カスペルスキー セキュリティ for Mac

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 セキュリティ

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 ▶ 10 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 ▶ 17 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 ▶ 19 ページ

製品の主な機能、画面構成、各種ウイ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 ▶ 27 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 ▶ 35 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 ▶ 39 ページ

子供のコンピュータ利用制限、セキュリティキーボード、危険なサイトの診断など、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！「保護者による管理」を使ってみよう！

もっと、カスタマイズ

7 プロテクション機能の設定 ▶ 44 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 詳細な設定 ▶ 48 ページ

コンピュータ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）

9 付録 ▶ 51 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（53 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（21 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**

メインウインドウの ? ［ヘルプ］をクリックして表示します。また、各ウインドウの ? （ヘルプ）をクリックすると、現在表示されている関連項目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**

メインウインドウの ［サポート］をクリックすると、サポートウイ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公開日時、Mac OS のバージョンなどのシステム情報を確認できます。（これらの情報は、テクニカルサポートへのお問い合わせの際、必要になる場合があります。）
サポートウインドウの［問い合わせ］または［テクニカルサポート］をクリックすると、それぞれの Web サイトが表示されます。Web サイトでは、製品の機能や使用方法に関する有益な情報、新着情報、よくある質問と回答などを参照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 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 セキュリティを「カスペルスキー」と表記します。
● 本書では、Mac OS X 10.6 / 10.7 を使用した場合の操作手順を説明しています。また、Mac OS X 10.7 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インドウ名、タブやセクション名、項目名、ウイ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：［環境設定］ウインドウで、［プロテクション］を選択します。［ファイルアンチウイルスを有効にする］にオンにして、［保護範囲］をクリックします。
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：［Finder］－［アプリケーション］－［カスペルスキー セキュリティ］
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。

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 10
インストール 11
インストールする前に 11
インストールする 12
アクティベーションを実行する 14
はじめて起動したときに行うこと 15
アンインストール 16
アンインストールする 16

2 ライセンス・アクティベーション

ライセンス 17
ライセンスを確認する 17
ライセンスを購入する 17
アクティベーション 18
アクティベーションを実行する（ライセンスを更新する） 18

3 主な機能と画面構成

主な機能 19
コンピュータの保護 19
コンピュータのスキャン 19
定義データベースとプログラムのアップデート 19
インターネットの保護 20
検知履歴の確認と処理の実行 20
Kaspersky Security Network への参加 21
画面構成 22
メインウインドウ 22
各種ウインドウ 24
環境設定ウインドウ 24
レポートウインドウ 25
メニューバーのアイコン 26

4 基本的な使い方

保護状態の確認 27
保護状態を確認する 27
保護状態の詳細を確認する 27
定義データベースとプログラムのアップデート 28
定義データベースの状態を確認する 28
アップデートを実行する 28
アップデート前の状態に戻す 29
アップデートの自動実行を設定する 29
スキャンの実行・設定 30
スキャンの種類 30
スキャンを実行する 30
スキャンの対象を設定する 32
脅威の検知時の処理方法を設定する 33
プロテクション機能の停止・再開 34
プロテクション機能を一時的に停止する・再開する 34
カスペルスキーを終了する・起動する 34

5 脅威への対処

通知ウインドウが表示されたら 35
処理結果の確認（レポート） 36
レポートを表示して確認する 36
検知された脅威を処理する 36
隔離されたオブジェクトを操作する 37
バックアップされたオブジェクトを処理する 38
タスクの実行履歴を確認する・保存する 38

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利用の制限 39
保護者による管理を有効にする 39
制限する内容を設定する 40
使用状況を確認する 41
入力情報の漏えいを防止 42
セキュリティキーボードを利用する 42
危険なサイトへのリンクを診断 43
危険サイト診断を設定する 43

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 44
プロテクションの有効・無効を切り替える 44
ファイルアンチウイルス 45
（ファイルからの感染を検知） 45
検知時の処理方法を設定する 45
保護範囲を設定する 46
ウェブアンチウイルス 47
（Web ページからの感染を検知） 47
検知時の処理方法を設定する 47

8 詳細な設定

検知する対象の設定 48
検知する脅威を設定する 48
信頼する対象の設定 49
信頼するファイルとフォルダを追加する 49
信頼する URL を追加する 50

9 付録

トラブルシューティング 51
用語解説 52

ユーザー登録とサポートサービスについて 53
ユーザー登録 53
サポートサービスをご利用になる前に 53
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 54
ライセンスに関するお問い合わせ 55
ご購入後の技術的なお問い合わせ 55
KASPERSKY LAB ZAO 56
索引 58

