルスキー インターネット セキュリティのみの機能です。

● **保護者による管理** ▶ 56 ページ

子供や青少年が有害なサイトにアクセスするのをブロックしたり、コンピューターの利用時間は使用範囲を制限したりする機能です。コンピューターやインターネットの利用履歴、インスタントメッセンジャーや SNS を利用したメッセージの全記録などを確認することもできます。

※保護者による管理は、カスペルスキー インターネット セキュリティのみの機能です。

● **ネット決済保護** ▶ 59 ページ

インターネットバンキングやオンラインショッピングなど、インターネット上での決済時の処理情報を保護します。決済に使用する Web ページへのアクセス時にコンピューターを保護し、クレジットカード番号などの情報が第三者に漏えいするのを防止します。

※ネット決済保護は、カスペルスキー インターネット セキュリティのみの機能です。

● **キー入力の保護** ▶ 62 ページ

銀行など特定のサイトでパスワードなど入力するときには、自動的に特別な入力保護を行い、キーロガーに入力情報が盗まれるのを防ぎます。さらに、セキュリティキーボードでは、マウスで入力を行うことで、情報の漏えい防止を強化します。

キーロガー

コンピューターに侵入し、キーボードの操作を記録して、入力したログインパスワードやクレジットカード番号などの個人情報を盗むプログラムのことをいいます。

● **危険サイト診断** ▶ 66 ページ

ブラウザーでページを表示したとき、そのページに含まれるリンクに危険なページがないかどうかを自動的にチェックし、リンクの横に危険を示すアイコンを表示します。知らずに危険なサイトへアクセスしてしまうのを未然に防ぎます。

コンピューターのスキャン

ウイルスを常時監視するほかに、定期的にコンピューター内のファイルをスキャンすることで、常時監視中に検知できなかった脅威を発見し、感染を未然に防ぎます。

● **スキャン** ▶ 39 ページ

コンピューター内のすべてのファイルをスキャンする完全スキャンや、重要な領域のみをすばやくスキャンする簡易スキャン、疑わしいファイルやフォルダーを直接指定するオブジェクトスキャンなど、用途に応じて、さまざまな方法が選べます。オペレーティングシステムやアプリケーションのぜい弱性をスキャンすることもできます。さらに、スケジュールを設定して、定期的にスキャンを実行することで、安全性がより高まります。

定義データベースとプログラムのアップデート

プログラムや定義データベースを最新の状態に保つことは、プロテクション機能を効果のあるものにするために重要です。

● **アップデート** ▶ 36 ページ

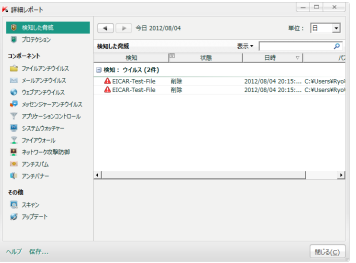
アップデートを有効にすることで、定義データベースとプログラムを常に最新に保つことができ、新たに発生する脅威から、リアルタイムでコンピューターを保護できます。

検知履歴の確認と処理の実行

ウイルスの検知や駆除など、各機能の履歴や結果は随時記録されます。日付や機能を指定して統計を出すこともでき、必要な情報をいつでも確認できます。また、未処理の脅威や疑わしいファイルを適切に処理することもできます。

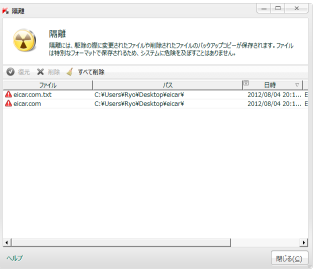
● **詳細レポート** ▶ 53 ページ

スキャンやアップデート、各プロテクション機能の実行履歴などを一覧で確認できます。さらに、これまでに検知した脅威の数や種類、またそれらの処理結果なども確認でき、未処理の脅威に対して駆除することもできます。



● **隔離** ▶ 55 ページ

感染されたかどうか疑わしいファイルを、特殊な領域に隔離して、システムを安全に保つことができます。また、駆除できたファイルは削除せずにバックアップしておくこともできます。

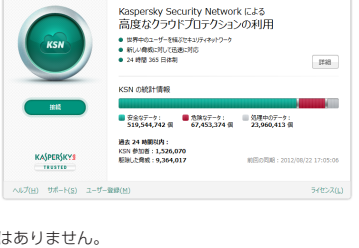


Kaspersky Security Network への参加

● **クラウドプロテクション**

Kaspersky Security Network（KSN）は、新しい脅威へいち早く対応できるようにする、オンラインサービスです。KSN は世界中のユーザーからデータを収集し、24 時間 365 日体制で、潜在的な脅威を分析します。KSN に参加すると、新しい脅威が発生したときにただちに Kaspersky Lab に報告され、いち早く対応策が開発されます。保護機能のパフォーマンスをさらに強化し、誤検知の可能性も軽減できます。

※KSN はいかなる個人情報も収集・転送することはありません。

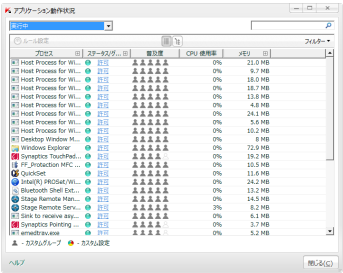


KSN へ参加するには、インストール時に選択するか、［設定］ウィンドウの［詳細設定］-［Kaspersky Security Network への参加］で、［Kaspersky Security Network への参加に同意する］をオンにします。

● **アプリケーション動作状況** ▶ 79 ページ

コンピューターで使用中のアプリケーションや、実行中のプロセスの情報を表示できます。また、グループ化されたアプリケーションのステータスを確認・変更することもできます。

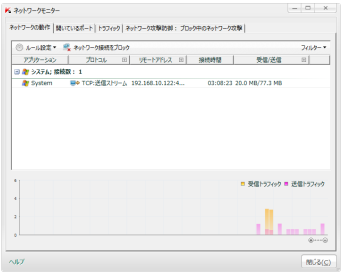
※アプリケーション動作状況は、カスペルスキー インターネット セキュリティのみの機能です。



● **ネットワークモニター** ▶ 100 ページ

ネットワークに接続しているアプリケーションの詳細情報や、アプリケーションごとの過去のトラフィック量、ファイアウォールとネットワーク攻撃防御による監視状態などが確認できます。

※ネットワークモニターは、カスペルスキー インターネット セキュリティのみの機能です。



● **レスキューディスク** ▶ 105 ページ

システムが破損してコンピューターが起動できなくなった場合、システムを修復する必要があります。修復時に、コンピューターの起動に必要な CD または USB メモリを作成します。この CD または USB メモリからコンピューターを起動すると、スキャンや駆除ができます。

● **Windows 設定診断** ▶ 107 ページ

Windows の設定状況をウィザード形式で診断します。ウイルスの感染によって引き起こされた、設定の誤りやぜい弱性を見つけ出し、問題が発見された場合は、正しい設定に修正します。

● **プライバシークリーナー** ▶ 108 ページ

コンピューターに残るさまざまな操作履歴をウィザード形式で検索し、削除します。操作履歴から、個人情報が漏えいするのを防ぎます。

● **Internet Explorer 設定診断** ▶ 109 ページ

Internet Explorer の設定状況をウィザード形式で診断します。ウイルス感染やシステム障害、アプリケーションの動作不良などを引き起こす恐れのある要因を見つけ出し、問題が発見された場合は、より安全な設定に修正します。

画面構成

メインウィンドウ

カスペルスキーの各機能、操作の中心となる画面です。コンピューターの保護状態や、各機能を起動するボタンなどが表示されています。

メインウィンドウを起動するには

Windows の [スタート] ボタンをクリックして、[すべてのプログラム - カスペルスキー インターネット セキュリティ 2013 - カスペルスキー インターネット セキュリティ 2013] を選択します。
タスクバーの通知領域のアイコンやガジェットからも起動できます。

▶ P.32 タスクバーのアイコン
▶ P.34 ガジェット

1 ボタン

各ボタンをクリックすると、それぞれの機能のウィンドウが表示されます。

項目	説明
クラウドプロテクション	Kaspersky Security Network（KSN）による高度なプロテクションについて、説明しています。
レポート	レポートウィンドウを表示します。これまでに検知した脅威をグラフで確認できます。 ▶ P.31 レポートウィンドウ
設定	設定ウィンドウを表示します。プロテクション、スキャン、アップデートなど、カスペルスキーの各機能の設定が行えます。 ▶ P.31 設定ウィンドウ
（検索）	機能の検索ができます。

2 情報表示エリア

コンピューターの現在の保護状態、データベースのアップデート状況、ライセンスの有効期間などが表示されています。
保護状態に問題が発生すると、情報が表示されます。
▶ P.35 保護状態の確認

クリックすると［セキュリティの問題］画面が表示され、問題解決の方法が確認できます。

3 機能やツールのランチャー群

スキャンやアップデート、便利ツールなど、カスペルスキーの主な機能やツールのアイコンが並んでいます。これらをクリックすることで必要な機能をすばやく起動できます。
アイコンは、左右の矢印ボタンをクリックしてスクロールできます。さらに、上向きの矢印ボタンをクリックすると、ウィンドウいっぱいにアイコンを表示されることができます。

項目	説明
スキャン	［スキャン］画面が表示されます。 ▶ P.39 スキャンの実行・設定
アップデート	［アップデート］画面が表示されます。 ▶ P.36 定義データベースとプログラムのアップデート
ネット決済保護	［ネット決済保護］画面が表示されます。 ▶ P.59 インターネット上の決済処理で使用する情報の保護
保護者による管理	［保護者による管理］画面が表示されます。 ▶ P.56 保護者によるコンピューター利用の制限
アプリケーション動作状況	アプリケーション動作状況ウィンドウが表示されます。 ▶ P.79 アプリケーションに設定されたステータスを確認・変更する
ネットワークモニター	ネットワークモニターウィンドウが表示されます。 ▶ P.100 ネットワークの接続状況を確認する（ネットワークモニター）
セキュリティキーボード	セキュリティキーボードが表示されます。 ▶ P.63 セキュリティキーボードを起動する

項目	説明
隔離	隔離ウィンドウが表示されます。 ▶ P.55 隔離されたオブジェクトを操作する
便利ツール	［便利ツール］画面が表示されます。 ▶ P.105 便利ツールの活用

4 サポート関連情報

それぞれクリックすると、次の項目を表示できます。

項目	説明
ヘルプ	ヘルプを起動します。詳細な設定方法や操作手順などを確認できます。
サポート	サポートウィンドウを表示します。製品のバージョンなどが確認できるほか、FAQ やテクニカルサポートサイトへアクセスできます。 ▶ P.115 ご購入後の技術的なお問い合わせ
ユーザー登録	ブラウザーを起動して、ユーザー登録ページを表示します。 ▶ P.113 ユーザー登録
ライセンス	ライセンス画面が表示されます。現在のライセンスの状態や、有効期限などが確認できます。この画面から、新たなライセンスの購入やアクティベーションの実行も可能です。 ▶ P.20 ライセンス

各種ウィンドウ

設定や確認を行うために、メインウィンドウから表示する主なウィンドウについて説明します。

設定ウィンドウ

［設定］ウィンドウでは、各機能やツールの設定を行います。スキャンやアップデートのスケジュールを設定したり、プロテクション機能のレベルを強くしたりできます。

［設定］ウィンドウは、メインウィンドウ右上にある［設定］をクリックして表示できます。

［設定］ウィンドウには、［プロテクション］／［スキャン］／［アップデート］／［詳細設定］の４つのカテゴリーがあり、ウィンドウ左上のアイコンで切り替えられます。
目的のカテゴリーに切り替えたら、項目一覧から設定したい項目を選択し、表示される内容を設定します。

レポートウィンドウ

［レポート］ウィンドウは、これまでに検知した脅威を分類して統計をとり、グラフで表示します。

［レポート］ウィンドウは、メインウィンドウ右上にある［レポート］をクリックして表示できます。
ウィンドウ上部にある、左右の矢印ボタンやドロップダウンリストで表示させる期間を指定できます。

ウィンドウ右下にある［詳細レポート］をクリックすると、［詳細レポート］ウィンドウが表示されます。
▶ P.53 処理結果の確認
また、レポートが準備されたことを通知させることもでき、 をクリックすると、通知の時間帯を設定することもできます。

タスクバーのアイコン

カスペルスキーのインストール後、タスクバーの通知領域にアイコンが表示されます。アイコンは、カスペルスキーの動作状態や保護状態により変化します。

Windows 7 では、通知領域の初期設定で、カスペルスキーアイコンの表示が隠れています。通知領域の左横にある、［隠れているインジケーターを表示します］をクリックすると表示されます。常に表示させたい場合は、［カスタマイズ］をクリックして、［通知領域アイコン］で設定を変更してください。

アイコンの表示

タスクバーの通知領域に表示されるアイコンは、カスペルスキーやコンピューターの状態によって、次のように表示が変わります。

	カスペルスキーは正常に動作しています。
	カスペルスキーが停止中です。またはプロテクション機能でエラーが発生しています。（「K」がモノクロで表示されます。）
	コンピューターの再起動が必要な状態です。

さらに、［設定］ウィンドウの［詳細設定］-［表示］で、［タスクの実行時に通知領域のアイコンをアニメーション表示する］をオンにして、アイコンのアニメーション表示を有効にすると、次のアイコンが表示されます。

	スキャンを実行しています。正常時と同じアイコンが大きくなったり小さくなったりします。
	アップデートを実行しています。
	メールアンチウイルスのメールスキャンを実行しています。
	ウェブアンチウイルスのトラフィックスキャンを実行しています。

アイコンの操作

タスクバーの通知領域にあるアイコンで、次の操作ができます。

● **メインウィンドウの表示**

クリックまたはダブルクリックをすると、メインウィンドウが表示されます。

▶ P.28 メインウィンドウ

● **メニューの表示**

右クリックするとメニューが表示され、ここから機能を実行できます。

右クリックして表示されるメニューには、次の項目が表示されます。

項目	説明
タスクマネージャー	タスクマネージャーを起動します。スキャンの進行状況や履歴など、スキャンに関する情報を確認できます。 ▶ P.40 タスクマネージャー
アップデート	プログラムと定義データベースのアップデートを行います。 ▶ P.36 定義データベースとプログラムのアップデート
ツール	アプリケーション動作状況、ネットワークモニター、セキュリティキーボードを起動します。 ※ アプリケーション動作状況、ネットワークモニターは、カスペルスキー インターネット セキュリティのみの機能です。 ▶ P.79 アプリケーションコントロール ▶ P.100 ネットワークの接続状況を確認する（ネットワークモニター） ▶ P.63 セキュリティキーボードを起動する
カスペルスキー インターネット セキュリティ	メインウィンドウが開きます。 ▶ P.28 メインウィンドウ
プロテクションの一時停止／再開	プロテクション機能の一時停止と再開を行います。 アップデートやスキャンスケジュールには影響を与えません。 ▶ P.47 プロテクション機能を一時的に停止する・再開する
保護者による管理を有効にする／無効にする	保護者による管理機能の有効／無効を切り替えます。 ※ 保護者による管理は、カスペルスキー インターネット セキュリティのみの機能です。 ▶ P.56 保護者によるコンピューター利用の制限
設定	［設定］ウィンドウが開きます。 ▶ P.31 設定ウィンドウ
カスペルスキー インターネット セキュリティについて	インストールされているカスペルスキーのバージョンやコピーライトが表示されます。
終了	カスペルスキーを終了します。 ▶ P.49 カスペルスキーを終了する・起動する

ガジェット

Windows 7 / Windows Vista では、カスペルスキー用のガジェットが使用できます。保護状態を確認したり、よく使う機能やツールをすばやく起動したりできます。スキャンしたいファイルやフォルダーをガジェットにドラッグすると、スキャンを実行することもできます。

Windows 7 の場合、カスペルスキーをインストールすると、ガジェットはデスクトップに自動的に表示されます。Windows Vista の場合、Windows サイドバーに手動でガジェットを追加する必要があります。Windows XP では使用できません。

画面の色で保護状態を確認できます。
クリックすると、メインウィンドウが表示されます。
右クリックすると、表示や設定に関するメニューが表示されます。

クリックすると、各ボタンに割り当てられた機能やツールが実行されます。

お知らせ **ガジェットのサイズを変更する**

ガジェットにポインターをあわせて表示されるアイコンで、[大きいサイズ] をクリックすると、大きいタイプのガジェットが表示されます。メインウィンドウとほぼ同様の操作が可能になります。

お知らせ **ボタンに割り当てる機能を変更する**

ガジェットにポインターをあわせて表示されるアイコンで、[オプション] をクリックすると、4 つのボタンに割り当てる機能を変更できます。

保護状態の確認

現在のコンピューターやネットワークの保護状態は、メインウィンドウやガジェットから確認できます。

保護状態を確認する

1. **メインウィンドウやガジェットに表示される、コンピューターのイラストで保護状態を確認します。**

▶ P.28 メインウィンドウ
▶ P.34 ガジェット

コンピューターの保護状態を色と説明文で示します。色の意味は、次のとおりです。

色［意味］	説明
緑［正常］	コンピューターの保護は適切に行われています。
黄［注意］	コンピューターは推奨する状態になっていません。
赤［危険］	コンピューターは危険な状態にあります。 すぐに対応が必要です。

保護状態の詳細を確認する

1. **メインウィンドウのコンピューターのイラストをクリックします。**

▶ P.29 情報表示エリア

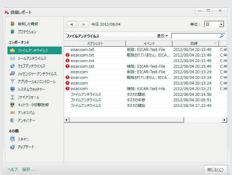
2. **［セキュリティの問題］画面に表示されている内容を確認します。**

問題がある場合は、その詳細を確認し、必要に応じて対処を行います。
問題ごとに、推奨する対処方法が表示されます。ボタンをクリックすると、それぞれの対処方法で解決します。

お知らせ **保護状態の履歴を確認する**

［詳細レポート］ウィンドウでは、保護の履歴を確認できます。

▶ P.53 処理結果の確認



定義データベースとプログラムのアップデート

日々発生する新たな脅威に備えるため、定期的にアップデートを実行することをおすすめします。カスペルスキーは、最新の脅威に対応できるようにするため、ウイルスなどを検知するための定義データベースと、プログラムを強化・修正するモジュールを、インターネットを経由して提供しています。
初期設定では、アップデートが必要か定期的に自動で確認されます。必要と判断されれば、他の作業をしていても、バックグラウンドで自動的に実行されます。

※アップデートを実行するには、コンピューターがインターネットに接続されている必要があります。

定義データベースの状態を確認する

現在使用している定義データベースが最新かどうかを確認します。

1. **メインウィンドウの［アップデート］をクリックします。**

2. **［アップデート］画面に、定義データベースの状態が表示されます。**
［定義データベースは最新です］と表示されていれば、問題ありません。
最新でない場合は、アップデートを実行します。

アップデートを実行する

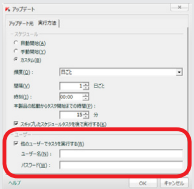
1. **メインウィンドウの［アップデート］をクリックします。**

2. **［アップデートの実行］をクリックします。**
［定義データベースをアップデートしています］と表示され、進行状況や経過時間が表示されます。
アップデートが終了すると、［定義データベースは最新です］と表示されます。

アップデートを実行中に［停止］をクリックすると、アップデートが中止されます。

お知らせ **権限のないアカウントでアップデートを実行する**

アップデート用のファイルが保存されるフォルダーへのアクセス権限を持たないユーザーでWindows にログオンしている場合、アップデートを実行するために、アクセス権限を持つユーザーを登録する必要があります。



1. メインウィンドウの［アップデート］をクリックします。
2. ［アップデートの実行］ボタン右横の［▼］をクリックして表示されるメニューから、［設定］をクリックします。
3. ［設定］ウィンドウの［アップデート］-［定義データベースのアップデート］で、［実行方法］をクリックします。
4. ［他のユーザーでタスクを実行する］をオンにします。
5. ［ユーザー名］と［パスワード］に、アクセス可能なユーザーのアカウント名とパスワードを入力します。
6. ［OK］をクリックします。

お知らせ **アップデートに必要なデータを複数のコンピューターで共有する**

複数のコンピューターを LAN で接続している場合、1 台に共有フォルダーを作成してアップデート用のファイルを共有することができます。アップデートサーバーにアクセスするのは複数あるコンピューターのうち 1 台だけで済むので、ネットワークトラフィックを軽減できます。

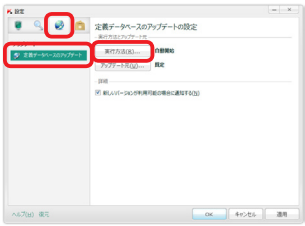
アップデートの実行方法を設定する

アップデートが実行されるスケジュールを設定します。
初期状態では、定義データベースが更新されると自動的にアップデートを実行するよう設定されています。通常はこのまま使用することをおすすめしますが、必要に応じて変更できます。

1. **メインウィンドウの［設定］をクリックします。**

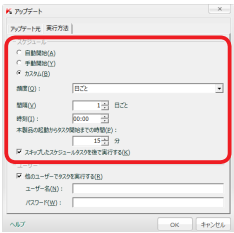
2. **［アップデート］の［定義データベースのアップデート］を選択します。**