システム要件

カスペルスキー セキュリティ（以下、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	Mac OS X 10.6、10.7、または 10.8
CPU	Intel プロセッサ（Power PC には対応しておりません。）
ハードディスク必要容量	350 MB 以上 ※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・バックアップで使用する容量は、製品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（アクティベーションおよびアップデートに使用）

注意事項

- 本製品のご使用前に使用許諾契約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。
  http://www.kaspersky.co.jp/security-mac

プラグイン

- **危険サイト診断**
  危険サイト診断に対応するブラウザは、次のとおりです。専用プラグインがインストールできます。
  - Safari
  - Mozilla Firefox
  - Google Chrome

Web の保護対象範囲

- **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。

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情報を準備する**

カスペルスキーを使用するユーザでログオンします。ログインしたユーザ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名とパスワードを入力する必要があります。

※Mac OS X で最初に設定するユーザアカウントが管理者アカウントです。［システム環境設定］の［アカウント］で確認することができます。

□ **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。

お知らせ　ライセンスの種類と複数のコンピュータへのインストール

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にインストールして使用できます。

メインウインドウの［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

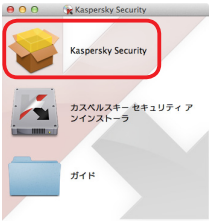
インストールを実行します。インストールは、画面の指示に従って進めます。

1. **コンピュータに本製品の CD-ROM をセットします。**

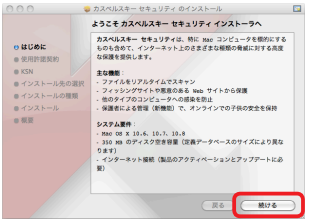
> **本製品をダウンロードで入手した場合**
> 手順 1 の代わりに、ダウンロードしたファイルを実行します。

2. **インストーラをダブルクリックします。**

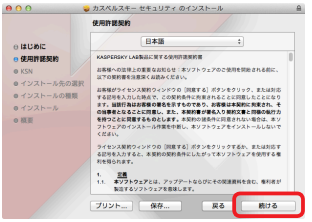
インストールを実行するかどうかを確認するメッセージが表示された場合は、［続ける］をクリックします



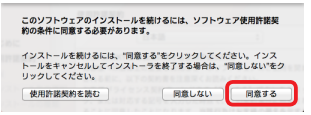
3. **インストーラが起動したら、製品の主な機能やシステム要件を確認し、［続ける］をクリックします。**



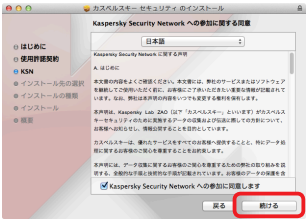
4. **ソフトウェア使用許諾契約の内容を確認し、［続ける］をクリックします。**



5. **ソフトウェア使用許諾契約条件への同意を求めるメッセージが表示されたら、［同意する］をクリックします。**



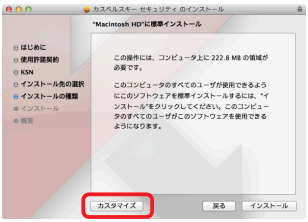
6. **Kaspersky Security Network 声明を確認し、Kaspersky Security Network に参加する場合は、［Kaspersky Security Network への参加に同意します］をオンにして、［続ける］をクリックします。**



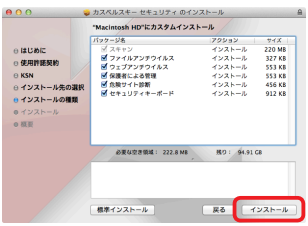
Kaspersky Security Network（KSN）

詳しくは、21 ページ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。

7. **インストールする機能を選択したい場合は［カスタマイズ］をクリックします。**



8. **一覧からインストールしたい機能のチェックボックスをオンにして、［インストール］をクリックします。**

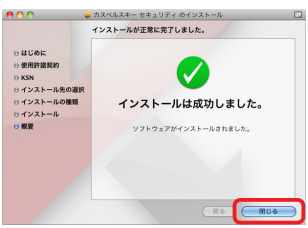


認証画面が表示される場合があります

お使いの環境によっては、認証画面が表示される場合があります。その場合、管理者のアカウント名とパスワードを入力してください。

9. **インストールが終了し、「インストールは成功しました。」と表示されたら、［閉じる］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を選択する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を選択する画面が表示されたら、次の手順を実行します。