3. **［実行方法］タブをクリックします。**



4. **［スケジュール］で、アップデートを開始する方法を選択します。**

選択できる方法は次のとおりです。



- **自動開始**
  アップデートサーバーで新しいデータが利用できるようになると、自動でアップデートファイルのダウンロードとインストールを実行します。
  自動的に定義データベースとプログラムが最新の状態になるので、この設定をおすすめします。
- **手動開始**
  ユーザーが手動でアップデートを行うまで、アップデートファイルのダウンロードとインストールは実行されません。
  定義データベースが古いまま放置される可能性があるので、通常はおすすめしません。
- **カスタム**
  指定するスケジュールに従って、自動的にアップデートを実行します。
  ［頻度］のドロップダウンリストから、アップデートの頻度を選択します。選択した頻度に応じて、日付や曜日、時間などを指定します。
  ［スキップしたスケジュールタスクを後で実行する］をオンにすると、指定した日時にコンピューターが起動していなかったなどの理由でアップデートが行われなかった場合に、処理が可能になった時点ですぐにアップデートが実行します。

5. **［OK］をクリックして、［アップデート］ウィンドウを終了します。**

6. **［OK］をクリックして、［設定］ウィンドウを終了します。**

スキャンの実行・設定

コンピューター内にウイルスが潜んでいないか、オペレーティングシステムやアプリケーションの設定にセキュリティの問題はないかなどを、スキャンします。
また、自動実行のスケジュールやスキャン対象の設定、検知時の処理などを設定できます。

スキャンの種類

次の種類のスキャンを実行できます。対象や用途によって使い分けることができます。

● **完全スキャン**
システムメモリ、ハードディスクドライブ、リムーバブルドライブなど、コンピューター内の全ファイルをスキャンします。

● **簡易スキャン**
システムメモリやオペレーティングシステムの起動時に読み込まれるプログラムなど、コンピューターが安定して動作するために重要なファイルをスキャンします。

● **オブジェクトスキャン**
ファイルやフォルダー、ドライブなど、スキャンする範囲や対象を個別に選択して、スキャンします。

● **ぜい弱性スキャン**
オペレーティングシステムやアプリケーションの設定内容をスキャンして、セキュリティの問題がないかを診断します。

ぜい弱性とは

コンピューターへの侵入やウイルス感染などを引き起こす、アプリケーションのセキュリティ上の弱点を指します。プログラムの欠陥（バグ）や仕様上の問題点が原因であることが多く、アプリケーションの開発元から提供される修正プログラムによって解消される場合があります。
一方で、ソフトウェアには問題なくとも、設定や運用方法などがぜい弱性を引き起こす原因となることもあります。

［完全スキャン］／［簡易スキャン］／［オブジェクトスキャン］の 3 つは、ファイルをスキャンして、主にウイルスを検知する目的で使用します。
［ぜい弱性スキャン］は、オペレーティングシステムやアプリケーションを分析して、セキュリティの問題を検知する目的で使用します。

スキャンを実行する

ファイルをスキャンして、コンピューター内のウイルスを検知します。
スキャン中は、メインウィンドウを閉じてもバックグラウンドで動作します。

スキャンを開始する前に

定義データベースが最新かどうかを確認してください。最新でない場合は、スキャンの前にアップデートを実行してください。

▶ P.36 定義データベースとプログラムのアップデート

完全スキャン／簡易スキャン／ぜい弱性スキャン

1. **メインウィンドウの［スキャン］をクリックします。**
2. **［スキャン］画面で、［完全スキャン］、［簡易スキャン］、［ぜい弱性スキャン］の ▶ をクリックします。**

   スキャンが実行されます。

お知らせ　タスクマネージャー

［スキャン］右上にある画面［タスクの管理］をクリックすると、［タスクマネージャー］ウィンドウが表示されます。

タスクマネージャーは、スキャン中の進行状況や終了したスキャンの履歴を確認できる機能です。実行中のスキャンを停止したり、ぜい弱性スキャン後に検知結果一覧を表示させたりすることもできます。さらに、［完了］または［停止］した時間のリンクをクリックすると、［詳細レポート］ウィンドウが表示され、より詳しいタスク履歴の情報が確認できます。

▶ P.53 処理結果の確認

お知らせ　スキャンを停止・再開する

スキャン中の ◉ をクリックすると、スキャンの停止を確認する画面が表示されるので、［はい］をクリックして、停止します。

停止したあとにもう一度 ▶ をクリックすると、前回中断したスキャンを再開するか、最初からスキャンを開始するかを選べます。

お知らせ　完全スキャンが完了したら、Windows をシャットダウンさせる

完全スキャンを実行した場合、スキャン完了時に Windows をシャットダウンしたり、休止状態にしたりすることができます。完全スキャンを実行すると表示される、［スキャン完了時］のドロップダウンメニューから、スキャン完了後の動作を選択します。

お知らせ　検知されたぜい弱性

ぜい弱性スキャンのあと、ぜい弱性が検知されると［検知されたぜい弱性］ボタンが表示されます。クリックすると、［ぜい弱性スキャン］ウィンドウが起動し、検知されたぜい弱性の詳細が一覧で表示されます。オペレーティングシステムとアプリケーションで検知されたぜい弱性がそれぞれ［システムに存在するぜい弱性］タブ、［ぜい弱性を持つアプリケーション］タブに表示されます。検知された項目を選択すると、ぜい弱性ごとに応じた解決策が表示されるので、必要に応じて対応できます。

オブジェクトスキャン

オブジェクトスキャンの対象を選択するには、次の 3 つの方法があります。

ファイルをドラッグ＆ドロップ

1. **メインウィンドウの［スキャン］をクリックします。**

2. **画面右下にあるドロップスペースに、スキャンしたいファイルやフォルダーをドラッグ＆ドロップします。**

   オブジェクトスキャンが実行されます。
   ［タスクマネージャー］ウィンドウが起動し、スキャンの進行状況が表示されます。

> カスペルスキーガジェットにドラッグ＆ドロップしても、同様にスキャンが実行されます。

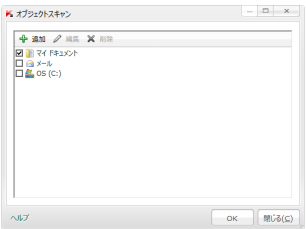
［オブジェクトスキャン］ウィンドウから選択

1. **メインウィンドウの［スキャン］をクリックします。**
2. **画面右下にあるドロップスペースをクリックします。**
3. **表示される［オブジェクトスキャン］ウィンドウの一覧から、スキャンしたい対象をオンにします。**

   一覧にスキャンしたい対象がない場合は、［追加］をクリックして、［オブジェクトの選択］ウィンドウから選択します。

4. **［OK］をクリックします。**

   ［オブジェクトスキャン］ウィンドウが終了し、オブジェクトスキャンが実行されます。



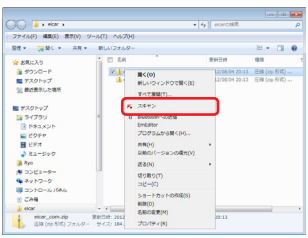
エクスプローラーで右クリック

1. **エクスプローラーを起動します。**
2. **スキャンしたい対象を表示し、右クリックします。**

   メニューが表示されます。

3. **［スキャン］を選択します。**

   オブジェクトスキャンが実行されます。

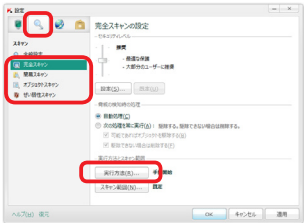


スキャンの自動実行を設定する

スケジュールを指定して、スキャンをバックグラウンドで自動実行させるように設定できます。重要なファイルやフォルダーを安全に保ち、コンピューターを安定して稼働させるために、定期的なスキャンの実行をおすすめします。

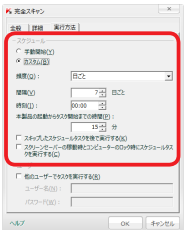
1. **メインウィンドウの［設定］をクリックします。**

2. **［スキャン］の［完全スキャン］／［簡易スキャン］／［ぜい弱性スキャン］のいずれかを選択します。**



3. **［実行方法］をクリックします。**

4. **表示される［完全／簡易／ぜい弱性スキャン］ウィンドウで、［スケジュール］の［カスタム］をオンにします。**



5. **［頻度］のドロップダウンリストから、スキャンの頻度を選択します。**

   選択した頻度に応じて、スキャンを実行する日付や曜日、時間などを指定します。
   ［スキップしたスケジュールタスクを後で実行する］では、スキャンをスキップする場合に、何分後にスキャンを再実行するかを指定します。
   ［スキップしたスケジュールタスクを後で実行する］をオンにすると、スキャンが実行されなかった場合に、実行可能な状態になった時点ですぐに実行されます。スキャンを指定した日時にコンピューターを起動していなかった場合などに役立ちます。
   ［スクリーンセーバーの稼働時とコンピューターのロック時にスケジュールタスクの実行する］オンにすると、ユーザーが作業していない時間にスキャンを実行させることができます。

6. **［OK］をクリックして、［完全／簡易／ぜい弱性スキャン］ウィンドウを終了します。**

7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

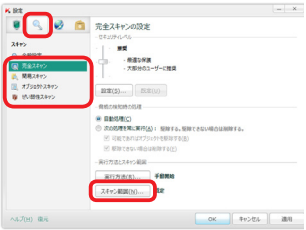
スキャンの対象を設定する

スキャンの対象となるファイルやフォルダーを設定します。

1. メインウィンドウの［設定］をクリックします。

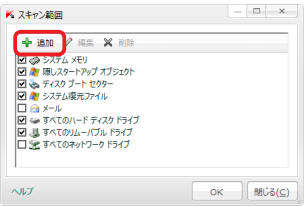
2. ［スキャン］の［完全スキャン］／［簡易スキャン］／［ぜい弱性スキャン］のいずれかを選択します。

3. ［スキャン範囲］をクリックします。



4. 表示される［スキャン範囲］ウィンドウの一覧から、スキャンしたい対象をオンにします。

5. 一覧にスキャンしたい対象がない場合は、［追加］をクリックします。

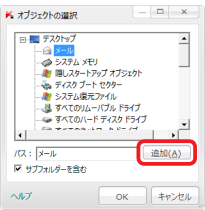


6. 表示される［オブジェクトの選択］ウィンドウのツリーから、追加したいオブジェクトやフォルダーを選択します。

   選択したフォルダーのサブフォルダーを対象に含める場合は、［サブフォルダーを含む］をオンにします。

7. ［追加］をクリックします。

   ［スキャン範囲］ウィンドウの一覧に、選択したオブジェクトやフォルダーが追加されます。



8. ［OK］をクリックして、［オブジェクトの選択］ウィンドウを終了します。

9. ［OK］をクリックして、［スキャン範囲］ウィンドウを終了します。

10. ［OK］をクリックして、［設定］ウィンドウが終了します。

セキュリティレベルを設定する

セキュリティレベルとは、複合ファイルの扱いやヒューリスティック分析を行うかどうかなど、スキャンの方法をあらかじめ定義したものです。セキュリティレベルを選択することで、スキャン方法を簡単に変更できます。

複合ファイル

圧縮ファイルやインストーラーファイルなど、1 つのファイルの中に複数のファイルが含まれているファイルを指します。カスペルスキーは、複合ファイルに含まれている内部のファイルもスキャンできます。

ヒューリスティック分析

定義データベースに登録されていない、未知のウイルスなどの脅威を検知する仕組みです。

ご注意

セキュリティレベルを高くすると安全性が増す代わりに、スキャンに時間がかかってコンピューターへの負荷が大きくなります。セキュリティレベルを低くすると、スキャン速度が向上してコンピューターに負荷が小さくなる反面、安全性が低くなります。

1. メインウィンドウの［設定］をクリックします。

2. ［スキャン］の［完全スキャン］／［簡易スキャン］／［オブジェクトスキャン］のいずれかを選択します。

3. ［セキュリティレベル］のバーを移動して、レベルを選択します。

選択できるレベルは次のとおりです。

- **高**
  最もセキュリティが高いレベルです。感染する危険性が高い環境で使用する場合におすすめします。
- **推奨**
  セキュリティとコンピューターへの負荷がバランスのとれたレベルです。一般的な環境で使用する場合におすすめします。
- **低**
  最もセキュリティが低いレベルですが、コンピューターへの負荷は一番軽くなります。

4. ［OK］をクリックして、［設定］ウィンドウを終了します。

お知らせ　スキャン方法を詳細に設定する

［設定］ウィンドウの［セキュリティレベル］で［設定］をクリックし、設定を変更します。各設定項目の詳細については、ヘルプを参照してください。

脅威の検知時の処理方法を設定する

スキャンの実行中にウイルスなどの脅威が検知された場合、どのように駆除や削除を行うかを設定します。

1. **メインウィンドウの［設定］をクリックします。**
2. **［スキャン］の［完全スキャン］／［簡易スキャン］／［オブジェクトスキャン］のいずれかを選択します。**
3. **［脅威の検知時の処理］で、処理方法を選択します。**

［脅威の処理方法］の設定で、［自動処理］がオンになっているかオフになっているかによって、選択できる項目が異なります。
▶ P.69 脅威の処理方法を変更する

- **自動処理（脅威の処理方法の自動処理がオンの場合）**
  検知されると、すぐに駆除が行われます。駆除できなかった場合は、オブジェクトごと削除されます。
- **スキャン完了時に通知する（脅威の処理方法の自動処理がオフの場合）**
  スキャン終了までオブジェクトの処理を行いません。スキャン完了時に検知されたオブジェクトが［タスクマネージャー］ウィンドウに表示されるので、オブジェクトごとに処理方法を選択します。
- **検知時に通知する（脅威の処理方法の自動処理がオフの場合）**
  検知されると、通知ウィンドウが表示されるので、処理を選択します。
  ▶ P.50 通知ウィンドウが表示されたら
- **次の処理を常に実行（脅威の処理方法共通）**
  検知されると通知ウィンドウを表示せず、感染されたかどうか疑わしいオブジェクトも含めて、常に同じ処理を行います。
  以下の項目を組み合わせて処理方法を指定します。

項目	説明
☑ 可能であればオブジェクトを駆除する ☑ 駆除できない場合は削除する	検知されると、すぐに駆除が行われます。駆除できなかった場合、オブジェクトごと削除されます。
☑ 可能であればオブジェクトを駆除する ☐ 駆除できない場合は削除する	検知されると、すぐに駆除が行われます。駆除できなかった場合は、隔離に移動されます。このオブジェクトは、あとで［タスクマネージャー］または［詳細レポート］で駆除できます。 ▶ P.53 処理結果の確認
☐ 可能であればオブジェクトを駆除する ☑ 削除する	検知されると、すぐにオブジェクトごと削除されます。
☐ 可能であればオブジェクトを駆除する ☐ 削除する	検知されると、そのオブジェクトへのアクセスがブロックされ、通知ウィンドウが表示されます。このオブジェクトは、あとで［タスクマネージャー］または［詳細レポート］で駆除できます。 ※この選択肢は、脅威がそのままコンピューターに存在し続けることになるので、おすすめしません。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

リムーバブルドライブ検出時の動作を設定する

USB メモリなどのリムーバブルドライブをコンピューターに取り付けたとき、そのドライブ内をスキャンするかどうか、どのようにスキャンするか、などを設定します。

1. **メインウィンドウの［設定］をクリックします。**
2. **［スキャン］の［全般設定］を選択します。**
3. **［リムーバブルドライブの検出時］で、スキャン方法を選択します。**

   選択できる項目は、次のとおりです。

   - **スキャンしない**
     スキャンしません。
   - **手動選択**
     リムーバブルドライブが検出されるたびに通知ウィンドウが表示され、スキャンするかどうかを選択します。
   - **完全スキャン**
     ［完全スキャン］と同じ設定で、リムーバブルドライブのスキャンを開始します。［スキャンするドライブサイズ］をオンにすると、スキャンするリムーバブルドライブの上限サイズを指定できます。
   - **簡易スキャン**
     ［簡易スキャン］と同じ設定で、リムーバブルドライブのスキャンを開始します。［スキャンするドライブサイズ］をオンにすると、スキャンするリムーバブルドライブの上限サイズを指定できます。
4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

スキャン実行用のショートカットアイコンを作成する

スキャンをひんぱんに、かつ不定期に実行したい場合、デスクトップなどにショートカットアイコンを作っておくと便利です。メインウィンドウを起動せずに、アイコンをダブルクリックしてスキャンを開始できます。また、スタートアップフォルダーにアイコンを作成すると、コンピューターの起動時に必ずスキャンを実行するようにも設定できます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［スキャン］の［全般設定］を選択します。**
3. **［ショートカット］で、［完全スキャン］／［簡易スキャン］／［ぜい弱性スキャン］のいずれかの［ショートカットの作成］をクリックします。**
4. **保存したい場所とショートカット名を指定して、［保存］をクリックします。**

   ショートカットアイコンが作成されます。
5. **［OK］をクリックして、［設定］ウィンドウを終了します。**

プロテクション機能の停止・再開

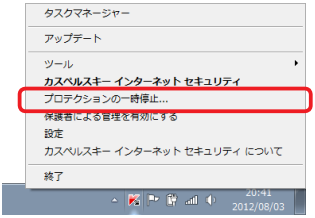
カスペルスキーでは、プロテクション機能を停止したり再開したりできます。他のアプリケーションをインストールする際など、必要に応じて停止できますが、その間はウイルス感染の危険性が非常に高くなるので、注意が必要です。

プロテクション機能を一時的に停止する・再開する

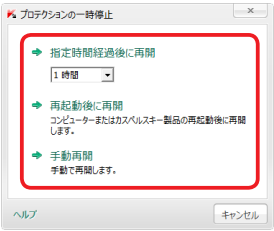
一時的にすべてのプロテクション機能を停止できます。再開までの時間を指定して、一定時間後に自動的に再開することもできます。

プロテクションを停止する

1. **タスクバーの通知領域にあるカスペルスキーのアイコンを右クリックし、［プロテクションの一時停止］を選択します。**



2. **表示される［プロテクションの一時停止］ウィンドウで、プロテクション機能を再開させる方法を選択します。**
［指定時間経過後に再開］／［再起動後に再開］／［手動再開］のいずれかをクリックします。
プロテクション機能が停止します。
［指定時間経過後に再開］の場合はドロップダウンリストから再開する時間を選択します。



プロテクションを再開する

1. **タスクバーの通知領域にあるカスペルスキーのアイコンを右クリックし、［プロテクションの再開］を選択します。**
プロテクション機能が再開します。

お知らせ **プロテクション機能の自動再開**

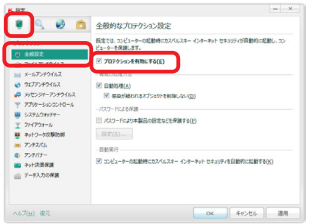
［設定］ウィンドウの［プロテクション］-［全般設定］で、［コンピューターの起動時にカスペルスキー インターネット セキュリティを自動的に起動する］がオンになっていると、コンピューターを再起動すればプロテクション機能が自動的に再開されます。この項目は、初期設定でオンになっています。

プロテクション機能を完全に停止する

すべてのプロテクション機能を完全に停止するには、プロテクションを無効にします。完全に停止した場合は、コンピューターの再起動後も手動で再開するまでプロテクション機能は開始されません。
ただし、スケジュールに従ったスキャンとアップデートは、プロテクション機能の停止中でも実行されます。

1. メインウィンドウの［設定］をクリックします。

2. ［プロテクション］の［全般設定］を選択します。



3. ［プロテクションを有効にする］をオフにします。

4. ［OK］をクリックして、［設定］ウィンドウを終了します。

お知らせ **プロテクション機能を個別に停止する**

［設定］ウィンドウの［プロテクション］では、［ファイルアンチウイルス］や［メールアンチウイルス］などのプロテクション機能ごとに無効にして、保護を停止することもできます。

お知らせ **他のアプリケーションでの作業を優先させる**

プロテクション機能によって、作業中のアプリケーションの応答速度が低下する場合があります。こうした場合は、作業中の他のアプリケーションに優先的にシステムリソースを使用させることで、改善される可能性があります。

この方法を利用する場合は、［設定］ウィンドウで［詳細］の［パフォーマンス］を選択し、［他のアプリケーションにシステムリソースを優先する］をオンにします。

▶ P.101 パフォーマンスに関する機能の設定

カスペルスキーを終了する・起動する

カスペルスキーのプログラムを終了する方法と、起動する方法は、次のとおりです。

カスペルスキーを終了する

1. **タスクバーの通知領域にあるカスペルスキーのアイコンを右クリックして、［終了］を選択します。**

   カスペルスキーが終了します。

   ネットワークに接続している場合

   カスペルスキーを正常に終了するには、ネットワーク接続を切断する必要があります。終了時にネットワークに接続しているアプリケーションがあるとき、接続の処理を確認するウィンドウが表示されるので、指示に従ってください。ネットワーク接続を切断しないと、カスペルスキーは終了できません。

カスペルスキーを起動する

1. **Windows の［スタート］ボタンをクリックし、［すべてのプログラム－カスペルスキー インターネット セキュリティ 2013 －カスペルスキー インターネット セキュリティ 2013］を選択します。**

   カスペルスキーが起動します。

※カスペルスキー アンチウイルス 2013 の場合は、［すべてのプログラム－カスペルスキー アンチウイルス 2013 －カスペルスキー アンチウイルス 2013］です。

通知ウィンドウが表示されたら

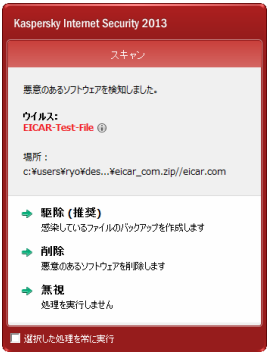
カスペルスキーがウイルスや危険なメールなどの脅威を検知すると、通知ウィンドウを表示して、処理の選択を促すことがあります。特に、脅威の処理方法が自動処理でない場合は、脅威が検知されるたびに表示されます。

▶ P.69 脅威の処理方法を変更する

通知ウィンドウが表示されたら、画面の指示に従って、処理を選択します。表示されている選択肢のいずれかに「推奨」と表示されている場合は、通常はその選択肢を選ぶことをおすすめします。

通知ウィンドウの種類

表示される通知ウィンドウは、危険の度合いによって色分けされます。



色［意味］	説明
赤［警告］	ウイルス感染やアプリケーションの危険な動作が検知された場合に表示されます。危険度が高いため、すぐに処理することをおすすめします。
黄［注意］	ウイルス感染の可能性やアプリケーションの疑わしい動作が検知された場合に表示されます。 ユーザーが確実に信頼できると判断した場合は、処理を行わない方法を選択できます。
緑［情報］	権限のないアプリケーションの動作や新しいネットワークの検出時などに、ユーザーに確認を促します。ユーザーの判断で選択します。

また、プロテクション機能が一部停止していたり、アップデートが実行されていなかったりする場合にメッセージが表示される場合があります。この場合は、メッセージをクリックして、処理を行います。

選択できる処理

通知ウィンドウに表示される選択肢は、検知された脅威の種類によって異なります。
代表的な選択肢は、次のとおりです。

● スキャン中やメールを受信中に検知された場合

駆除	ウイルスを駆除します。
削除	ウイルスを含んだファイルを削除します。
隔離	疑わしいオブジェクトを隔離へ移動します。定義データベースが更新されたあとに再度スキャンを実行し、脅威かどうかあらためて確認できます。
ブロック	ウイルスを含んだファイルへのアクセスをブロックします。駆除・削除は行われません。
無視／スキップ	ウイルスへの処理を何も行いません。

● Web サイトからオブジェクトをダウンロード中に検知された場合

要求を許可	オブジェクトのダウンロードを続行します。
要求のブロック	オブジェクトのダウンロードを中止します。

● アプリケーションが不正なアクセスを試みた場合

［許可］に変更	アプリケーションの実行を常に許可します。アプリケーションルールに設定され、以降は検知されなくなります。 ▶ P.79 アプリケーションに設定されたステータスを確認・変更する
今回は許可	そのときに限り、アプリケーションの実行を許可します。
今回はブロック	そのときに限り、アプリケーションの実行をブロックします。
アプリケーションの終了とブロックの設定	アプリケーションの実行を中止し、実行をブロックするグループに設定します。

● アクセスしようとしている Web サイトがフィッシングサイトだと検知された場合

許可	Web サイトへのアクセスを続行します。
ブロック	Web サイトへのアクセスをブロックします。

● 新しいネットワークが検出された場合

パブリックネットワーク	インターネットやファイアウォールなどで保護されていないネットワークに接続するときに選択します。ファイルとプリンターの共有をブロックします。また、自分のコンピューターを外部から接続できないようにします。
プライベートネットワーク	企業の LAN など、保護されているが脅威に遭遇する可能性があるネットワークのときに選択します。ファイルとプリンターの共有を許可します。
信頼できるネットワーク	安全性が高いネットワークのときに選択します。すべての接続が許可されます。

通知方法を変更する

ウイルスの検知やプロテクション機能の停止などのイベントが発生すると、警告やお知らせを通知します。どのように通知するかをイベントの種類ごとに設定できます。

1. **メインウィンドウの［設定］をクリックします。**

2. **［詳細］の［イベント通知］を選択します。**

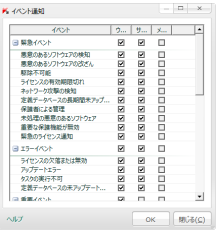
3. **［イベント通知を有効にする］をオンにします。**

必要に応じて、［メールによるイベント通知を有効にする］／［サウンドによるイベント通知を有効にする］をオンにします。

4. **イベントごとに細かい設定を行う場合は、［設定］をクリックします。**

5. **表示される［イベント通知］ウィンドウで、イベントごとに［ウィンドウ］／［サウンド］／［メール］のオン／オフを設定します。**

   オンにした方法で通知されます。



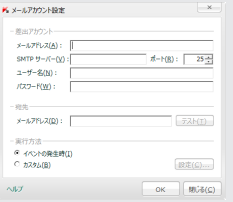
6. **［OK］をクリックして、［イベント通知］ウィンドウを終了します。**

7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **メールアカウントを設定する**

通知をメールで受け取る場合、送信用のアカウントや通知先のメールアドレス、さらに通知のタイミングなどを設定する必要があります。

1. **［設定］ウィンドウで、［メールによるイベント通知を有効にする］をオンにします。**
2. **［メールアカウント設定］をクリックします。**
   表示される［メールアカウント設定］ウィンドウで、各項目を設定します。



［メールアカウント設定］ウィンドウの各設定項目の詳細については、ヘルプを参照してください。

処理結果の確認

カスペルスキーがこれまでに検知した脅威の数や種類、またそれらの処理結果などを、リストやグラフで確認できます。
検知されて未処理のオブジェクトを駆除したり、駆除後のオブジェクトを削除したりもできます。

レポートを表示して確認する

1. **メインウィンドウの［レポート］をクリックします。**

   ［レポート］ウィンドウが表示されます。

2. **表示される［レポート］ウィンドウで、検知済みの脅威をグラフで確認します。**

   ウィンドウ右上のドロップダウンリストで表示する期間を選んだり、ウィンドウ左上にある矢印のアイコンをクリックして表示する期間を切り替えたりできます。

3. **［詳細レポート］をクリックします。**

4. **表示される［詳細レポート］ウィンドウで、項目を選択して内容を確認します。**

   ［表示］のドロップダウンリストで表示方法を選んだり、検索ボックスに入力して表示する内容を絞り込んだりできます。

ご注意　レポートの保存期間・サイズによるパフォーマンス低下を防ぐには

記録されるレポートは、プログラム内に蓄積されます。蓄積されたレポートが増大すると、ディスク容量を圧迫してコンピューターのパフォーマンスが低下する場合があります。［設定］ウィンドウの［詳細］-［レポートと隔離］で、［レポート］の［保存期間］と［保存サイズ］を設定したり、定期的にレポートを削除したりして、ディスク容量を空けることをおすすめします。

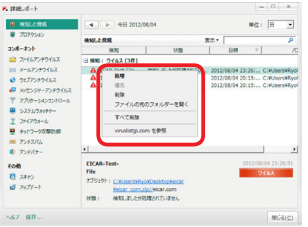
検知された脅威を処理する

1. ［詳細レポート］ウィンドウで、［検知した脅威］を選択します。

2. 表示された一覧から、処理したいオブジェクトを選択して、右クリックします。

3. 表示されたショートカットメニューから、実行したい処理を選択します。

   オブジェクトの種類によって、表示される項目が異なります。



主な項目は次のとおりです。

項目	説明
処理 （未処理の場合）	選択したオブジェクトを処理します。 通知ウィンドウが表示された場合は、処理方法を選択します。
復元	選択したオブジェクトを元の場所へ復元します。 安全が確認されたファイルに対して行ってください。
削除	選択したオブジェクトを削除します。
ファイルの元のフォルダーを開く	ファイルがあったフォルダーが開きます。
すべて削除	表示されているすべてのオブジェクトを削除します。
viruslistjp.com を参照 （未処理の場合）	ブラウザーが起動し、オブジェクトについての詳細情報が記載された Web ページが開きます。

ご注意　オブジェクトを駆除できないとき

処理を実行しても駆除できない場合は、［削除］を選択し、オブジェクトごと削除することをおすすめします。なお、自分で作ったプログラムなど、安全であることが確実なオブジェクトの場合、信頼リストに設定して、アクセスのブロックを解除できます。

▶ P.94 信頼する対象の設定

ご注意　復元には十分に注意してください

隔離からオブジェクトを復元するときは、安全であることを十分に確認してから行ってください。復元されたファイルがウイルスに感染したままだった場合、コンピューター全体の感染を招く恐れがあります。

レポートを保存する

詳細レポートで表示された一覧は、テキストファイルに保存することも可能です。

1. ［詳細レポート］ウィンドウで、保存したい内容を表示させます。

2. ウィンドウ左下の［保存］をクリックします。

3. 保存するフォルダーとファイル名を指定します。

   拡張子は「*.txt」か「*.csv」のどちらかを選択できます。

4. ［保存］をクリックします。

   レポートファイルが保存されます。

隔離されたオブジェクトを操作する

隔離とは、駆除・削除された危険なオブジェクトを、安全な状態にして特殊な領域に保存する処理です。ウイルスに感染した危険なファイルでも、特別なフォーマットに変換されて安全に閉じ込めておけます。隔離されたオブジェクトは、コンピューターのシステムにアクセスできなくなるので、ウイルスや悪意のあるプログラムによる被害やその拡散を防ぐことができます。また、隔離されたオブジェクトを、あとから削除・復元することもできます。

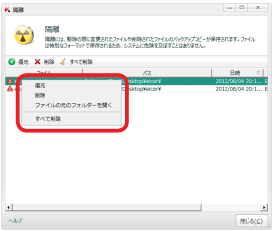
ご注意　復元には十分に注意してください

隔離されたオブジェクトを復元するときは、安全であることを十分に確認してから行ってください。復元されたファイルがウイルスに感染したままだった場合、コンピューター全体の感染を招く恐れがあります。

1. メインウィンドウの［隔離］をクリックします。

2. 表示される［隔離］ウィンドウの一覧から、操作対象のファイルを右クリックし、操作したい項目を選択します。

※一部の項目は、一覧の上にあるアイコンをクリックしても操作可能です。



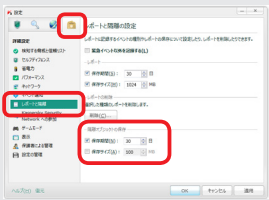
操作可能な項目は、次のとおりです。

項目	説明
復元	選択したファイルを元のフォルダーへ復元します。 安全が確認されたファイルに対して行ってください。
削除	ファイルを削除します。
ファイルの元のフォルダーを開く	ファイルがあったフォルダーが開きます。
すべて削除	隔離に格納されている、すべてのファイルを削除します。

お知らせ　隔離の保存期間・サイズを設定する

［設定］ウィンドウの［詳細］-［レポートと隔離］-［隔離オブジェクトの保存］で、隔離する期間や、オブジェクトのサイズなどを設定で来ます。

各設定項目の詳細についてはヘルプで説明していますので、そちらを参照してください。



保護者によるコンピューター利用の制限

保護者による管理は、コンピューターやインターネットを子供が使用できる範囲を制限する機能です。利用時間や使用できるアプリケーションを限定したり、有害なサイトへのアクセスを制限したりできます。
Windows のユーザーアカウント単位で設定できるため、ログオンするアカウントごとに制限の内容を変えることができます。
※保護者による管理は、カスペルスキー インターネット セキュリティのみの機能です。

カスペルスキーの設定変更や終了などの際にパスワードの入力を求める、パスワードによる保護機能があります。保護者による管理を使用する場合は、子供が設定を変更できないように、パスワードによる保護を設定することをおすすめします。
▶ P.69 パスワードを設定して操作を制限する

保護者による管理を有効にする

制限したいユーザーアカウントを選択して、保護者による管理機能を有効にします。

1. メインウィンドウの［保護者による管理］をクリックします。

パスワードによる保護を設定していない場合は、設定を促す画面が表示されるので、ここで設定することをおすすめします。

コンピューターに登録されているユーザーアカウントが一覧で表示されます。

2. 保護者による管理を有効にしたいユーザーアカウントの［有効にする］をクリックします。

［有効にする］が［無効にする］に切り替わり、ユーザーアカウント名の下に「管理が有効になっています」と表示されます。

お知らせ　設定ウィンドウから保護者による管理を設定する

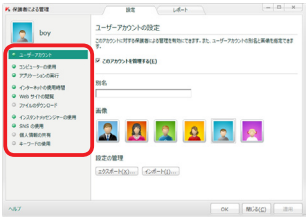
機能の有効／無効の切り替えや設定内容の設定は、設定ウィンドウから行うこともできます。［設定］ウィンドウで［詳細］の［保護者による管理］を選択すると、有効／無効の切り替えや設定が行えます。

制限する内容を設定する

ユーザーアカウントごとに、制限する内容を設定します。

1. ［保護者による管理］画面で、制限内容を設定したいユーザーアカウントの ⚙ をクリックします。

2. 表示される［保護者による管理］ウィンドウで、設定したい項目を選択して設定します。



設定できる項目は、次のとおりです。

項目	説明
ユーザーアカウント	保護者による管理の有効／無効を切り替えたり、一覧に表示されるユーザーを区別するための画像や表示名を指定したりします。設定内容をファイルに保存したり、保存した設定内容を読み込んだりすることもできるので、同じ設定内容を複数のユーザーに設定するときに便利です。
コンピューターの使用	コンピューターを使用できる時間を制限します。 使用可能な時間帯を曜日ごとに指定したり、1 日の使用時間を限定したりできます。
アプリケーションの実行	使用できるアプリケーションを制限します。 アプリケーションごとに使用の許可またはブロックを設定したり、許可する場合は使用できる時間を設定したりできます。
インターネットの使用	インターネットを使用できる時間を制限します。 使用可能な時間帯を曜日ごとに指定したり、1 日の使用時間を限定したりできます。
Web サイトの閲覧	閲覧可能な Web サイトを制限します。 ブロックする Web サイトのジャンルを選択したり、許可またはブロックする Web サイトを個別に指定したりできます。 検索エンジンによる検索結果に、ブロックする Web サイトへのリンクを表示させないようにすることもできます。
ファイルのダウンロード	ダウンロードできるファイルを制限します。 ファイルのジャンルごとに許可またはブロックを設定できます。
インスタントメッセンジャーの使用	インスタントメッセンジャーを使ったやりとりを制限します。送受信されたメッセージをすべて記録し、接続する相手ごとに許可またはブロックを設定できます。
SNS の使用	ソーシャルネットワークサービスを使ったやりとりを制限します。送受信されたメッセージをすべて記録し、接続する相手ごとに許可またはブロックを設定できます。
個人情報の送信	設定した個人情報の送信を制限します。 もし設定した情報をデータの中に見つけると、送信をブロックし、履歴を残します。
キーワードの使用	送信されるデータ中に、特定の語句が含まれていないかを監視します。もし設定した語句をデータの中に見つけると、相手先やその時間などの履歴を残します。

項目名の冒頭のマークが緑色の項目は、制限が有効になっています。

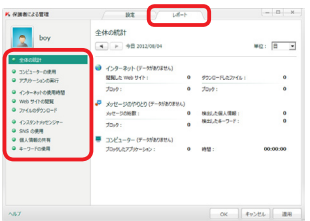
使用状況を確認する

保護者による管理を有効にすると、ユーザーごとの使用状況が確認できます。
インターネットに接続した時間やアクセスした URL、SNS でやりとりしたメッセージなどをすべて記録します。これを保護者があとで確認し、制限する内容を見直すこともできます。

1. **［保護者による管理］画面で、確認したいユーザーアカウントの をクリックします。**

2. **表示される［保護者による管理］ウィンドウで、［レポート］タブをクリックします。**

3. **確認したい項目を選択して、使用状況を確認できます。**
さらに、使用状況に応じた制限を設定することもできます。
たとえば、Web サイトの閲覧では、ユーザーがアクセスした URL がすべて表示されます。その中に好ましくない Web サイトがあった場合は、個別にブロックすることもできます。



※設定方法について、詳しくはヘルプを参照してください。

インターネット上の決済処理で使用する情報の保護

インターネットバンキングやオンラインショッピングを利用するときには、ネット上で銀行口座やクレジットカードなどの大切な情報を扱うことになります。ネット決済保護機能は、こうした個人情報を悪意ある第三者に盗まれないよう、安全に入力できる環境を作成する機能です。ネット決済で使用するコンピューターやブラウザーを保護し、操作内容や個人情報の漏えいを防ぐので、インターネット上での決済を安全に行うことができます。

ネット決済保護機能を利用する

ネット決済保護機能は、初期設定で有効になっており、銀行や決済システムの Web サイトにアクセスすると、保護されたブラウザーを使って表示するかどうかを確認するように設定されています。

1. **ブラウザーを起動し、銀行などの Web サイトへアクセスします。**
2. **ログインページへのリンクをクリックします。**
3. **保護されたブラウザーを使ってアクセスするかどうかを選択するページが表示されます。次の操作を選択します。**

- **実行**
  保護されたブラウザーを使ってアクセスします。
- **スキップ**
  通常のブラウザーを使ってアクセスします。
- **この Web サイトでの設定を保存する**
  オンにすると、［実行］または［スキップ］のどちらをクリックしたかを記憶し、次回同じページへアクセスするときには、この選択画面を表示せず、次回以降も同じ方法で Web サイトへアクセスします。
  オフにすると、次回もこの選択画面を表示します。

4. **［実行］をクリックすると、保護されたブラウザーが起動し、ログインページが表示されます。**

   保護されたブラウザーは、ウィンドウの周りが緑色で囲まれています。このブラウザー上で入力した情報は一切記録されず、外部からの不正なアクセスからも保護された、安全な状態で取引操作が行えます。

ご注意 **「重要なシステム更新がインストールされていません」と表示されたら**

Windows のシステムが最新版に更新されていない場合に表示されることがあります。
［アップデートの実行］をクリックすると、Windows Update が表示されるので、更新プログラムのダウンロード／インストールを行ってからログインページへアクセスすることをおすすめします

ネット決済保護機能を設定する

保護されたブラウザーを使ってアクセスする Web サイトを特定したり、選択画面を表示せずに保護されたブラウザーを自動で起動するように設定したりすることができます。

Web サイトを手軽に追加する

少ない手順で簡単に Web サイトを設定します。

1. **メインウィンドウの［ネット決済保護］をクリックします。**

2. **［追加］をクリックします。**

3. **追加する Web サイトの URL と、一覧に表示される説明を入力します。**

4. **［OK］をクリックします。**

［ネット決済保護］画面の一覧に追加した Web サイトが表示されます。リンクをクリックすると、保護されたブラウザーで追加した Web サイトが開きます。

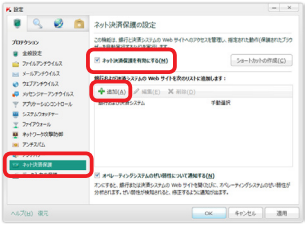
［ネット決済保護］画面の一覧で、⚙または🗑をクリックすると、設定内容の編集や削除ができます。

詳細に設定する

Web サイトにアクセスしたときの動作など、詳しく設定します。

1. **メインウィンドウの［設定］をクリックします。**

2. **［プロテクション］の［ネット決済保護］を選択します。**



3. **［ネット決済保護を有効にする］をオンにします。**

   ［銀行および決済システムの Web サイトを次のリストに追加します］の一覧に、登録済みの Web サイトの URL が表示されます。

4. **［追加］をクリックします。**

   設定を変更する場合は、登録済みの Web サイトを選択して［編集］をクリックします。

5. **表示された［ネット決済保護の Web サイト］ウィンドウで、次の項目を設定します。**

   - **銀行または決済システムの Web サイト：**
     保護されたブラウザーを使ってアクセスしたい Web サイトの URL を入力します。
   - **説明：**
     一覧に表示される Web サイトの説明を入力します。
   - **この Web サイトへのアクセス時：**
     登録する Web サイトへアクセスした際の動作を、次から選択します。
     - **手動選択**
       アクセスするたびに保護されたブラウザーを使用するかどうかを選択します。
     - **保護されたブラウザーを自動実行する**
       自動的に保護されたブラウザーを使ってアクセスします。
     - **保護されたブラウザーを実行しない**
       保護されたブラウザーを使わず、通常のブラウザーでアクセスします。

6. **［OK］をクリックして、［ネット決済保護の Web サイト］ウィンドウを終了します。**

   ［オペレーティングシステムのぜい弱性について通知する］

   オンにすると、Web サイトにアクセスする直前に Windows のぜい弱性がチェックされます。Windows に問題がある場合、「重要なシステム更新がインストールされていません」というメッセージを表示し、Windows Update を実行して Windows を最新の状態にすることを促します。