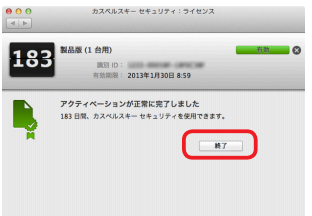
有効期限が切れていないライセンスが保存されている場合（ライセンス情報を残したままアンインストールした場合など）、アクティベーション方法を選択する画面は表示されず、自動的にアクティベーションが実行されます。カスペルスキーのメインウインドウが起動したら、アクティベーションが完了した状態になっています。あらためてアクティベーションを実行する必要はありません。

1. **［アクティベート］をクリックします。**

2. **アクティベーションコードを入力し、［アクティベート］をクリックします。**

> **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。

3. **正常にアクティベーションが完了すると、「アクティベーションが正常に完了しました」と表示されるので、ライセンス情報を確認して［終了］をクリックします。**



4. **［ようこそ カスペルスキー セキュリティ］画面が表示されます。**

機能名をクリックすると、各機能の説明が表示されます。
［使用開始］をクリックすると、メインウイ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、ライセンスウインドウを確認してください。

▶ P.17 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.18 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が保護されているか、メインウインドウの表示から確認してください。

▶ P.27 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

最新のウイルスからコンピュータ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.28 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の完全スキャンを実行してください。

▶ P.30 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。

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. **メニューバーにあるカスペルスキーのアイコンをクリックして、［終了］を選択します。**

2. **コンピュータに本製品の 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。

3. **［カスペルスキー セキュリティ アンインストーラ］をダブルクリックします。**

4. **［続行］をクリックします。**

   認証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、認証画面が表示される場合があります。その場合、管理者のアカウント名とパスワードを入力してください。

5. **アンインストールが完了し、「アンインストールは正常に完了しました」と表示されたら、［完了］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。

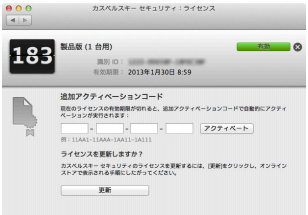
ライセンスを確認する

ライセンスの種類や状態、有効期限は、ライセンスウインドウから確認できます。

1. メインウインドウの （ライセンス）をクリックします。

ライセンスウインドウが表示されます。
ライセンスの状態、種類、有効期限、残り日数などが確認できます。

▶ P.17 ライセンスを購入する
▶ P.18 アクティベーション



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、ライセンスウインドウから購入できます。

1. メインウインドウの （ライセンス）をクリックします。

2. ［更新］をクリックします。

ブラウザが起動し、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.18 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。インストール時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。

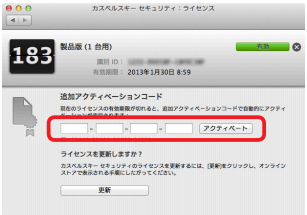
アクティベーションを実行する（ライセンスを更新する）

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. メインウインドウの （ライセンス）をクリックします。

2. アクティベーションコードを入力し、［アクティベート］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。xxxxx-xxxxx-xxxxx-xxxxx の形式で記載されています。
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.17 ライセンスを購入する

3. 正常にアクティベーションが完了すると、「アクティベーションが正常に完了しました」と表示されるので、ライセンス情報を確認して［終了］をクリックします。

ライセンスウインドウに戻ります。
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、さまざまな保護機能によって、ウイルスなどの脅威からコンピュータのデータを保護します。

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、［環境設定］ウインドウから行います。
▶ P.24 環境設定ウインドウ

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。

● **ファイルアンチウイルス　▶ 45 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。

● **ウェブアンチウイルス　▶ 47 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。

コンピュータのスキャン

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　▶ 30 ページ**
コンピュータ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を直接指定するスキャンなど、用途に応じて、さまざまな方法が選べます。

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　▶ 28 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を保護できます。

インターネットの保護

● **保護者による管理**　▶ 39 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。

● **セキュリティキーボード**　▶ 42 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、自動的にセキュリティキーボードを起動し、マウスで入力を行うことで、キーロガーに入力情報が盗まれるのを防ぎます。