7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **ネット決済保護のショートカットを作成する**

［設定］ウィンドウで［ショートカットの作成］をクリックすると、デスクトップにネット決済保護のショートカットアイコンが作成されます。

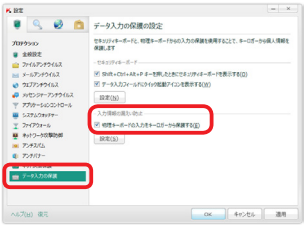
入力情報の漏えいを防止

悪意のあるプログラムの中には、キーボードの操作を記録して、入力したログイン ID やパスワードなどの個人情報を盗む、キーロガーと呼ばれるプログラムがあります。
カスペルスキーは、キーの入力情報からデータの漏えいを防ぐための機能を備えています。銀行など特定のサイトで入力するときには、入力されたデータを自動的に保護し、キーロガーに入力情報が盗まれるのを防ぎます。
さらに、仮想のキーボードである「セキュリティキーボード」はマウス操作でキー入力ができます。物理的なキー入力を行わないことによって、キーロガーに情報を与えません。

キーボード入力の保護を設定する

特定の Web サイトでデータ入力を行う際に、キー入力が保護されるように設定します。

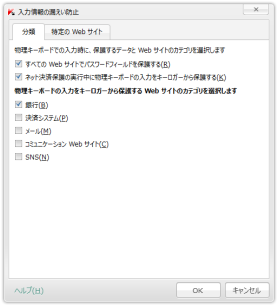
1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［データ入力の保護］を選択します。**



3. **［入力情報の漏えい防止］で、［物理キーボードの入力をキーロガーから保護する］をオンにします。**

   はじめてこの機能を使う場合は、コンピューターの再起動が必要になります。メッセージが表示されたら、［再起動する］をクリックします。
   再起動したら、もう一度［設定］ウィンドウを表示して、［プロテクション］の［データ入力の保護］を選択します。

4. **［設定］をクリックします。**
5. **表示された［入力情報の漏えい防止］ウィンドウで、Web サイトのカテゴリーを選択します。**



   ［すべての Web サイトでパスワードフィールドを保護する］をオンにすると、Web サイトのカテゴリーを問わず、すべての Web サイトのパスワード入力欄で保護が有効になります。
   ［ネット決済保護の実行中に物理キーボードの入力をキーロガーから保護する］をオンにすると、ネット決済保護機能とデータ入力保護機能の組み合わせによって、セキュリティがさらに強まります。
   ▶ P.59 インターネット上の決済処理で使用する情報の保護

   保護する Web サイトを個別に設定したい場合は、［特定の Web サイト］タブをクリックして、Web サイトの URL を指定します。

6. ［OK］をクリックして、［入力情報の漏えい防止］ウィンドウを終了します。

7. ［OK］をクリックして、［設定］ウィンドウを終了します。

設定した Web サイトにブラウザーでアクセスし、データ入力欄をクリックすると「キーボード入力の保護が有効です」というポップアップメッセージが表示され、保護が有効であることを確認できます。

セキュリティキーボードを起動する

セキュリティキーボードを起動するには、次の方法があります。

Windows の再起動が必要です

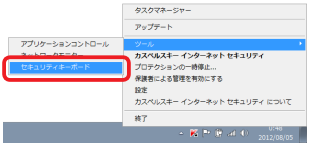
カスペルスキーをインストールした直後は、セキュリティキーボードを使用できません。一度、Windows を再起動すると、使用可能になります。

● **メインウィンドウから起動する**

メインウィンドウの［セキュリティキーボード］をクリックすると、セキュリティキーボードを起動できます。

● **タスクバーのアイコンから起動する**

タスクバーの通知領域にあるアイコンを右クリックして、表示されるメニューから、［ツール］-［セキュリティキーボード］をクリックすると、セキュリティキーボードを起動できます。



● **ショートカットキーで起動する**

Shift+Ctrl+Alt+P キーを同時に押すと、セキュリティキーボードを起動できます。このショートカットキーは、設定で有効／無効の切り替えができます。初期設定ではオンになっています。［設定］ウィンドウで［プロテクション］の［データ入力の保護］を選択し、［Shift+Ctrl+Alt+P キーを押したときにセキュリティキーボードを表示する］のオン／オフを切り替えます。

● **ブラウザーのツールバーアイコンで起動する**

Microsoft Internet Explorer、Mozilla Firefox、Google Chrome のツールバーにあるアイコン K をクリックすると、セキュリティキーボードを起動できます。

● **ブラウザーの入力欄に表示されるクイック起動アイコンで起動する**

ブラウザーでインターネットバンキングなどの特定の Web サイトにアクセスしたときに、パスワードなどの入力欄にカーソルを置くと、入力欄の中にキーボードのアイコンが表示されます。そのアイコンをクリックすることでセキュリティキーボードを起動できます。

クイック起動アイコンを表示させるには、次ページの設定が必要です。

クイック起動アイコンの表示設定

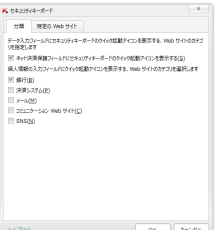
1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［データ入力の保護］を選択します。**

3. **［セキュリティキーボード］で、［データ入力フィールドにクイック起動アイコンを表示する］をオンにします。**

   はじめてこの機能を使う場合は、コンピューターの再起動が必要になります。メッセージが表示されたら、［再起動する］をクリックします。

   再起動したら、もう一度［設定］ウィンドウを表示して、［プロテクション］の［データ入力の保護］を選択します。

4. **［設定］をクリックします。**
5. **表示された［セキュリティキーボード］ウィンドウで、起動アイコンを表示させる Web サイトのカテゴリーを選択します。**



   ［ネット決済保護フィールドにセキュリティキーボードのクイック起動アイコンを表示する］をオンにすると、ネット決済保護機能の保護されたブラウザー上でもセキュリティキーボードが使用でき、セキュリティがさらに強まります。

   ▶ P.59 インターネット上の決済処理で使用する情報の保護

   Web サイトを個別に設定したい場合は、［特定の Web サイト］タブをクリックして、Web サイトの URL を指定します。

6. **［OK］をクリックして、［セキュリティキーボード］ウィンドウを終了します。**
7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

セキュリティキーボードを利用する

セキュリティキーボードは、キーをクリックすることでキーボード入力と同じ操作ができます。
ここでは、セキュリティキーボードを使うために、特殊なキー操作やヒントなどを説明します。

● Shift / Ctrl / Alt キーを同時に押す場合

複数のキーを同時に押す必要がある Shift / Ctrl / Alt キーは、クリックするとキーを押したままの状態になります。たとえば、Shift キーをクリックすると、キーボードの英字が大文字に変わり、大文字での入力が可能になります。他のキーをクリックすると、押したままの状態が解除されます。

● フルキーボードを表示する

をクリックすると、テンキー付きのフルキーボードが表示されます。

● クイック起動アイコンの設定を変更する

をクリックすると、［セキュリティキーボード］ウィンドウが表示され、クイック起動アイコンを表示させる Web サイトなどの設定ができます。

▶ P.63 ブラウザーの入力欄に表示されるクイック起動アイコンで起動する

現在ブラウザーで表示している Web サイトでは、今後クイック起動アイコンを表示させたくない場合は、をクリックして表示されるウィンドウで、［指定した Web ページでのみアイコンを表示しない］を選択して、［OK］をクリックします。

危険なサイトへのリンクを診断

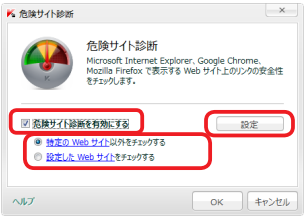
危険サイト診断は、ブラウザーでページを表示したとき、そのページに含まれるリンクをスキャンして、危険なページがないかどうかを自動的にチェックする機能です。もし、危険なページへのリンクが検知された場合、リンクの横に危険を示すアイコン が表示されます。安全な場合は が表示されます。アイコンにマウスポインターをあわせると、説明がポップアップ表示されます。

対応するブラウザーは、Microsoft Internet Explorer、Mozilla Firefox、Google Chrome です。ブラウザーの設定で、カスペルスキー製品のアドオンが有効になっていることを確認してください。

危険サイト診断を設定する

診断対象とする Web サイトを設定します。すべての Web サイトを診断するか、診断する Web サイトを指定するか、選択できます。

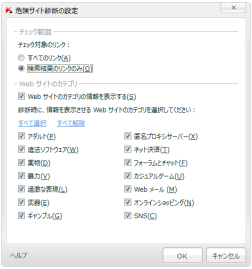
1. **ブラウザーのツールバーにあるアイコン ［危険サイト診断］をクリックします。**
2. **［危険サイト診断］ウィンドウで、［危険サイト診断を有効にする］をオンにします。**



3. **診断の対象となる Web サイトの種類を指定します。［設定］をクリックします。**

［危険サイト診断の設定］ウィンドウが表示されます。

［チェック範囲］では、すべてのリンクを診断の対象とするか、検索サイトによる検索結果のリンクのみにするかを選択します。
［Web サイトのカテゴリー］では、診断する Web サイトの種類を選択します。



4. **［OK］をクリックして、［危険サイト診断］ウィンドウに戻ります。**
5. **診断の対象となる Web サイトの範囲を次から選択します。**

- **特定の Web サイト以外をチェックする**
  すべての Web サイトを診断します。通常はこちらを選択します。
  確実に安全だとわかっていて、診断を行わない Web サイトがある場合には、その URL を指定して、診断の対象から除外することもできます。
- **設定した Web サイトをチェックする**
  特定の Web サイトのみを診断したい場合、そのサイトの URL を指定します。

診断を除外する、または診断する特定の Web サイトの指定方法は、選択した項目によって以降の手順が異なります。

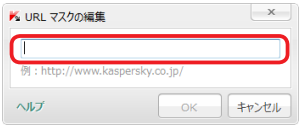
[特定の Web サイト以外をチェックする] を選択した場合

診断を行わない Web サイトの URL を設定します。

1. [危険サイト診断] ウィンドウで、[特定の Web サイト] をクリックします。
2. [特定の Web サイト] ウィンドウで、[追加] をクリックします。

3. [URL マスクの編集] ウィンドウで、診断しない Web サイトの URL を入力して [OK] をクリックします。

   [URL マスクの編集] ウィンドウが終了し、一覧に URL が表示されます。

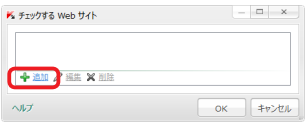


4. URL 横のチェックボックスがオンになっていることを確認し、[OK] をクリックして [特定の Web サイト] ウィンドウを終了します。
5. [OK] をクリックして、[危険サイト診断] ウィンドウを終了します。

[設定した Web サイトをチェックする] を選択した場合

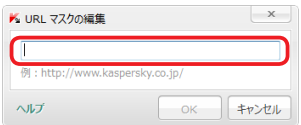
診断する Web サイトの URL を設定します。

1. [危険サイト診断] ウィンドウで、[設定した Web サイト] をクリックします。
2. [チェックする Web サイト] ウィンドウで、[追加] をクリックします。



3. [URL マスクの編集] ウィンドウで、チェックする Web サイトの URL を入力して、[OK] をクリックします。

   [URL マスクの編集] ウィンドウが終了し、一覧に URL が表示されます。



4. URL 横のチェックボックスがオンになっていることを確認し、[OK] をクリックして [チェックする Web サイト] ウィンドウを終了します。
5. [OK] をクリックして、[危険サイト診断] ウィンドウを終了します。

お知らせ 設定ウィンドウで危険サイト診断を設定する

危険サイト診断の設定は、[設定] ウィンドウでも同様に設定できます。

[設定] ウィンドウの [プロテクション] - [ウェブアンチウイルス] で、[設定] をクリックします。表示される [ウェブアンチウイルス] ウィンドウの [セーフサーフ] タブで設定します。

全般的なプロテクション設定

各機能に共通な、プロテクション全般の設定を行います。

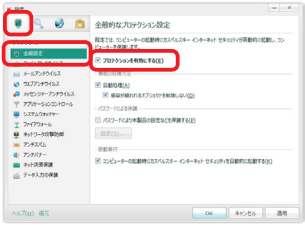
プロテクションの有効・無効を切り替える

各プロテクション機能は、アンチバナー機能を除き、初期設定で有効になっています。
次の手順で、プロテクションの有効／無効を切り替えられます。

プロテクション機能を無効にすることはおすすめしませんが、アプリケーションの種類によっては、一部のプロテクション機能を停止することで正常に動作する場合があります。

すべてのプロテクション機能の有効・無効を切り替える

1. メインウィンドウの［設定］をクリックします。
2. ［設定］ウィンドウで［プロテクション］の［全般設定］を選択します。
3. ［プロテクションを有効にする］をオン／オフして、有効／無効を切り替えます。
4. ［OK］をクリックして、［設定］ウィンドウを終了します。



タスクバーの通知領域のアイコンを右クリックして表示されるメニューからも、プロテクション機能の有効／無効が切り替えられます。
▶ P.32 タスクバーのアイコン

プロテクションごとに有効・無効を切り替える

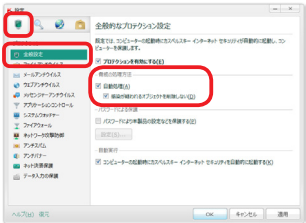
1. メインウィンドウの［設定］をクリックします。
2. ［設定］ウィンドウの［プロテクション］から、有効／無効を切り替えたい機能名を選択します。
3. ［○○を有効にする］をオン／オフして、機能の有効／無効を切り替えます。
   ※「○○」には、選択した機能名が表示されます。
4. ［OK］をクリックして、［設定］ウィンドウを終了します。

脅威の処理方法を変更する

脅威の処理方法は、ウイルスなどの脅威が検知されたときの動作を設定します。
自動処理に設定しておくと、ウイルスが検知されたとき、カスペルスキーが処理方法を判断して自動的に駆除や削除を行います。自動処理にしなかった場合は、検知するたびに通知ウィンドウが表示されますので、ユーザーが処理方法を判断して指示する必要があります。通常は、自動処理にしておくことをおすすめします。

脅威の処理方法の設定によって、検知時の処理方法が変わります。
▶ P.70 検知時の処理方法を設定する

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［全般設定］を選択します。**
3. **［脅威の処理方法］の［自動処理］をオン／オフして、自動で処理するか手動で処理するかを設定します。**
4. **必要に応じて、［感染が疑われるオブジェクトを削除しない］を設定します。**



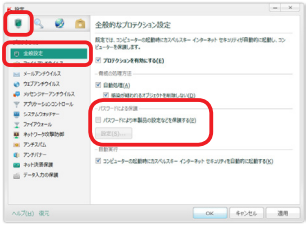
5. **［OK］をクリックして、［設定］ウィンドウを終了します。**

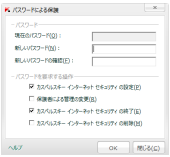
パスワードを設定して操作を制限する

複数のユーザーでコンピューターを使用する場合、他のユーザーがプログラムを停止したり、設定を変更したりできないようにできます。特に、保護者による管理機能を有効にして、子供が有害なサイトへアクセスできないように制限する場合には、設定を自由に変更できないよう、パスワードを設定することをおすすめします。
▶ P.56 保護者によるコンピューター利用の制限

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［全般設定］を選択します。**
3. **［パスワードによる保護］の［パスワードにより本製品の設定などを保護する］をオンにします。**
4. **［設定］をクリックします。**
5. **［パスワードによる保護］ウィンドウで、現在設定中のパスワードと新しく設定したいパスワードをそれぞれ入力します。**

   新規にパスワードによる保護を設定する場合は、［現在のパスワード］を入力する必要はありません。





6. ［パスワードを要求する操作］で、パスワード入力が必要になる操作を選択します。

選択した操作を実行すると、パスワードを求めるウィンドウが表示されるようになります。

- **カスペルスキー インターネット セキュリティの設定**
  プロテクション／スキャン／アップデート機能の設定を変更したり、機能の有効／無効を切り替えたりする操作を保護します。
  ※ただし、保護者による管理機能の設定変更は制限されません。
- **保護者による管理の変更**
  保護者による管理機能の設定変更の操作を保護します。
- **カスペルスキー インターネット セキュリティの終了**
  カスペルスキーを終了する操作を保護します。
- **カスペルスキー インターネット セキュリティの削除**
  カスペルスキーをアンインストールする操作を保護します。

7. ［OK］をクリックして、［パスワードによる保護］ウィンドウが終了します。

8. ［OK］をクリックして、［設定］ウィンドウを終了します。

検知時の処理方法を設定する

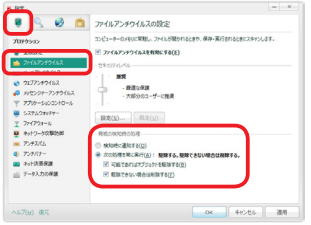
ウイルスなどの脅威が検知された場合、ファイルアンチウイルス／メールアンチウイルス／ウェブアンチウイルスの 3 機能は、あらかじめ設定された方法に従ってウイルスを処理します。初期設定では、［自動処理］に設定されています。使用する環境に応じて変更できます。

脅威の処理方法の設定で、自動処理がオンになっている場合の選択肢は［自動処理］、オフになっている場合の選択肢は［検知時に通知する］になります。
▶ P.69 脅威の処理方法を変更する

1. メインウィンドウの［設定］をクリックします。

2. ［プロテクション］で、［ファイルアンチウイルス］／［メールアンチウイルス］／［ウェブアンチウイルス］のいずれかを選択します。

3. ［脅威の検知時の処理］で、処理方法を次から選択します。



● **自動処理（脅威の処理方法の自動処理がオンの場合）**
感染したオブジェクトが検知されると、最も推奨される方法で、すぐに駆除が行われます。駆除できなかった場合は、オブジェクトごと削除されます。
感染が疑わしいオブジェクトが検知された場合は、処理は行われません。
ウェブアンチウイルスの場合は、Web サイトやオブジェクトへのアクセスがブロックされます。

● **検知時に通知する（脅威の処理方法の自動処理がオフの場合）**
感染した、または疑わしいオブジェクトが検知されると、通知ウィンドウが表示されます。ウイルスの情報、感染されたファイル名、処理方法のオプションを確認しながら、オブジェクトごとに処理方法を指定します。
ウェブアンチウイルスの場合は、通知ウィンドウで Web サイトやオブジェクトへのアクセスを継続するか中断するかを選択します。
▶ P.50 通知ウィンドウが表示されたら

● **次の処理を常に実行（ファイルアンチウイルス／メールアンチウイルスの場合）**
感染されたかどうか疑わしいオブジェクトも含めて脅威が検知されると、通知ウィンドウを表示せず、以下の項目を組み合わせて指定する方法で処理されます。

項目	説明
☑ 可能であればオブジェクトを駆除する ☑ 駆除できない場合は削除する	検知されると、すぐに駆除が行われます。駆除できなかった場合、オブジェクトごと削除されます。
☑ 可能であればオブジェクトを駆除する ☐ 駆除できない場合は削除する	検知されると、すぐに駆除が行われます。駆除できなかった場合は、［隔離］に移動されます。このオブジェクトは、あとで［詳細レポート］で駆除できます。 ▶ P.55 隔離されたオブジェクトを操作する ▶ P.54 検知された脅威を処理する
☐ 可能であればオブジェクトを駆除する ☑ 削除する	検知されると、すぐにオブジェクトごと削除されます。
☐ 可能であればオブジェクトを駆除する ☐ 削除する	検知されると、そのオブジェクトへのアクセスがブロックされ、［レポート］に記録されます。このオブジェクトは、あとで［履歴］で駆除できます。 ※危険なオブジェクトがそのままコンピューターに存在し続けることになるので、おすすめしません。

● **ダウンロードのブロック（ウェブアンチウイルスの場合）**
オブジェクトへのアクセスがブロックされ、通知ウィンドウが表示されます。

● **ダウンロードの許可（ウェブアンチウイルスの場合）**
オブジェクトへのアクセスを継続します。

4. ［OK］をクリックして、［設定］ウィンドウを終了します。

ファイルアンチウイルス
（ファイルからの感染を検知）

ファイルアンチウイルスは、ファイル操作を監視し、ウイルス感染からコンピューターを保護する機能です。コンピューターが起動すると自動的にファイルアンチウイルスが起動して、ファイルを開く、保存する、実行するなどの操作が行われるときに、リアルタイムでファイルをスキャンして、ウイルスをチェックします。

セキュリティレベルを設定する

セキュリティレベルとは、複合ファイルの扱いやヒューリスティック分析を行うかなど、スキャンの方法をあらかじめ定義したものです。セキュリティレベルを選択することで、スキャン方法を簡単に変更できます。

複合ファイル

圧縮ファイルやインストーラーファイルなど、1 つのファイルの中に複数のファイルが含まれているファイルを指します。カスペルスキーは、複合ファイルに含まれている内部のファイルもスキャンできます。

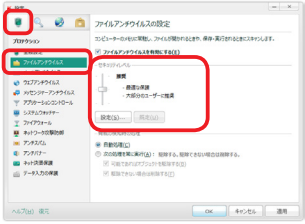
ヒューリスティック分析

定義データベースに登録されていない、未知のウイルスなどの脅威を検知する仕組みです。

初期設定では、［推奨］に設定されています。使用する環境にあわせて変更できます。

セキュリティレベルを高くすると、安全性が増す代わりにスキャンに時間がかかり、コンピューターへの負荷が大きくなります。セキュリティレベルを低くすると、スキャン速度が向上し、コンピューターに負荷が小さくなる反面、安全性が低くなります。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［ファイルアンチウイルス］を選択します。**
3. **［セキュリティレベル］のバーを移動してレベルを選択します。**



選択できるレベルは次のとおりです。

- **高**

  最もセキュリティが高いレベルです。
  すべてのドライブにあるすべての種類のファイルと、新規作成または更新された圧縮ファイル・インストールパッケージ、すべての OLE 埋め込みオブジェクトをスキャンします。
  感染する危険性が高い環境で使用する場合におすすめします。

● **推奨**

安全性と速度が最適化されたレベルです。
すべてのドライブにあるファイルのファイル形式を分析してスキャンします。新規作成または更新されたOLE埋め込みオブジェクトはスキャンしますが、圧縮ファイル・インストールパッケージはスキャンしません。
一般的な環境で使用する場合におすすめします。

● **低**

最もセキュリティが低いですが、スキャン速度が最も速いレベルです。
すべてのドライブにある新規作成または更新されたファイルの、拡張子を分析してスキャンします。
保護されたネットワーク環境（社内ネットワークなど）では、このレベルで快適に操作できます。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **ファイルを監視対象から除外する**

ファイルアンチウイルスの監視対象から除外したいオブジェクトがある場合は、信頼リストを設定してください。

▶ P.94 信頼する対象の設定

お知らせ **詳細な設定**

ファイルアンチウイルスのスキャン方法をより詳細に設定できます。スキャンの技術を選択したり、コンピューター負荷の大きい時間帯や特定のアプリケーションを起動したときなどにファイルアンチウイルスを一時的に停止したりすることもできます。

［設定］ウィンドウで［プロテクション］の［ファイルアンチウイルス］を選択し、［セキュリティレベル］で［設定］をクリックすると、［ファイルアンチウイルス］ウィンドウが表示されます。設定を変更すると、セキュリティレベルは「カスタム」と表示されます。初期値に戻すには［既定］をクリックします。

［ファイルアンチウイルス］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

メールアンチウイルス
（メールからの感染を検知）

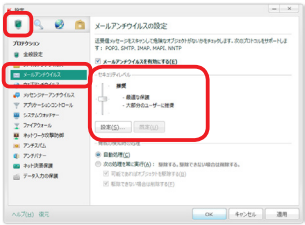
メールアンチウイルスは、メールを監視し、メールで受信または送信されそうになったウイルスなど悪意のあるオブジェクトを取り除く機能です。メールで使用される通信方式（POP3、SMTP、IMAP、MAPI、NNTP）を利用した送受信を監視し、リアルタイムでメールをスキャンしてウイルスをチェックします。

セキュリティレベルを設定する

セキュリティレベルとは、複合ファイルの扱いやヒューリスティック分析を行うかなど、スキャンの方法をあらかじめ定義したものです。セキュリティレベルを選択することで、スキャン方法を簡単に変更できます。
初期設定では、［推奨］に設定されています。使用する環境にあわせて変更できます。

セキュリティレベルを高くすると、安全性が増す代わりにスキャンに時間がかかり、コンピューターへの負荷が大きくなります。セキュリティレベルを低くすると、スキャン速度が向上し、コンピューターに負荷が小さくなる反面、安全性が低くなります。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［メールアンチウイルス］を選択します。**
3. **［セキュリティレベル］のバーを移動してレベルを選択します。**



選択できるレベルは次のとおりです。

- **高**
  最もセキュリティが高いレベルです。
  送信／受信メールの両方を監視し、圧縮ファイルを含むすべての添付ファイルもスキャンします。また、ヒューリスティック分析のレベルが［強］に設定されます。
  感染する危険性が高い環境で使用する場合におすすめします。
- **推奨**
  安全性と速度が最適化されたレベルです。
  送信／受信メールの両方を監視し、圧縮ファイルを含むすべての添付ファイルもスキャンします。また、ヒューリスティック分析のレベルが［中］に設定されます。
  一般的な環境で使用する場合におすすめします。
- **低**
  最もセキュリティが低いですが、スキャン速度が最も速いレベルです。
  受信メールだけを監視し、圧縮ファイルを含む添付ファイルはスキャンしません。
  また、ヒューリスティック分析のレベルが［弱］に設定されます。保護されたネットワーク環境（社内ネットワークなど）では、このレベルで快適に操作できます。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **メールを監視対象から外す**

メールアンチウイルスの監視対象から除外したいオブジェクトがある場合は、除外ルールを設定してください。

▶ P.94 信頼する対象の設定

お知らせ **詳細な設定**

メールアンチウイルスのスキャン方法をより詳細に設定できます。添付ファイルを拡張子やファイル名でフィルタリングし、条件にあった添付ファイルを受信前に削除することもできます。

［設定］ウィンドウで［プロテクション］の［メールアンチウイルス］を選択し、［セキュリティレベル］で［設定］をクリックすると、［メールアンチウイルス］ウィンドウが表示されます。設定を変更すると、セキュリティレベルは「カスタム」と表示されます。初期値に戻すには［既定］をクリックします。

［メールアンチウイルス］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

Microsoft Office 使用時にスキャンのタイミングを設定する

Microsoft Office Outlook を使用している場合は、専用のプラグインを利用して、スキャンする項目の設定が行えます。

1. **Microsoft Office Outlook 2010 の場合は［ファイル - オプション］を選択し、［アドイン］の［アドイン オプション］をクリックします。**
   Microsoft Office Outlook 2007 / 2003 の場合は、［ツール - オプション］を選択します。

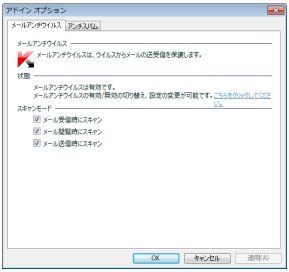
2. **［アドイン オプション］ウィンドウで、［メールアンチウイルス］タブをクリックします。**

3. **［スキャンモード］から必要な項目をオンにします。**

   スキャンのタイミングを選択します。

   ［アンチスパム］タブをクリックすると、アンチスパムの設定ができます。

   ▶ P.90 迷惑メールの処理方法を設定する



4. **［OK］をクリックして、［アドイン オプション］ウィンドウを終了します。**

ご注意 **IMAP プロトコルを利用する場合**

メール受信に IMAP プロトコルを利用する場合、［メール受信時にスキャン］をオンにすると、サーバー上のメールがコンピューターへダウンロードされます。不要なメールをダウンロードしないという IMAP の利点が失われるので、注意してください。

ウェブアンチウイルス
（Web ページからの感染を検知）

ウェブアンチウイルスは、Web ページを閲覧する際に使用される通信手段（HTTP）によって送られてくるデータを監視して、ウイルスや不正なスクリプトなど悪意のあるオブジェクトを検知したり、フィッシングサイトへのアクセスを未然に防いだりする機能です。

ご注意　監視対象のネットワークポートを確認してください

ウェブアンチウイルスは、監視するネットワークポートリストに記載されているポートを通過する HTTP の通信のみを監視します。一般的に使われる HTTP やメールに利用されるポートなどはリストに設定されています。リストにないポートを使用する場合は、手動で追加してください。

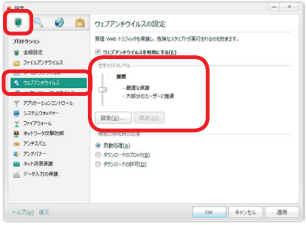
▶ P.86 ファイアウォール

セキュリティレベルを設定する

セキュリティレベルとは、フィッシングサイトのチェックやヒューリスティック分析を行うかなど、スキャンの方法をあらかじめ定義したものです。セキュリティレベルを選択することで、スキャン方法を簡単に変更できます。
初期設定では、［推奨］に設定されています。使用する環境にあわせて変更できます。

セキュリティレベルを高くすると、安全性が増す代わりにスキャンに時間がかかり、コンピューターへの負荷が大きくなります。セキュリティレベルを低くすると、スキャン速度が向上し、コンピューターに負荷が小さくなる反面、安全性が低くなります。
バッファリング時間を長く設定すると、ダウンロード時のスキャンの精度は向上します。その結果、安全性は高まりますが、ダウンロードしたデータにアクセス可能になるまで時間がかかることがあります。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［ウェブアンチウイルス］を選択します。**
3. **［セキュリティレベル］のバーを移動してレベルを選択します。**



選択できるレベルは次のとおりです。

- **高**
  最もセキュリティが高いレベルです。
  バッファリング時間が 60 秒、ヒューリスティック分析のレベルが［強］に設定されます。
  感染する危険性が高い環境で使用する場合におすすめします。
- **推奨**
  安全性と速度が最適化されたレベルです。
  バッファリング時間が 1 秒、ヒューリスティック分析のレベルが［中］に設定されます。
  一般的な環境で使用する場合におすすめします。

● **低**

最もセキュリティが低いですが、スキャン速度が最も速いレベルです。
スキャンの方法は推奨レベルと同じですが、ヒューリスティック分析のレベルが［弱］に設定されます。
保護されたネットワーク環境（社内ネットワークなど）では、このレベルで快適に操作できます。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **詳細な設定**

ウェブアンチウイルスのスキャン方法をより詳細に設定できます。HTTP スキャンの必要のない信頼できるサイトを登録したり、ドメインを元にアクセスを制限したりできます。

［設定］ウィンドウで［プロテクション］の［ウェブアンチウイルス］を選択し、［セキュリティレベル］で［設定］をクリックすると、［ウェブアンチウイルス］ウィンドウが表示されます。設定を変更すると、セキュリティレベルは「カスタム」と表示されます。初期値に戻すには［既定］をクリックします。

［ウェブアンチウイルス］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

お知らせ **設定ウィンドウで危険サイト診断を設定する**

［設定］ウィンドウの［ウェブアンチウイルス］で、危険サイト診断の設定もできます。
▶ P.66 危険なサイトへのリンクを診断

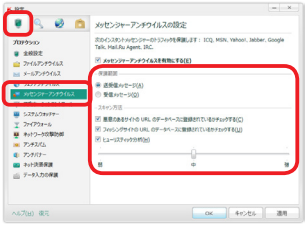
［設定］ウィンドウの［プロテクション］-［ウェブアンチウイルス］で、［設定］をクリックします。表示される［ウェブアンチウイルス］ウィンドウの［セーフサーフ］タブで設定します。

メッセンジャーアンチウイルス
（インスタントメッセージングからの感染を検知）

メッセンジャーアンチウイルスは、インスタントメッセージングの経路を使って送られてくるデータを監視して、ウイルスなど悪意のあるオブジェクトを検知したり、フィッシングサイトへのアクセスを未然に防いだりする機能です。

スキャン方法を設定する

1. メインウィンドウの［設定］をクリックします。
2. ［プロテクション］の［メッセンジャーアンチウイルス］を選択します。
3. ［保護範囲］で、スキャンの対象を選択します。
4. ［スキャン方法］で、スキャンの方法を選択します。



フィッシングサイトや疑わしいサイトのURL をスキャンするかどうかを選択します。
ヒューリスティック分析を行う場合は、バーをスライドしてレベルを指定します。

ヒューリスティック分析

定義データベースに登録されていない、未知のウイルスなどの脅威を検知する仕組みです。

5. ［OK］をクリックして、［設定］ウィンドウを終了します。

アプリケーションコントロール
（アプリケーションの動作を監視）

アプリケーションコントロールは、アプリケーションの動作を監視して、必要に応じて動作を制限する機能です。悪意のあるプログラムがシステムリソースや重要なファイルへ不正にアクセスするのを防ぎます。あらかじめアプリケーションごとに動作のルールを作成し、そのルールに従って監視します。ルールはアプリケーションの初回起動時に自動的に作成されますが、変更や追加もできます。
※アプリケーションコントロールは、カスペルスキー インターネット セキュリティのみの機能です。

アプリケーションのネットワークを経由したアクセスは、ファイアウォールで監視します。ネットワークによるアクセスを制限するには、ファイアウォールで設定してください。
▶ P.86 ファイアウォール

アプリケーションに設定されたステータスを確認・変更する

ルールは、アプリケーションステータスと呼ばれるグループに分けられます。アクセスの制限内容によってあらかじめ決められており、次の 4 つのグループがあります。

グループ	説明
許可	すべての動作を許可します。信頼されている製造元のデジタル署名があるか、Kaspersky Security Network のデータベースに登録されている場合、このカテゴリーに分類されます。
弱い制限付き	ユーザーが作成したファイルや、オペレーティングシステムやアプリケーションの設定情報へのアクセスを制限します。製造元のデジタル署名がなく、Kaspersky Security Network のデータベースにも登録されていないが、ヒューリスティック分析で危険性が低いと判定された場合、このカテゴリーに分類されます。
強い制限付き	ユーザーが作成したファイルや、オペレーティングシステムやアプリケーションの設定情報へのアクセスをブロックします。さらに、システムファイルやオペレーティングシステムが設定した情報などの、システムリソースへのアクセスを制限します。製造元のデジタル署名がなく、Kaspersky Security Network のデータベースにも登録されていない、さらにヒューリスティック分析で危険性が高いと判定された場合、このカテゴリーに分類されます。
ブロック	すべての動作をブロックします。製造元のデジタル署名がなく、Kaspersky Security Network のデータベースにも登録されていない、さらにヒューリスティック分析で非常に危険性が高いと判定された場合、このカテゴリーに分類されます。

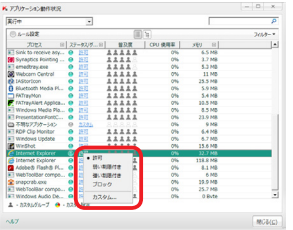
アプリケーションは初回起動時、自動的にこの 4 つのいずれかに分類されます。分類されたアプリケーションステータスは変更することもできます。
アプリケーションステータスの確認・変更は、［アプリケーション動作状況］で行えます。
※アプリケーション動作状況は、カスペルスキー インターネット セキュリティのみの機能です。

1. **メインウィンドウの［アプリケーション動作状況］をクリックします。**

［アプリケーション動作状況］ウィンドウが表示され、どのアプリケーションに何のステータスが設定されているか、確認できます。

2. **変更したいアプリケーションの［ステータス / グループ］の列をクリックします。**

3. **表示されるメニューから、変更したいステータスを選択します。**

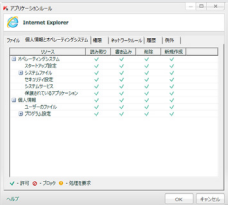


4. **［閉じる］をクリックして、［アプリケーション動作状況］ウィンドウを終了します。**

> アプリケーションステータスを変更すると、ステータスを変更するメニューに［既定］の項目が追加されます。［既定］を選択すると、自動的に設定された元のステータスに戻せます。

お知らせ　ルールを個別に設定する

アプリケーションごとにルールを個別に設定したい場合は、［アプリケーションルール］ウィンドウから設定します。

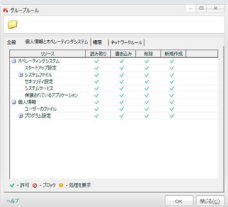


1. **［アプリケーション動作状況］ウィンドウで、変更したいアプリケーションを右クリックします。**
2. **表示されるメニューから［アプリケーションルール］を選択します。**
   ［アプリケーションルール］ウィンドウが表示されます。

［アプリケーションルール］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

お知らせ　ステータスグループの設定内容を変更する

4 つのステータスグループは、各制限内容を変更することもできます。変更は、［グループルール］ウィンドウで行います。

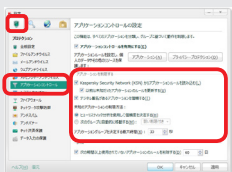


1. **［設定］ウィンドウで［プロテクション］-［アプリケーションコントロール］を選択します。**
2. **［アプリケーション］をクリックします。**
   ［アプリケーション］ウィンドウが表示されます。
3. **変更したいステータスグループを右クリックして表示されるメニューから［グループのルール］を選択します。**
   ［グループルール］ウィンドウが表示されます。

［グループルール］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

お知らせ　その他の設定

自動的に分類されるアプリケーションステータスは、どのような条件や結果を基に判断されているのか、その基準を設定できます。



1. **［設定］ウィンドウで［プロテクション］の［アプリケーションコントロール］を表示します。**
2. **［アプリケーションを制限する］の方法を選択します。**
3. **必要に応じて、次の項目を設定します。**
   - ［未知のアプリケーションの制限方法］
     デジタル署名がない、かつ Kaspersky Security Network のデータベースにも登録されていないアプリケーションの場合の判断方法を指定します。
   - ［アプリケーショングループを決定する最大時間］
     サイズの大きいアプリケーションの場合、初回起動時に行うステータスの分析に時間がかかってコンピューターに負荷をかける場合があります。それを防ぐために設定します。
   - ［次の期間以上使用されていないアプリケーションのルールを削除する］
     アンインストールしたアプリケーションなど、実体のないアプリケーションのルールを削除するために設定します。

各設定項目について、詳しくはヘルプを参照してください。

保護するデータを確認・変更する（プライバシープロテクション）

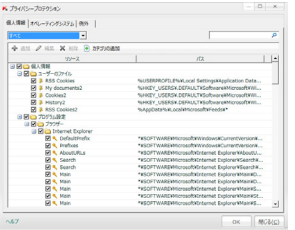
プライバシープロテクションは、アプリケーションコントロールでアクセスを監視する対象データを設定します。対象データは、追加したり変更したりすることもできます。

1. **メインウィンドウの［設定］をクリックします。**

2. **［プロテクション］の［アプリケーションコントロール］を選択します。**

3. **［プライバシープロテクション］をクリックします。**

   ［プライバシープロテクション］ウィンドウが表示され、保護されているデータが確認できます。



   - **［個人情報］タブ**
     アクセスを監視する対象データで、ユーザーが作成したファイルやアプリケーションに設定した情報などが表示されます。ウィンドウ左上のドロップダウンリストで、表示するカテゴリーを選択できます。
   - **［オペレーティングシステム］タブ**
     オペレーティングシステムのシステムファイルや起動に必要なファイルなどが表示されます。ウィンドウ左上のドロップダウンリストで、表示するカテゴリーを選択できます。
   - **［例外］タブ**
     アプリケーションコントロールの保護範囲から除外されたリソースが表示されます。

4. **データの保護を解除したい場合は、チェックボックスをオフにします。**
   保護したいデータを追加したい場合は、［追加］をクリックします。

   データの種類によって、設定内容が異なります。詳しくは、ヘルプを参照してください。

   ユーザーが追加した項目のみ、設定内容を変更したり、一覧から削除したりできます。

5. **［OK］をクリックして、［プライバシープロテクション］ウィンドウを終了します。**

6. **［OK］をクリックして、［設定］ウィンドウを終了します。**

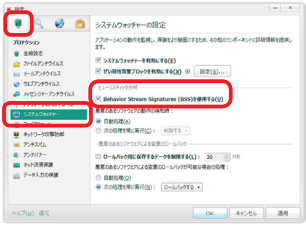
システムウォッチャー

（システムプロセスを監視）

システムウォッチャーは、システム内のアプリケーションの動作を監視し、データを収集・記録します。収集された情報は、他のプロテクション機能に提供され、未知の脅威の検知にいち早く対応します。もし、アプリケーションの不正な動作があった場合、記録に基づいて不正な動作を元に戻すこともできます。

検知時の処理方法を設定する

システムウォッチャーは、収集したデータに基づいて、BSS（Behavior Stream Signatures）と呼ばれる、アプリケーションの危険な動作パターンを分析する仕組みを使います。これによって検知された脅威をどう処理するか、設定します。



1. **メインウィンドウの［設定］をクリックします。**

2. **［プロテクション］の［システムウォッチャー］を選択します。**

3. **［ヒューリスティック分析］の［Behavior Stream Signatures (BSS) を使用する］をオンにします。**

4. **［悪意のあるソフトウェアの動作の検知時］で、処理方法を選択します。**

   ［脅威の処理方法］の設定で、自動処理がオンになっているかオフになっているかによって、選択できる項目が異なります。

   ▶ P.69 脅威の処理方法を変更する

   - **自動処理（脅威の処理方法の自動処理がオンの場合）**
     検知されると、そのオブジェクトを隔離フォルダーに移動し、アプリケーションの動作をロールバックし、状況に応じて通知ウィンドウで通知されます。
   - **手動選択（脅威の処理方法の自動処理がオフの場合）**
     検知されると、通知ウィンドウが表示されるので、処理を選択します。
   - **次の処理を常に実行**
     検知されると、通知ウィンドウを表示せず、ドロップダウンリストから選択した処理を実行します。

項目	説明
削除する	悪意のあるソフトウェアを削除します。
悪意のあるソフトウェアを終了する	悪意のあるソフトウェアのすべての処理を終了させます。
無視する	ソフトウェアに何の処理も行いません。