キーロガー

コンピュータに侵入し、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**　▶ 43 ページ

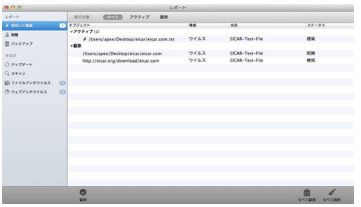
ブラウザでページを表示したとき、そのページに含まれるリンクに危険なページがないかどうかを自動的にチェックし、リンクの横に危険を示すアイコンを表示します。知らずに危険なサイトへアクセスしてしまうのを未然に防ぎます。

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、情報を確認できます。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。

● **レポート**　▶ 36 ページ

これまでに検知した脅威の数や種類、処理結果などを確認でき、未処理の脅威に対して駆除することもできます。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。
また、感染し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。
さらに、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。



Kaspersky Security Network への参加

● Kaspersky Security Network

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カスペルスキーに報告され、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、[環境設定］ウインドウの［KSN］で、［Kaspersky Security Network への参加に同意する］をオンにします。

画面構成

メインウインドウ

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

表示するには

次のいずれかの方法でメインウインドウを表示します。

- Finder で、［アプリケーション］ － ［カスペルスキー］を選択します。
- メニューバーでカスペルスキーのアイコン をクリックし、表示されるメニューから［カスペルスキー］をクリックします。

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インドウが表示されます。

ボタン	説明
レポート	レポートウインドウを表示します。脅威の検知駆除の履歴が確認でき、未処理の脅威に対しては、処理を実行できます。さらに、アップデートやスキャンなどのタスクの履歴を確認することもできます。 ▶ P.25 レポートウインドウ
環境設定	設定ウイ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.24 環境設定ウインドウ
サポート	サポートウイ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、テクニカルサポートなどの情報ページへアクセスできます。 ▶ P.53 ユーザー登録とサポートサービスについて
ヘルプ	ヘルプウインドウを表示します。 詳細な設定方法や操作手順などを確認できます。

2 情報表示エリア

コンピュータの現在の保護状態が表示されます。スキャンまたはアップデートの実行中にはその進行状況が、完了時にはタスクの結果が表示されます。

3 アップデート

定義データベースとプログラムをアップデートします。

4 スキャン

スキャン、簡易スキャン、完全スキャンのいずれかを実行できます。

5 インジケータ

コンピュータの現在の保護状態が以下の色で表示されます。

- 緑（正常）：コンピュータが正常に保護されていることを示します。
- 黄（注意）：カスペルスキーの設定または動作に問題があり、コンピュータの保護に一部問題があることに注意を喚起しています。
- 赤（危険）：カスペルスキーの設定または動作に問題があり、コンピュータが危険な状態にあることを警告しています。
  これらの問題を解決するには、インジケータをクリックしてプロテクションセンターを起動します。

6 ライセンス

現在のライセンス情報（ライセンス番号、有効期間、ライセンスの種類）を表示するウインドウが表示されます。このウインドウからライセンスのアクティベーションや更新を行うことができます。

7 保護機能

ファイルアンチウイルス、ウェブアンチウイルス、保護者による管理の各設定画面が表示されます。

8 統計・定義データベース情報

保護機能の上に表示されるハンドルマークをクリックすると、［統計］と［定義データベース情報］が表示されます。の最終アップデート日時と状態が表示されます。

［統計］には最後にスキャンされた結果が、［定義データベース情報］には現在の定義データベースの情報が表示されます。

各種ウインドウ

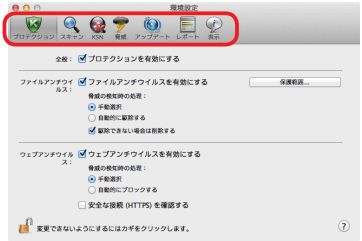
設定や確認を行うために、メインウインドウから表示する主なウインドウについて説明します。

環境設定ウインドウ

［環境設定］ウインドウでは、各機能の設定を行います。スキャン範囲を設定したり、プロテクション機能の処理方法の変更したりできます。

［環境設定］ウインドウは、メインウインドウ左上にある［環境設定］をクリックして表示できます。

［環境設定］ウインドウには、［プロテクション］／［スキャン］／［KSN］／［脅威］／［アップデート］／［レポート］／［表示］の 7 つのカテゴリがあり、ウインドウ上部のアイコンで切り替えられます。
目的のカテゴリに切り替えたら、表示される内容を設定します。