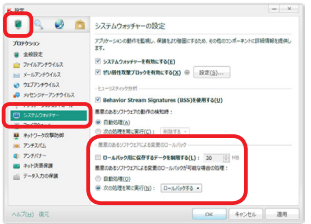
5. **［OK］をクリックして、［設定］ウィンドウを終了します。**

不正な動作を元に戻す設定をする

システムウォッチャーは、アプリケーション動作を記録します。もし悪意のあるプログラムによってファイルなどを変更された場合、その記録に基づいて、元の正常な状態へ戻すことができます。これをロールバックといいます。不正な動作があった場合、どのようにロールバックするかを設定できます。

1. **メインウィンドウの［設定］をクリックします。**

2. **［プロテクション］の［システムウォッチャー］を選択します。**



3. **［悪意のあるソフトウェアによる変更のロールバックが可能な場合の処理］で、処理方法を選択します。**

   ［脅威の処理方法］の設定で、自動処理がオンになっているかオフになっているかによって、選択できる項目が異なります。

   ▶ P.69 脅威の処理方法を変更する

   - **自動処理（脅威の処理方法の自動選択がオンの場合）**
     検知されると、ロールバックが必要かどうかを自動で判断して、実行されます。
   - **手動選択（脅威の処理方法の自動選択がオフの場合）**
     検知されると、通知ウィンドウが表示されるので、処理を選択します。
   - **次の処理を常に選択**
     検知されると、通知ウィンドウを表示せず、ロールバックをするかしないか、ドロップダウンリストから選択した処理を実行します。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

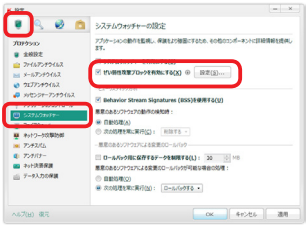
お知らせ　ロールバック用のデータを保存するメモリ容量を設定する

ロールバックのために記録したデータを保存できる、メモリの容量を設定することができます。［設定］ウィンドウの［プロテクション］-［システムウォッチャー］で、［ロールバック用に保存するデータを制限する］をオンにし、保存可能な容量を指定します。

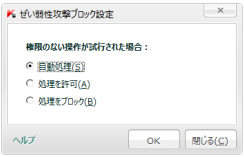
ぜい弱性への攻撃をブロックする

長期間アップデートされていないアプリケーションには、ぜい弱性が存在する可能性があります。ぜい弱性は、悪意のある第三者から遠隔でアプリケーションを操作されるなど、外部からの攻撃の標的となり得ます。
ぜい弱性攻撃ブロックは、ぜい弱性を持つアプリケーションのユーザー以外の操作での実行を検知すると、その動作をブロックできます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［システムウォッチャー］を選択します。**
3. **［ぜい弱性攻撃ブロックを有効にする］をオンにします。**
4. **［設定］をクリックします。**



5. **［ぜい弱性攻撃ブロック設定］ウィンドウで、ぜい弱性を持つアプリケーションの動作を検知した場合の処理方法を選択します。**



［脅威の処理方法］の設定で、自動処理がオンになっているかオフになっているかによって、選択できる項目が異なります。
▶ P.69 脅威の処理方法を変更する

- **自動処理（脅威の処理方法の自動選択がオンの場合）**
  検知されると、動作を自動で判断して、処理を実行します。
- **手動選択（脅威の処理方法の自動選択がオフの場合）**
  検知されると、通知ウィンドウが表示されるので、処理を選択します。
- **処理を許可**
  検知された動作をすべて許可します。
- **処理をブロック**
  検知された動作をすべてブロックします。

6. **［OK］をクリックして、［ぜい弱性攻撃ブロック設定］ウィンドウを終了します。**
7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

ファイアウォール
（ネットワークからのアクセスを監視）

ファイアウォールは、アプリケーションがネットワーク経由でシステムリソースや重要なファイルへアクセスするのを監視する機能です。パケットごとにアクセスするためのルールを作成し、そのルールに従って監視します。ルールは自動的に作成されますが、変更や追加することもできます。
※ファイアウォールは、カスペルスキー インターネット セキュリティのみの機能です。

ファイアウォールは、アプリケーションコントロールのサブセット機能として、ネットワーク経由のアクセス監視を行います。アプリケーションごとのアクセスを制限するには、アプリケーションコントロールから設定してください。
▶ P.79 アプリケーションコントロール

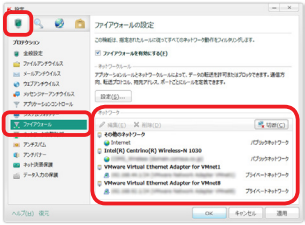
ネットワークに設定されたステータスを確認・変更する

ルールは、ネットワークステータスと呼ばれるグループに分けられます。アクセスの制限内容によってあらかじめ決められており、次の 3 つのグループがあります。

項目	説明
パブリックネットワーク	アクセスを制限し、一部ブロックします。 インターネットなど、不特定多数のユーザーが参加し、危険性の高いネットワークです。
プライベートネットワーク	一部のアクセスを制限します。 社内 LAN など、特定のユーザーのみが参加し、比較的安全が保たれているネットワークです。
許可するネットワーク	すべてのアクセスを許可します。 家庭内 LAN など、高い安全性が保たれているネットワークです。

ネットワークは自動的にこの 3 つのいずれかに分類されます。分類されたネットワークステータスは変更することもできます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［ファイアウォール］を選択します。**
   ［ネットワーク］に、現在接続しているネットワークが一覧に表示され、どのネットワークに何のステータスが設定されているか、確認できます。

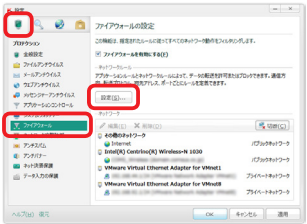


3. **変更したいネットワークを右クリックし、メニューから変更したいステータスを選択します。**
4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

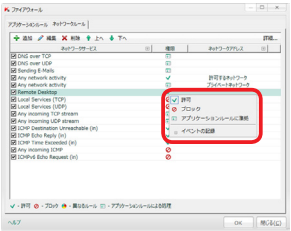
ネットワークルールを変更する

パケットごとにアクセス制限やネットワークステータスを指定して、ルールを設定します。アプリケーション共通のネットワークルールを設定する方法と、アプリケーション固有のネットワークルールを設定する方法があります。これらのルールを設定して、ネットワークからのアクセスを制御します。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［ファイアウォール］を選択します。**
3. **［ネットワークルール］の［設定］をクリックします。**



4. **［ファイアウォール］ウィンドウで、［ネットワークルール］タブをクリックします。**
   設定済みのネットワークルールがパケットの種類ごとに一覧で確認できます。
   ネットワークルールを適用しない場合は、チェックボックスをオフにします。
5. **変更したいパケットの［権限］の列を右クリックし、メニューから変更したいルールを選択します。**



6. **［OK］をクリックして、［ファイアウォール］ウィンドウを終了します。**
7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

ネットワークルールは、追加や内容の編集もできます。ウィンドウ上部の［追加］／［編集］をクリックすると、［ネットワークルール］ウィンドウが表示されます。
［ネットワークルール］ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

ネットワーク攻撃防御
（ネットワークからの攻撃をブロック）

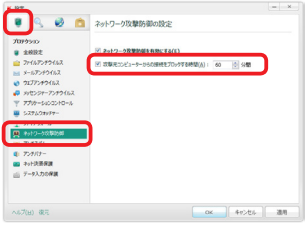
ネットワーク攻撃防御は、ネットワークに接続中のコンピューターが外部から攻撃された場合、攻撃元からのネットワーク接続を一定時間すべてブロックする機能です。また、攻撃を受けている旨の警告を表示し、攻撃元の情報を通知します。
想定されるネットワーク攻撃には、次のようなものがあげられます。
※ネットワーク攻撃防御は、カスペルスキー インターネット セキュリティのみの機能です。

- **ポートスキャン**
  ネットワークに接続しているコンピューターの、空いているポートを調べます。空きポートを確認すると、直接攻撃してきたり、他のコンピューターへ DoS や侵入などの攻撃を仕掛けるための踏み台にしたりします。
- **DoS**
  大量の無意味なパケットを送りつけてコンピューターに過度の負荷をかけたり、オペレーティングシステムを停止や再起動をさせるような不正なデータを送信したりしてコンピューターを攻撃し、システムを不安定あるいは動作不能にします。
- **侵入攻撃**
  ネットワークを経由して接続し、コンピューターを不正に操作します。コンピューターから個人情報や機密情報を盗み出したり、コンピューターを制御不能にしたりします。

攻撃元からの接続をブロックする時間を設定する

ネットワーク接続をブロックし、そのブロックを解除するまで待機する時間を設定します。待機している時間内に新たな攻撃を受けると、さらにそこから設定した時間がブロックされます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［ネットワーク攻撃防御］を選択します。**
3. **［攻撃元コンピューターからの接続をブロックする時間］に時間を指定します。**
4. **［OK］をクリックして、［設定］ウィンドウを終了します。**



お知らせ　ネットワークモニターで接続をブロックしている攻撃元を確認する

ネットワーク攻撃防御によってネットワーク接続がブロックされると、ネットワークモニターの［ネットワーク攻撃防御：ブロック中のネットワーク攻撃］で詳細が確認できます。
▶ P.100 ネットワーク攻撃防御：ブロック中のネットワーク攻撃

接続をブロックしている相手の IP アドレスと最後にブロックした時間が表示されます。
手動でブロックを解除することもできます。

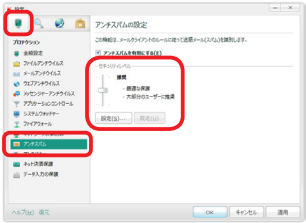
アンチスパム　（迷惑メールを識別）

広告などのダイレクトメールや、Web サイトへアクセスするよう勧誘するメールなど、不特定多数に無差別に送られるメールを、スパムまたは迷惑メールといいます。迷惑メールの中には、クリックさせることでコンピューター内部の情報を盗み出そうとする悪質なものもあります。
アンチスパムは、迷惑メールを自動で判別する機能です。迷惑メールと判定されたメールは、件名にメッセージを付加します。実際に届いた迷惑メールを覚えさせることで、迷惑メール検知の精度を向上させることもできます。
※アンチスパムは、カスペルスキー インターネット セキュリティのみの機能です。

セキュリティレベルを設定する

セキュリティレベルとは、迷惑メール判定の適合率や使用するアルゴリズムなどを組み合わせて、あらかじめ定義したものです。セキュリティレベルを選択することで、判定の度合いを変更できます。
初期設定では、［推奨］に設定されています。使用する環境にあわせて変更できます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［プロテクション］の［アンチスパム］を選択します。**
3. **［セキュリティレベル］のバーを移動してレベルを選択します。**



選択できるレベルは次のとおりです。

- **高**
  迷惑メールと判定されるメールの割合が多くなります。
  迷惑メールを多く受け取る場合に適しています。
- **推奨**
  迷惑メールを判定する基準が最適化されたレベルです。
  多くの場合、このレベルを選択します。
- **低**
  迷惑メールと判定されるメールの割合が少なくなります。会社内のメールシステムなど、安全な環境で迷惑メールをほとんど受け取らない場合に適しています。

4. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ **詳細な設定**

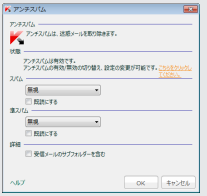
迷惑メールの判定方法をより詳細に設定できます。

[設定] ウィンドウで [プロテクション] の [アンチスパム] を選択し、[セキュリティレベル] で [設定] をクリックすると、[アンチスパム] ウィンドウが表示されます。設定を変更すると、セキュリティレベルは「カスタム」と表示されます。初期値に戻すには [既定] をクリックします。

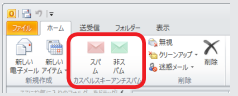
[アンチスパム] ウィンドウの各設定項目について、詳しくはヘルプを参照してください。

お知らせ **迷惑メールの処理方法を設定する・メールを指定して学習させる**
－アンチスパム対応メールソフトをお使いの場合－

カスペルスキーをインストール後、Microsoft Office Outlook や Windows メール、Microsoft Outlook Express を起動すると、アンチスパム学習の設定ウィンドウが開きます。「スパム」「準スパム」について、それぞれ特定のフォルダーに移動したり、コピーや削除をしたりするなどの対処方法を設定できます。



また、Microsoft Office Outlook や Windows メール、Microsoft Outlook Express には [スパム] [非スパム] のアイコンが追加されています。メールを選択して、それぞれのアイコンをクリックすることで、学習させていくことができます。



アンチバナー　（バナー広告を非表示）

アンチバナーは、ブラウザーで Web サイトを閲覧中に表示されるポップアップ広告や、アプリケーションのメニュー部分などに勝手に追加されるバナー広告をスキャンして、表示をブロックする機能です。ユーザーが表示を許可／ブロックしたいサイトを登録することもできます。
アンチバナー機能は初期設定では無効になっていますので、使用する場合は、機能を有効にしてから設定を行ってください。

▶ P.68 プロテクションの有効・無効を切り替える

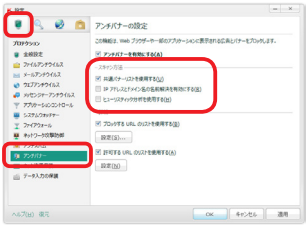
※アンチバナーは、カスペルスキー インターネット セキュリティのみの機能です。

スキャン方法を設定する

アンチバナーのスキャンの方法を設定します。

1. メインウィンドウの［設定］をクリックします。

2. ［プロテクション］の［アンチバナー］を選択します。



3. ［スキャン方法］で、次の選択肢から、使用するスキャン方法をオンにします。

- **共通バナーリストを使用する**
  定義データベースに登録されている共通のバナーリストを元にスキャンします。
- **IP アドレスとドメイン名の名前解決を有効にする**
  ［ブロックする URL］／［許可する URL］に IP アドレスで登録されていた場合、名前解決してスキャンします。
- **ヒューリスティック分析を使用する**
  ヒューリスティック分析を元にスキャンします。

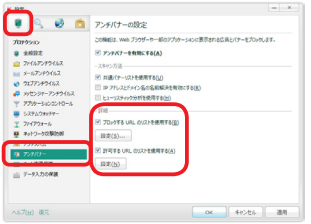
> **ヒューリスティック分析**
> 定義データベースに登録されていない、未知のウイルスなどの脅威を検知する仕組みです。

4. ［OK］をクリックして、［設定］ウィンドウを終了します。

ブロックまたは許可するサイトを登録する

バナー広告を非表示にしたいまたは表示したいサイトを登録します。

1. メインウィンドウの［設定］をクリックします。
2. ［プロテクション］の［アンチバナー］を選択します。
3. ［詳細］で［ブロックする URL のリストを使用する］／［許可する URL のリストを使用する］をオンにします。
4. それぞれの［設定］をクリックします。



5. ［ブロック／許可する URL］ウィンドウで、［追加］をクリックします。

6. ［URL マスクの編集］ウィンドウで、ブロックまたは許可したい URL を入力して、［OK］をクリックします。

   URL リストに指定した URL が登録されます。

7. ［OK］をクリックして、［ブロック／許可する URL］ウィンドウが終了します。
8. ［OK］をクリックして、［設定］ウィンドウを終了します。

ブロック／許可する URL は、テキストファイルに保存したり、読み込んだりできます。［ブロック／許可する URL］ウィンドウで、［インポート］または［エクスポート］をクリックします。

検知する対象の設定

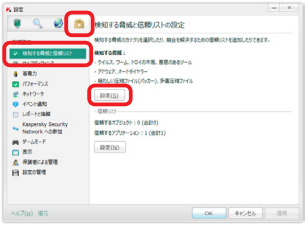
コンピューターにとって脅威となる危険なプログラムには、さまざまな種類があります。カスペルスキーでは、検知する脅威を選択できます。初期設定のままでも十分な保護が可能ですが、必要に応じて詳細な設定ができます。

検知する脅威を設定する

1. **メインウィンドウの［設定］をクリックします。**

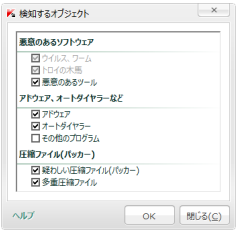
2. **［詳細設定］の［検知する脅威と信頼リスト］を選択します。**

3. **［検知する脅威］の［設定］をクリックします。**



4. **［検知するオブジェクト］ウィンドウで、検知対象に含める脅威の種類をオンにします。**

   脅威の種類は次のとおりです。



   - **悪意のあるソフトウェア**
     脅威となる、最も典型的なプログラムです。データの破壊や漏えい、脅威の進入路（バックドア）の作成などを目的とし、中には自己増殖可能なプログラムも含みます。これらを監視することで、最低限のセキュリティレベルを提供します。
   - **アドウェア、オートダイヤラーなど**
     危険なふるまいの発生源となるプログラムです。ユーザーの望まない広告を表示したり、通話料金が高額なサービスに自動的に電話したりするような、潜在的に危険なプログラムを含みます。
   - **圧縮ファイル（パッカー）**
     自動的に解凍するプログラムが含まれていたり、検知を難しくするために二重にも三重にも圧縮処理が行われていたりするファイルです。

5. **［OK］をクリックして、［検知するオブジェクト］ウィンドウを終了します。**

6. **［OK］をクリックして、［設定］ウィンドウを終了します。**

信頼する対象の設定

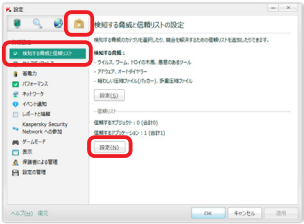
信頼リストは、スキャンの対象に含めないオブジェクトやアプリケーションのリストです。信頼リストには、ファイルなどのオブジェクトを登録する「信頼するオブジェクト」と、アプリケーション単位で登録する「信頼するアプリケーション」があります。

信頼するオブジェクトを追加する

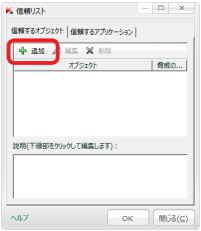
1. **メインウィンドウの［設定］をクリックします。**

2. **［詳細設定］の［検知する脅威と信頼リスト］を選択します。**

3. **［信頼リスト］の［設定］をクリックします。**



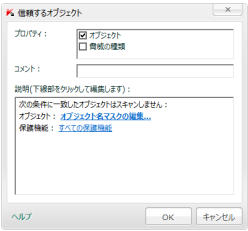
4. **［信頼リスト］ウィンドウの［信頼するオブジェクト］タブで、［追加］をクリックします。**



5. **［信頼するオブジェクト］ウィンドウの［プロパティ］で、信頼するオブジェクトの指定方法をオンにします。**

   ［オブジェクト］は、コンピューター内のファイルやフォルダーを選択できます。
   ［脅威の種類］は、ウイルス百科事典にのっている脅威の種類名で指定できます。

6. **必要に応じて、［コメント］に信頼するオブジェクトの説明を入力します。**



7. **［説明］でリンクをクリックして、信頼する対象を指定します。**

   ［オブジェクト］または［脅威の種類］では、信頼するオブジェクトを指定します。
   保護機能では、審理するオブジェクトに対して実行しない機能を選択します。

8. **［OK］をクリックして、［信頼するオブジェクト］ウィンドウを終了します。**

   ［信頼リスト］ウィンドウの［信頼するオブジェクト］タブの一覧に、設定したオブジェクトが追加されます。
   続けて信頼するオブジェクトを登録する場合は、手順 4 に戻ります。

9. 信頼するオブジェクトがオンになっていることを確認し、[OK] をクリックして、[信頼リスト] ウィンドウを終了します。

10. [OK] をクリックして、[設定] ウィンドウを終了します。

お知らせ **ウイルスとして検知されたオブジェクトを信頼リストに追加する**

検知されたオブジェクトに危険がないとわかっている場合は、まず通知ウィンドウで [無視] を選択します。そのあと [セキュリティの問題] 画面で、[▼] をクリックして表示されるメニューから [信頼するオブジェクトに追加] を選択すると、信頼リストに設定できます。

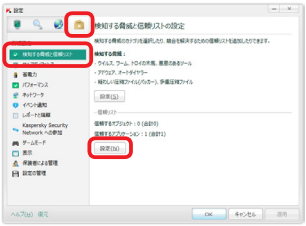
▶ P.51 選択できる処理

信頼するアプリケーションを追加する

1. メインウィンドウの [設定] をクリックします。

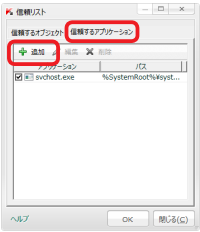
2. [詳細設定] の [検知する脅威と信頼リスト] を選択します。

3. [信頼リスト] の [設定] をクリックします。



4. [信頼リスト] ウィンドウの [信頼するアプリケーション] タブをクリックします。

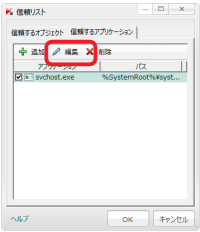
5. [追加] をクリックして表示されるメニューで、次のどちらかの方法でアプリケーションを指定します。



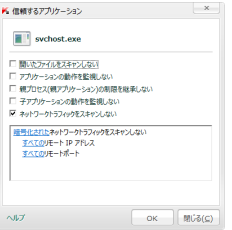
- **[アプリケーション]**
  [アプリケーションの選択] ウィンドウが表示され、一覧からアプリケーションを選択し、[OK] をクリックします。
- **[参照]**
  [ファイルを開く] ウィンドウが表示され、アプリケーションの実行ファイルを指定し、[開く] をクリックします。

アプリケーションを指定し終えると、[信頼アプリケーション] タブの一覧に追加されます。

6. 追加されたアプリケーションを選択して、[編集] をクリックします。



7. ［信頼するアプリケーション］ウィンドウで、実行しない機能を選択します。



- **開いたファイルをスキャンしない**
  指定したアプリケーションが開いているファイルを、スキャン対象から除外します。
- **アプリケーションの動作を監視しない／子アプリケーションの動作を監視しない**
  指定したアプリケーション、またはそれが呼び出すアプリケーション（子アプリケーション）の活動や疑わしい動作などを、アプリケーションコントロールの監視対象から除外します。
  ▶ P.79 アプリケーションコントロール
- **親プロセス（親アプリケーション）の制限を継承しない**
  通常、子アプリケーションは親アプリケーションに設定された制限を継承します。親アプリケーションに設定されている同じ制限を適用せず、独自に設定した制限を適用します。
- **ネットワークトラフィックをスキャンしない**
  指定したアプリケーションのネットワークトラフィックに含まれるウイルスやスパムを、スキャン対象から除外します。オンにすると表示されるリンクをクリックして、指定のポートやホストに対して除外制限を設定することもできます。

［ネットワークトラフィックをスキャンしない］をオンにしても、ファイアウォールがネットワーク動作をブロックするかどうかには影響しません。

8. ［OK］をクリックして、［信頼するアプリケーション］ウィンドウを終了します。

［信頼リスト］ウィンドウの［信頼するアプリケーション］タブの一覧に、設定したアプリケーションが追加されます。
続けて信頼するアプリケーションを登録する場合は、手順 5 に戻ります。

9. 信頼するアプリケーションがオンになっていることを確認し、［OK］をクリックして、［信頼リスト］ウィンドウを終了します。

10. ［OK］をクリックして、［設定］ウィンドウを終了します。

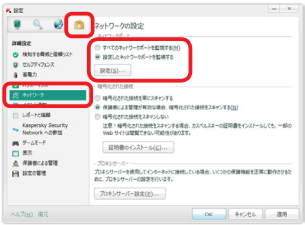
ネットワークに関する機能の設定

カスペルスキーには、暗号化された接続のスキャンや特定のポートを監視する機能があります。初期設定では無効になっていますので、機能を有効にして使用します。
また、お使いの環境にプロキシサーバーがある場合は、その設定も必要です。

監視するネットワークポートを設定する

メールアンチウイルスやウェブアンチウイルスは、SMTP や HTTP などのプロトコルを利用してデータの送受信が行われるネットワークポートを監視します。カスペルスキーでは、初期設定でメールや HTTP などで通常利用されるネットワークポートが登録されています。監視するネットワークポートを追加したり、変更したりすることもできます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［ネットワーク］を選択します。**
3. **［ネットワークポート］で、［すべてのネットワークポートを監視する］または［設定したネットワークポートを監視する］のどちらかを選択します。**

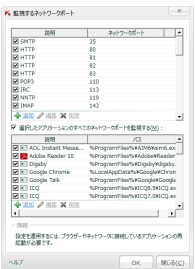


● ［すべてのネットワークポートを監視する］を選択した場合

4. **［OK］をクリックして［設定］ウィンドウを終了します。**

● ［設定したネットワークポートを監視する］を選択した場合

4. **［設定］をクリックします。**
5. **［監視するネットワークポート］ウィンドウの上段のリストから、監視したいポートをオンにします。**
   リストにない場合は、［追加］をクリックしてポートを追加できます。



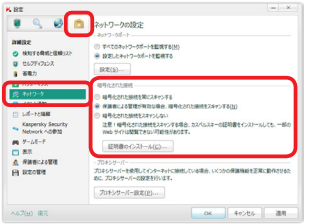
6. **アプリケーションごとにポートの監視を行いたい場合は、［選択したアプリケーションのすべてのネットワークポートを監視する］をオンにし、下段のリストから監視したいアプリケーションをオンにします。**
   リストにない場合は、［追加］をクリックしてアプリケーションを追加できます。
7. **［OK］をクリックして、［監視するネットワークポート］ウィンドウを終了します。**
8. **［OK］をクリックして、［設定］ウィンドウを終了します。**

暗号化された接続のスキャンを有効にする

インターネットで安全にデータをやりとりするために、SSL プロトコルを使用して暗号化された接続方法が使用される場合があります。SSL 通信は電子証明書を使って通信相手を確認し、データを暗号化し、安全性を保証します。しかし、SSL 通信を利用するウイルスも存在します。
SSL 通信のスキャンを実行するにはこの機能を有効化して、証明書をインストールする必要があります。

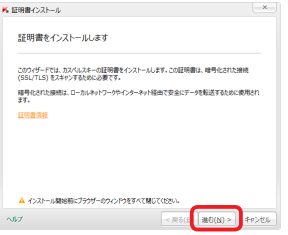
以下の手順は、Microsoft Internet Explorer と Google Chrome の場合です。

1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［ネットワーク］を選択します。**
3. **［暗号化された接続］の［暗号化された接続を常にスキャンする］または［保護者による管理が有効な場合、暗号化がされた接続をスキャンする］をオンにします。**
4. **［証明書のインストール］をクリックします。**



5. **［証明書インストール］ウィンドウで、［進む］をクリックします。**
   証明書がインストールされます。

   インストールが実行されると、［セキュリティ警告］画面が表示される場合があります。表示されたら、［はい］をクリックします。



6. **インストールが終了したら、［終了］をクリックします。**
7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

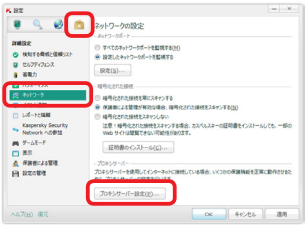
ご注意　Web サイトへの接続に失敗する場合

暗号化された接続をスキャンするために、要求されたセキュリティ証明書を代理の証明書に取り替えます。場合によっては、代理の証明書では認証を受けられず、Web サイトに接続できないこともあります。その場合、信頼できる Web サイトに限り、［暗号化された接続をスキャンしない］に設定してください。

プロキシサーバーを設定する

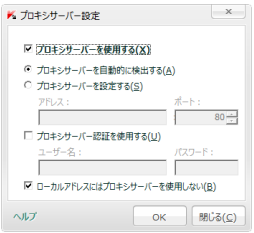
LAN 内でプロキシサーバーを使用している場合、プロキシサーバーをあらかじめ登録しておく必要があります。

1. メインウィンドウの［設定］をクリックします。
2. ［詳細設定］の［ネットワーク］を選択します。
3. ［プロキシサーバー］の［プロキシサーバー設定］をクリックします。



4. ［プロキシサーバーを使用する］をオンにして、［プロキシサーバーを自動で検出する］または［プロキシサーバーを設定する］のどちらかを選択します。

   ［プロキシサーバーを設定する］を選択した場合は、プロキシサーバーの情報を入力します。不明な場合は、ネットワーク管理者に確認してください。



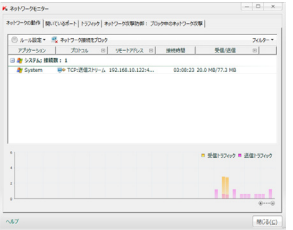
5. ［OK］をクリックして、［プロキシサーバー設定］ウィンドウを終了します。
6. ［OK］をクリックして、［設定］ウィンドウを終了します。

ネットワークの接続状況を確認する（ネットワークモニター）

ネットワークに接続しているアプリケーションやサービスごとのプロトコルやポート、接続時間やデータ量などがリアルタイムで確認できます。ネットワーク攻撃防御機能によってブロックされているネットワーク接続なども確認できます。
※ネットワークモニターは、カスペルスキー インターネット セキュリティのみの機能です。

1. メインウィンドウの［ネットワークモニター］をクリックします。

［ネットワークモニター］ウィンドウが表示され、ネットワークの状態が表示されます。



ネットワークモニターには次の 4 つのタブがあります。目的によって切り替えて使用します。

● **ネットワークの動作**
ネットワークに接続しているアプリケーションやサービスごとに、プロトコルや接続先の IP アドレス、接続時間、送受信データの量などの情報を、リアルタイムで表示します。
［ネットワーク接続をブロック］をクリックすると、強制的にネットワークをブロックすることができます。

● **開いているポート**
ネットワークに接続しているアプリケーションやサービスのポートごとに、IP アドレスやプロトコル、接続時間などの情報を、リアルタイムで表示します。

● **トラフィック**
ネットワークに接続しているアプリケーションやサービスごとに、受信／送信トラフィックの集計データを、期間を指定して表示します。

● **ネットワーク攻撃防御：ブロック中のネットワーク攻撃**
ネットワーク攻撃防御機能によるブロックが起きると、ブロックしている相手の IP アドレスとブロックしている時間が表示されます。ブロックを解除することもできます。
▶ P.88 ネットワークモニターで接続をブロックしている攻撃元を確認する

パフォーマンスに関する機能の設定

コンピューターの使用状況や環境によって、カスペルスキーの動作を一時的に変えて、他のアプリケーションの動作を優先させたりできます。

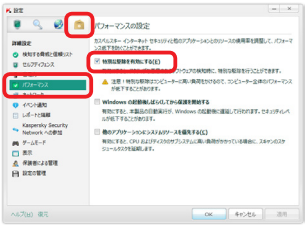
特別な駆除機能を有効にする

特別な駆除を実行するように設定します。特別な駆除機能は、アクティブな悪意のあるソフトウェアを検知すると、駆除を試みます。

ご注意

特別な駆除の実行時はコンピューターに高い負荷がかかるので、コンピューターのパフォーマンスが低下することがあります。また、駆除後はコンピューターの再起動が必要です。

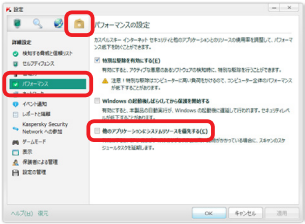
1. メインウィンドウの［設定］をクリックします。
2. ［詳細設定］の［パフォーマンス］を選択します。
3. ［特別な駆除を有効にする］をオンにします。
4. ［OK］をクリックして、［設定］ウィンドウを終了します。



スキャンやアップデートを自動的に延期する

他のアプリケーションによりシステムリソースが大量に使用されている場合、スキャンを延期します。システムリソースに空きができたときに、延期していたスキャンが実行されます。

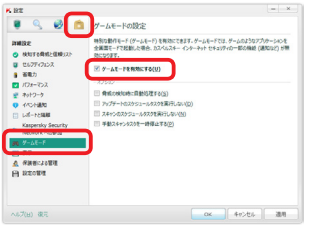
1. メインウィンドウの［設定］をクリックします。
2. ［詳細設定］の［パフォーマンス］を選択します。
3. ［他のアプリケーションにシステムリソースを優先する］をオンにします。
4. ［OK］をクリックして、［設定］ウィンドウを終了します。



全画面使用時に設定を自動的に切り替える（ゲームモード）

ゲームモードは、ゲームなどのアプリケーションが全画面に表示になったとき、脅威の処理方法を自動処理に切り替えたり、アップデートやスキャンを実行しないようにしたりする機能です。通知ウィンドウを表示したり、スキャンが自動実行してコンピューターに負荷をかけたりといった、ゲームの最中には実行して欲しくない機能を、一時的に実行しないようにできます。

1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［ゲームモード］を選択します。**
3. **［ゲームモードを有効にする］をオンにします。**
4. **［オプション］で次の項目をオンにします。**



- **脅威の検知時に自動処理する**
  脅威が検知されると通知ウィンドウを表示せず、自動で処理されます。
- **アップデートのスケジュールタスクを実行しない**
  設定した日時になってもアップデートを実行しません。
- **スキャンのスケジュールタスクを実行しない**
  設定した日時になってもスキャンを実行しません。
- **手動スキャンタスクを一時停止する**
  手動で開始されたスキャンが実行中の場合、スキャンを一時停止します。

5. **［OK］をクリックして、［設定］ウィンドウを終了します。**

お知らせ　ノート PC でバッテリー使用時にスキャンやアップデートを延期する

ノート PC をバッテリーで使用中だった場合、スケジュールされたアップデートやスキャンを行わない設定ができます。
［設定］ウィンドウで［詳細設定］の［省電力］を選択し、［バッテリー使用中はスケジュールタスクをスキップする］をオンにします。

お知らせ　スキャンの負荷を分散する

コンピューターへの負荷を分散させるため、自動アップデートと定期スキャンをコンピューターがロックされている間や、スクリーンセーバーが起動している間など、コンピューターがアイドリング状態のときに実行させるよう設定できます。
［設定］ウィンドウで［スキャン］の［全般設定］を選択し、［低負荷スキャン設定を有効にする］をオンにします。
ただし、ノート PC でバッテリーを使用している場合は、アイドリング状態であってもアップデートやスキャンは実行されません。
また、［ルートキットスキャンを定期的に実行する］をオンにすると、定期的なルートキットスキャンをバックグラウンドで実行させることもできます。

お知らせ　スキャンを一時停止する（ファイルアンチウイルス）

決まった時間帯やあるアプリケーションが起動したときには、ファイルアンチウイルスのスキャン機能を一時的に停止することができます。
［設定］ウィンドウで［プロテクション］の［ファイルアンチウイルス］を選択し、［セキュリティレベル］で［設定］をクリックすると、［ファイルアンチウイルス］ウィンドウが表示されます。［詳細］タブの［ファイルアンチウイルスの一時停止］で設定します。設定方法について、詳しくはヘルプを参照してください。

設定のエクスポート・インポートと初期化

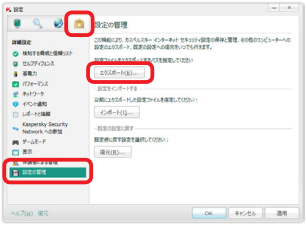
カスペルスキーで設定した内容は、エクスポートしてファイルに保存したり、保存したファイルをインポートしたりできます。複数のコンピューターで同じ設定を利用したい場合などに役立ちます。

設定をエクスポートする

設定内容をファイルに保存します。

1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［設定の管理］を選択します。**
3. **［エクスポート］をクリックします。**
4. **［設定ファイルの指定］ウィンドウで、保存するフォルダーとファイル名を指定して、［保存］をクリックします。**

   拡張子は「*.cfg」です。
5. **［OK］をクリックして、［設定］ウィンドウを終了します。**

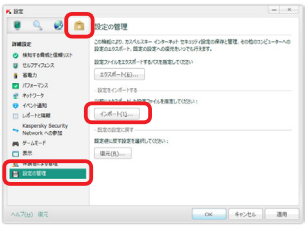


設定をインポートする

エクスポートした設定ファイルを読み込みます。別のコンピューターからエクスポートした設定ファイルを読み込むことも可能です。

1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［設定の管理］を選択します。**
3. **［インポート］をクリックします。**
4. **［設定ファイルの指定］ウィンドウで、読み込むファイル（*.cfg）を指定して、［開く］をクリックします。**

   設定内容が反映されます。
5. **［OK］をクリックして、［設定］ウィンドウを終了します。**



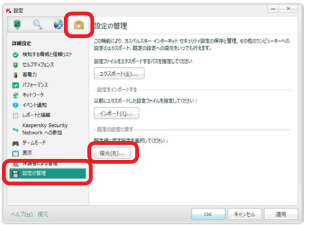
設定を初期化する

カスペルスキーの設定をリセットして初期状態に戻します。特定の機能だけを初期化することもできます。

ご注意　初期化しない方がよい項目

アプリケーションコントロールとファイアウォールの各ルールは、プログラムを使用していると増加していきます。これらのルールの設定には時間がかかるため、これらの設定は初期化せずに残しておくことをおすすめします。

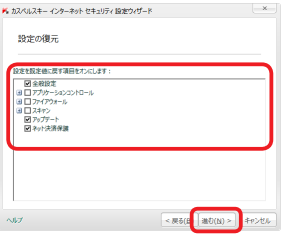
1. **メインウィンドウの［設定］をクリックします。**
2. **［詳細設定］の［設定の管理］を選択します。**
3. **［復元］をクリックします。**



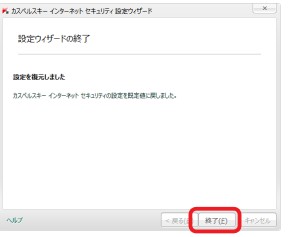
4. **［設定ウィザード］で、［進む］をクリックします。**

5. **［設定の復元］画面で、設定を初期値に戻したい項目をオンにして、［進む］をクリックします。**

   セキュリティ診断が行われ、完了すると［設定ウィザードの終了］画面が表示されます。



6. **［設定ウィザードの終了］画面が表示されたら、［終了］をクリックします。**



7. **［OK］をクリックして、［設定］ウィンドウを終了します。**

便利ツールの活用

カスペルスキーには各プロテクション機能のほかに、コンピューターを安全に保つための便利なツールがあります。
メインウィンドウの［便利ツール］をクリックすると、各ツールが起動できます。
各ツールの詳細な使用方法については、各ヘルプも参照してください。

起動できなくなったシステムの感染を検知・駆除する（レスキューディスク）

システムが起動できなくなった場合、修復するためのレスキューディスクを作成できます。

ご注意　レスキューディスクはサポート対象外です

レスキューディスクは、ウイルスなどの感染が原因で起動不可能になったシステムに対して使用します。レスキューディスクよりシステムを起動し、スキャンや駆除が可能です。
何らかの不具合が発生し起動できないシステムを、必ず復旧することを保証するものではありません。

1. メインウィンドウの［便利ツール］画面で、［レスキューディスク］の［作成］をクリックします。

すでに ISO イメージファイルを作成していた場合、［既存の Kaspersky Rescue Disk 用 ISO イメージファイルが見つかりました。］と表示されます。既存の ISO イメージファイルを使用する場合は、［既存の Kaspersky Rescue Disk のイメージファイルを使用する］をオンにして、手順 5 に進みます。

2. ［Kaspersky Rescue Disk 作成ウィザード］が表示されたら、［進む］をクリックします。

3. **［ステップ 1. ISO イメージファイルの選択］画面で、ISO イメージファイルを選択します。**

- **CD/DVD ディスクまたはネットワークドライブから ISO イメージファイルをコピーする**
  作成済みの ISO イメージファイルがある場合、選択して指定します。
- **Kaspersky Lab のサーバーから ISO イメージファイルをダウンロードする**
  はじめて作成する場合に選択します。

4. **［進む］をクリックします。**
   コピーまたはダウンロードが開始されます。

5. **［ステップ 3. ISO イメージファイルの更新］画面が表示されたら、［進む］をクリックします。**
   定義データベースと設定ファイルの更新が開始されます。更新には数分かかる場合があります。

6. **［ステップ 4. ディスクへのデータの記録］画面が表示されたら、イメージファイルの保存先を指定します。**

- **CD/DVD へ書き込む**
  書き込み可能な CD/DVD に書き込みます。光学メディアを CD/DVD ドライブへ挿入します。
- **USB フラッシュドライブへ書き込む**
  USB 接続のリムーバブルドライブに書き込みます。
  USB リムーバブルドライブをコンピューターに接続します。
- **イメージファイルをローカルディスクまたはネットワークドライブへ保存する**
  コンピューター内のフォルダー、またはネットワーク共有フォルダーへ保存します。

7. **［進む］をクリックします。**

8. **イメージファイルを保存する場所を指定して、［進む］をクリックします。**
   イメージが書き込まれます。

9. **［Kaspersky Rescue Disk 作成ウィザードの完了］画面が表示されたら、［終了］をクリックして、［Kaspersky Rescue Disk 作成ウィザード］を終了します。**

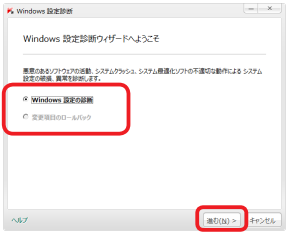
Windows の設定を検査する（Windows 設定診断）

Windows 設定診断は、Windows の設定状況をウィザード形式で診断します。ウイルスの感染によって引き起こされた、設定の誤りやぜい弱性を見つけ出し、問題が発見された場合は、正しい設定に修正します。

1. **メインウィンドウの［便利ツール］画面で、［Windows 設定診断］の［開始］をクリックします。**

2. **［Windows 設定診断ウィザード］が表示されたら、［Windows 設定の診断］を選択して［進む］をクリックします。**

   診断が開始されます。



3. **［問題点の検索の完了］画面が表示され、一覧に問題点が表示されていたら、修正したい項目をオンにします。**

   問題が発見されなかった場合は、「問題点は検出されませんでした。」と表示されます。

4. **［進む］をクリックします。**

   問題が修正されます。

5. **［Windows 設定診断ウィザードの完了］画面が表示されたら、［終了］をクリックして Windows 設定診断を終了します。**

ユーザーの操作履歴を消去する（プライバシークリーナー）

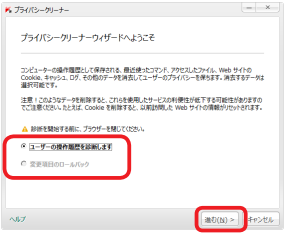
プライバシークリーナーは、コンピューターに残るさまざまな操作履歴をウィザード形式で検索し、削除します。操作履歴から、個人情報が漏えいするのを防ぎます。
検索・削除の対象となるのは、次のとおりです。

- Web ページの閲覧履歴
- アプリケーションの起動履歴
- アプリケーションが開いたファイル履歴
- 検索履歴
- Windows のログ
- 一時ファイル（テンポラリーファイル）

1. メインウィンドウの［便利ツール］画面で、［プライバシークリーナー］の［開始］をクリックします。

2. ［プライバシークリーナーウィザード］が表示されたら、［ユーザーの操作履歴を診断します］を選択して［進む］をクリックします。

診断が開始されます。

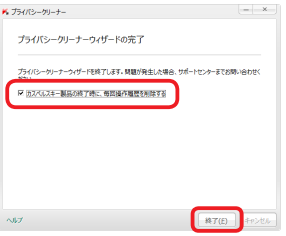


3. ［操作履歴の検索の完了］画面が表示されたら、削除したい項目をオンにして［進む］をクリックします。

削除が実行されます。

4. 削除が終了すると、［プライバシークリーナーウィザードの完了］画面が表示されます。必要に応じて、［カスペルスキー製品の終了時に、毎回操作履歴を削除する］をオンにします。

オンにすると、操作履歴の削除が自動的に行われます。



5. ［終了］をクリックして、プライバシークリーナーを終了します。

Internet Explorer の設定を検査する（Internet Explorer 設定診断）

Internet Explorer 設定診断は、ウィザード形式で Microsoft Internet Explorer の設定状況を診断します。ウイルス感染やシステム障害、アプリケーションの動作不良などを引き起こす恐れのある要因を見つけ出し、問題が発見された場合は、より安全な設定に修正します。

Internet Explorer 設定診断が対応するブラウザーのバージョンは、Microsoft Internet Explorer 9 / 8 / 7 / 6 です。

1. **メインウィンドウの［便利ツール］画面で、［Internet Explorer 設定診断］の［開始］をクリックします。**

2. **［Internet Explorer 設定診断ウィザード］が表示されたら、［Internet Explorer 設定の診断の実行］を選択して［進む］をクリックします。**
   診断が開始されます。

3. **［問題点の検索の完了］画面が表示され、一覧に問題点が表示されていたら、修正したい項目をオンにします。**
   問題が発見されなかった場合は、「問題点は検出されませんでした。」と表示されます。

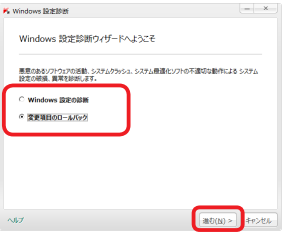
4. **［進む］をクリックします。**
   問題が修正されます。
   修正が完了すると、と表示されます。

5. **［Internet Explorer 設定の修正が完了しました。］画面が表示されたら、［終了］をクリックして Internet Explorer 設定診断を終了します。**

変更・削除した内容を元に戻す

Windows 設定診断／プライバシークリーナー／ Internet Explorer 設定診断で削除または変更した項目は、元に戻すことができます。（中には元に戻せない項目もあります。）

1. **各ウィザードの開始画面で、［変更項目のロールバック］をオンにし、［進む］をクリックします。**



2. **前回修正した問題点が表示されるので、元に戻したい項目をオンにし、［進む］をクリックします。**

   元に戻す処理が行われます。

3. **完了画面が表示されたら、［終了］をクリックして、ウィザードを終了します。**

トラブルシューティング

カスペルスキーのインストール中に、共存できないソフトウェアが見つかった

➡ カスペルスキーは、他のセキュリティソフトと同時にお使いいただくことはできません。現在他のセキュリティソフトがインストールされている場合は、カスペルスキーをインストールする前にアンインストールしてください。カスペルスキーのインストール操作中に、他のセキュリティソフトをアンインストールすることもできます。

削除ツールを使用する

セキュリティソフトを完全にアンインストールするための削除ツールを、メーカーサイトから入手できる場合があります。削除ツールを使ってアンインストールすることをおすすめします。

アクティベーションが実行できない

➡ アクティベーションを実行するためには、コンピューターがインターネットに接続している必要があります。ブラウザーを起動してインターネットに接続可能であることを確認してから、アクティベーションを実行してください。

2台目、3台目で使う方法がわからない

➡ ライセンスの種類によっては、1つのアクティベーションコードで複数台のコンピューターにカスペルスキーをインストールできます。1台目のコンピューターでアクティベーションを行ったあと、残りの台数のコンピューターにカスペルスキーをインストールし、1台目と同じアクティベーションコードを使ってアクティベーションを実行してください。

ライセンス更新のメッセージが表示された

➡ ライセンスの有効期限が切れる前後に、ライセンスの更新を促すメッセージが表示されます。有効期限を延長するためには、[ライセンス管理] ウィンドウから、新しいライセンスをご購入いただき、新しいアクティベーションコードでアクティベーションを実行してください。

▶ P.20 ライセンス
▶ P.21 アクティベーション

用語解説

アクティベーション
ライセンスを認証し、プログラムを有効（動作可能）にすること。

アドウェア
ユーザーが希望していない広告を勝手に表示するプログラム。

オブジェクト
ファイルやフォルダーなど、スキャンや検知の対象となるものの総称。

隔離
ウイルスの感染が疑われるオブジェクトを、専用のフォルダーに安全な形に変換して格納すること。

スキャン
ファイルを検査することにより、侵入したウイルスなどの脅威を検知すること。

スパイウェア
コンピューターに侵入し、ユーザーの操作を記録したり、情報を盗んだりするプログラム。

スパム
不特定多数に向けたダイレクトメールなどの迷惑メール。

ぜい弱性
コンピューターへの侵入やウイルス感染などを引き起こす、セキュリティ上の弱点。プログラムの欠陥（バグ）、仕様上の問題点、特定の運用方法や設定などが原因となる。メーカー提供の修正プログラムによって解消される場合がある。

ダイアラー
通話料金が高額な海外や Q2 ダイヤルなどのサービスに電話するプログラム。

トロイの木馬
コンピューターに侵入し、データを外部に流出させたり、他のプログラムが侵入するための入り口を作ったりする悪質なウイルス。

ヒューリスティック分析
定義データベースに登録されていない、未知のウイルスなどの脅威を検知する仕組み。

フィッシング（詐欺）
銀行など実在の金融機関を装った詐欺。金融機関からの連絡と偽ったメールを送り、偽サイトにアクセスさせ、個人情報を入力させる。入力した情報を悪用して、お金を引き出すなどの犯罪が起きている。

複合ファイル
アーカイブファイルなど、外見上は 1 つのファイルに圧縮された、複数のファイルが含まれているファイル。カスペルスキーは、複合ファイル内のファイルをスキャンできる。

マルウェア
ウイルスやスパイウェアなど、悪意のあるソフトウェア。

ルートキット
オペレーティングシステム内の侵入者や悪意のあるソフトウェアの痕跡を隠すために開発されたプログラムまたはプログラムのセット。

ワーム
自己増殖しながら、データの破壊活動などを行うコンピューターウイルス。

ユーザー登録とサポートサービスについて

ユーザーのみなさまが快適に製品をご利用いただけるように、各種サポートサービスをご用意しています。

ユーザー登録

ユーザー登録されたお客様には、新製品のご案内や製品のアップグレードなどに関する情報を提供いたします。

メインウィンドウの［ユーザー登録］をクリックするとブラウザーが起動し、ユーザー情報登録ページが表示されます。ページの指示に従って、ユーザー登録してください。

サポートサービスをご利用になる前に

サポートサービスをご利用になる前に、次の Web サイトをご確認ください。

- **サポートセンターのご案内（個人向け製品）：**
  http://support.kaspersky.co.jp/support/consumer_contact/
- **テクニカルサポートへのご連絡に関するヒント：**
  http://support.kaspersky.co.jp/support/details/

マイカスペルスキーアカウントによるテクニカルサポート

マイカスペルスキーアカウントは、テクニカルサポートサイトにある各ユーザー固有のエリアです。
マイカスペルスキーアカウントにアクセスするには、登録ページで登録処理を行う必要があります。すでに登録されている場合は、メールアドレスとパスワードを入力し、マイカスペルスキーアカウントにログインします。

マイカスペルスキーアカウントでは、次のサービスなどをご利用いただけます。

- **テクニカルサポートサービスへの、Web お問い合わせフォームを利用したご連絡**
- **お問い合わせのステータスをリアルタイムに追跡**
- **お問い合わせの詳細履歴の表示**
- **アクティベーションコードと登録情報の管理**

お問い合わせの送信フォームの項目に、次の情報を指定してください。

- ○ 製品
- ○ バージョン
- ○ オペレーティングシステム
- ○ お問い合わせの種類
- ○ お問い合わせ内容
- ○ 添付するファイル

マイカスペルスキーアカウントで指定されたメールアドレス宛てに、お問い合わせに対する返答が送信されます。

ライセンスに関するお問い合わせ

「ライセンスの期限が切れたので再購入したい」、「自分のライセンスの情報を知りたい」、「ライセンスを追加したい（プライベートライセンスのみ可能）」など、ライセンスに関するお問い合わせは、お電話でカスペルスキーインフォメーションセンターにお問い合わせください。

カスペルスキーインフォメーションセンター
電話番号：0570-001269（別途通話料がかかります）
03-6745-0303（ナビダイヤル非対応の場合、こちらにおかけください）
受付時間：9:30-18:00 365 日

ご注意

インフォメーションセンターでは、お客様からのお問い合わせ内容を正確に把握し、かつ早期に解決するためお問い合わせ内容を記録・保管・録音させていただくことがあります。

ご購入後の技術的なお問い合わせ

製品の操作方法、不具合、その他技術的なお問い合わせができます。電話でのお問い合わせをご利用いただけます。

カスペルスキーテクニカルサポートセンター
電話番号：0570-006269（別途通話料がかかります）
03-6745-0304（ナビダイヤル非対応の場合、こちらにおかけください）
受付時間：9:30-18:00 365 日

日にちや時間帯によっては、電話のお問い合わせが集中し、電話が通じにくい場合がございます。
待たずにお問い合わせができるマイカスペルスキーアカウントもぜひご利用ください。

ご注意

お電話の際にお使いのコンピューターを実際に操作できる状態で連絡いただきますと、解決までの時間を短縮できる場合がございます。またご質問内容によってはお時間をいただくことがございますので、あらかじめご了承ください。
サポートセンターでは、お客様からのお問い合わせ内容を正確に把握し、かつ早期に解決するためお問い合わせ内容を記録・保管・録音させていただくことがあります。

KASPERSKY LAB ZAO

Kaspersky Lab は、ウイルス、マルウェア、スパム、ネットワーク攻撃、ハッカーによる攻撃などの脅威に対する保護を提供する国際企業です。

2008 年、Kaspersky Lab は、エンドユーザー向け情報セキュリティソフトウェアのソリューション開発企業として、世界第 4 位に選ばれました（2008 年 IDC『Worldwide Endpoint Security Revenue by Vendor』）。また、コンピューター保護システムの開発企業としてロシアのホームユーザーから高い支持を受けています（2009 年 COMCON『TGI-Russia 2009』）。

Kaspersky Lab は 1997 年にロシアで設立され、今日モスクワの本部を中心に、5 つの地域部門を持つ国際的なグループ企業です。各地域部門は、ロシア、西ヨーロッパ、東ヨーロッパ、中東、アフリカ、北アメリカ、南アメリカ、日本、中国、およびその他のアジア太平洋諸国をまたにかけ、2,000 名を超える有資格スペシャリストが働いています。

製品：Kaspersky Lab の製品は、スマートフォンから家庭用 PC、大規模な企業ネットワークにいたるまで、すべてのシステムに保護を提供しています。

個人向けアンチウイルス製品は、デスクトップ PC、ノート PC、タブレットおよびスマートフォンなどのモバイル端末に対応しています。

法人向けには、ワークステーション、ファイルおよび Web サーバー、メールゲートウェイ、ファイアウォールを保護する製品やサービスを提供しています。これらの製品を Kaspersky Lab の一元管理システムと併用し、コンピューターへの脅威から企業や組織を自動保護する効率的なソリューションを実現しています。Kaspersky Lab の製品は主要なテスト機関で認定されており、多数のアプリケーションベンダーの製品と互換性があります。また、多くのハードウェアプラットフォーム向けに動作が最適化されています。

Kaspersky Lab のウイルスアナリストは 24 時間体制で活動しており、毎日何百と発生する IT 上の脅威を解析し、駆除ツールの作成ならびに Kaspersky 製品で使用する定義データベースの登録を行っています。Kaspersky Lab のウイルス定義データベースは毎時更新され、アンチスパムのデータベースは 5 分ごとに更新されます。

技術：現在のアンチウイルスツールに不可欠な技術の多くは、Kaspersky Lab が最初に開発したものです。Kaspersky Anti-Virus のカーネルは、多くの他社製品に使用されています。例として、SafeNet（米国）、Alt-N Technologies（米国）、Blue Coat Systems（米国）、Check Point Software Technologies（イスラエル）、Clearswift（米国）、CommuniGate Systems（米国）、Critical Path（アイルランド）、D-Link（台湾）、M86 Security（米国）、GFI（Malta）、IBM（米国）、Juniper Networks（米国）、LANDesk（米国）、Microsoft（米国）、NETASQ（フランス）、NETGEAR（米国）、Parallels（ロシア）、SonicWALL（米国）、WatchGuard Technologies（米国）、ZyXEL Communications（台湾）があげられます。またこれらの企業の革新的な技術の多くは特許を受けています。

成果：長年に渡り、Kaspersky Lab はコンピューターの脅威に対抗するサービスで数々の賞を受けてきました。たとえば、2010 年は、権威あるオーストリアのアンチウイルス機関 AV-Comparatives が実施するテストで最高レベルの Advanced+ を取得しています。しかし、最も大きな成果は、世界各国のユーザーの信頼を獲得したことと言ってよいでしょう。現在 Kaspersky Lab の製品と技術は、3 億人を超えるユーザー、および 20 万社以上のクライアント企業を保護しています。

Kaspersky Lab の Web サイト：	http://www.kaspersky.com
ウイルス百科事典（英語）：	http://www.securelist.com
アンチウイルスラボ：	newvirus@kaspersky.com （危険な可能性があるオブジェクトの送付のみ受け付けます。送付前に必ず圧縮してください）
	http://support.kaspersky.com/virlab/helpdesk.html （ウイルスアナリストへの問い合わせ用フォーム。英語）
Kaspersky Lab Web フォーラム：	http://forum.kaspersky.com

索引

アルファベット

BBS 83
CPU 12
DoS 88
IMAP 75
Internet Explorer 設定診断 109
Kaspersky Lab 116
Kaspersky Security Network 15, 26
Microsoft Office Outlook 75, 90
OS 12
SNS 57
SSL 98
USB メモリ 46
Windows 設定診断 107

あ

アクティベーション 14, 17, 21
アクティベーションコード 14, 17, 21
アクティベーションの実行 21
アップデート 36
アドウェア 93
アプリケーションコントロール 79
アプリケーションステータス 79
アプリケーション動作状況 79
アプリケーションルール 81
アンインストール 14, 19
暗号化 98
アンチスパム 89
アンチバナー 91
イベント通知 52
インスタントメッセージング 78
インスタントメッセンジャー 57
インストール 14
インポート 103
ウェブアンチウイルス 76
エクスプローラー 41
エクスポート 103
オートダイヤラー 93
お問い合わせ 115
オブジェクトスキャン 39, 41
主な機能 22

か

隔離 55
ガジェット 34
画面構成 28
簡易スキャン 39, 40
完全スキャン 39, 40
管理者アカウント 14
キーロガー 24
危険サイト診断 24, 66
起動する 49
脅威の検知時の処理 45, 70
脅威の処理方法 69
許可するネットワーク 86
クイック起動アイコン 64
駆除 51
クラウドプロテクション 26
グループルール 81
ゲームモード 102
検知した脅威 54
検知時の処理 83
検知する脅威 93
個人情報 57

さ

サウンド 12
削除 51
サポートサービス 113
システムウォッチャー 83
システム要件 12
システムリソース 101
自動実行 42
終了する 49
使用許諾契約書 15
詳細レポート 53
証明書 98
ショートカットアイコン 46
初期化 104
侵入攻撃 88
信頼するアプリケーション 95
信頼するオブジェクト 94
信頼リスト 94
スキャン 39
スキャンの対象 43
スキャンの中断 40
スケジュール 38, 42
スパム 89

ぜい弱性 39
ぜい弱性攻撃ブロック 85
ぜい弱性スキャン 39, 40
セキュリティキーボード 24, 63
セキュリティレベル 44, 72, 74, 76, 89
設定ウィンドウ 31
ソーシャルネットワークサービス 57

た

タスクバーアイコン 32
タスクマネージャー 33, 40
通知ウィンドウ 50
ツール 33
強い制限付き 79
定義データベース 36
ディスプレイ 12
低負荷スキャン 102
データ入力保護 62
テクニカルサポート 114
トラブルシューティング 111

な

特別な駆除 101
ネット決済保護 24, 59
ネットワーク攻撃防御 88, 100
ネットワークステータス 86
ネットワークポート 97
ネットワークモニター 100
ネットワークルール 87
ノート PC 102

は

ハードディスク 12
パスワード 69
パッカー 93
バッテリー 102
バナー広告 91
パフォーマンス 101
パブリックネットワーク 86
ヒューリスティック分析 44, 72, 83
ファイアウォール 86
ファイルアンチウイルス 72
フィッシングサイト 22
復元 54, 55
複合ファイル 44, 72
複数台用ライセンス 14
プライバシークリーナー 108
プライバシープロテクション 82
プライベートネットワーク 86
プラグイン 13
プロキシサーバー 99
プログラム 36
プロテクション 47
プロテクションの再開 47
プロテクションの停止 47, 48
プロテクションを有効にする 68
プロトコル 100
便利ツール 105
ポート 100
ポートスキャン 88
保護されたブラウザー 59
保護者による管理 24, 56
保護状態 35

ま

マイカスペルスキーアカウント .. 14, 17, 114
迷惑メール 89
メインウィンドウ 28
メールアンチウイルス 74
メッセンジャーアンチウイルス 78
メモリ 12

や

有効期限 20, 21
ユーザー登録 113
弱い制限付き 79

ら

ライセンス 20
ライセンスの更新 21
ライセンスの購入 20
ランチャー 29
リムーバブルドライブ 46
ルートキットスキャン 102
レスキューディスク 105
レポートウィンドウ 31
ロールバック 84, 110

著作権について

本ガイド（紙媒体または電子データで提供するものを含みます）は株式会社カスペルスキーが作成したものであり、その著作権は、Kaspersky Lab に帰属します。使用許諾契約書の条項のほか、以下の点も併せてご確認ください。

- お客様は、ガイドを現状の内容のまま、もしくは編集・修正して、画面上もしくは紙資料として利用することができます。ただし、これを第三者へ提供したり、貸し出しすることはできません。
- 権利者の許諾を得ることなく、本ガイドの全部または一部を複製、転用、送信等を行うことは、著作権法上禁止されております。また、当社の書面による許可なく複写、複製して頒布することは、その形態を問わず禁じます。
- 記載された内容は、改良のため予告なく変更することがあります。

サードパーティコードについて

サードパーティコードに関する情報は、製品をインストールしたフォルダー内のファイル legal_notices.txt に記載されています。

商標について

- Kaspersky® Internet Security 2013、カスペルスキー インターネット セキュリティ 2013、Kaspersky® Anti-Virus 2013、カスペルスキー アンチウイルス 2013、Kaspersky®、iArc™、iChecker™、iCure™、iStream™、iSwift™ は、Kaspersky Lab の商標または登録商標です。
- Microsoft、Windows、Windows Vista、Internet Explorer、Outlook は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- Intel、Pentium、Intel Atom は、米国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。
- Mozilla、Firefox、Thunderbird は、Mozilla Foundation の米国およびその他の国における商標または登録商標です。
- Google、Google Chrome、Google Talk は、Google Inc. の商標または登録商標です。
- Yahoo! は、Yahoo! Inc. の商標または登録商標です。
- その他記載された会社名、製品名等は、各社の商標または登録商標、もしくは弊社の商標です。なお本文中は ®、™ マークは記載していません。

テクニカルサポートサイトについて

テクニカルサポートサイトには、製品のインストールや使用方法に関する情報や推奨事項、よくある質問に対する回答などが記載されています。
製品の使用中に問題が発生した場合などに、ご利用ください。

http://support.kaspersky.co.jp

カスペルスキー インターネット セキュリティ 2013
カスペルスキー アンチウイルス 2013

2012 年 10 月 11 日第 1 版第 1 刷発行
©2012 Kaspersky Lab ZAO. 無断複写・転載を禁じます。