設定できる内容は、次のとおりです。

カテゴリ	説明
プロテクション	プロテクションに関する設定を行います。 ▶ P.44 全般的なプロテクション設定 ▶ P.45 ファイルアンチウイルス ▶ P.47 ウェブアンチウイルス
スキャン	スキャンに関する設定を行います。 ▶ P.30 スキャンの実行・設定
KSN	KSN への参加設定のほか、危険サイト診断とセキュリティキーボードのプラグイン設定を行います。 ▶ P.21 Kaspersky Security Network への参加 ▶ P.43 危険なサイトへのリンクを診断 ▶ P.42 入力情報の漏えいを防止
脅威	検知する脅威や信頼リストの設定を行います。 ▶ P.48 検知する対象の設定 ▶ P.49 信頼する対象の設定
アップデート	アップデートに関する設定を行います。 ▶ P.28 定義データベースとプログラムのアップデート
レポート	レポートに関する設定を行います。 ▶ P.36 処理結果の確認（レポート）
表示	通知に関する設定を行います。 ▶ P.35 通知ウインドウが表示されたら

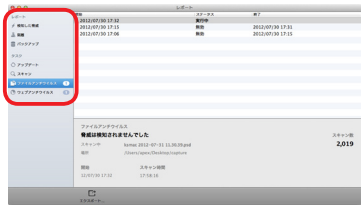
レポートウインドウ

［レポート］ウインドウは、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］ウインドウは、メインウインドウ左上にある［レポート］をクリックして表示できます。

［レポート］では、検知した脅威を確認したり、隔離やバックアップに格納されたオブジェクトを処理したりできます。
［タスク］では、アップデートやスキャン、各プロテクションの実行履歴が確認できます。

▶ P.36 処理結果の確認（レポート）



メニューバーのアイコン

カスペルスキーのインストール後、メニューバーにアイコンが表示されます。クリックして表示されるメニューから、操作を実行できます。

メニューには、次の項目が表示されます。

項目	説明
カスペルスキー セキュリティ	メインウインドウが表示されます。 ▶ P.22 メインウインドウ
プロテクションを無効／有効にする	プロテクション機能の一時停止と再開を行います。 その下にグレーで現在の状態が表示されます。 ▶ P.34 プロテクション機能の停止・再開
プロテクションセンター	プロテクションセンターが表示されます。保護に問題がある場合、状態と解決方法が表示されます。
簡易スキャン	簡易スキャンが実行されます。 ▶ P.30 スキャンの実行・設定
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が実行されます。 ▶ P.28 定義データベースとプログラムのアップデート
保護者による管理	［保護者による管理］ウインドウが表示されます。 ▶ P.39 保護者によるコンピュータ利用の制限
環境設定	［環境設定］ウインドウが表示されます。 ▶ P.24 環境設定ウインドウ
終了	カスペルスキーを終了します。 ▶ P.34 カスペルスキーを終了する・起動する

保護状態の確認

現在のコンピュータの保護状態は、メインウインドウから確認できます。

保護状態を確認する

1. **メインウインドウに表示される、インジケータで保護状態を確認します。**

▶ P.22 メインウインドウ

コンピュータ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］	コンピュータの保護は適切に行われています。
黄［注意］	コンピュータは推奨する状態になっていません。
赤［危険］	コンピュータ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. **メインウインドウのインジケータをクリックします。**

▶ P.22 メインウインドウ

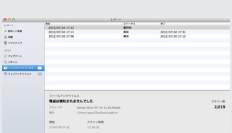
2. **［プロテクションセンター］に表示されている内容を確認します。**

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**

［レポート］ウインドウでは、保護の履歴を確認できます。

▶ P.36 処理結果の確認（レポート）



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が行われ、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. メインウインドウの [redacted] をクリックします。

［定義データベース情報］欄に、現在使用している定義データベースのアップデート日時と、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. メインウインドウの （アップデート）をクリックします。

アップデートが開始され、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 をクリックすると、［プロテクションセンター］が表示され、進捗状況の確認や、アップデートの停止ができます。

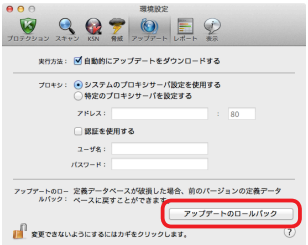
アップデート前の状態に戻す

アップデートの実行中に、ネットワークトラブルなどでアップデートに失敗した場合、前回の定義データベースに戻すことができます。このことをロールバックといいます。

※定義データベースを、前回より前の状態に戻すことはできません。

1. **メインウインドウの ⚙ ［環境設定］をクリックします。**
2. **［環境設定］ウインドウの［アップデート］をクリックします。**
3. **［アップデートのロールバック］をクリックします。**

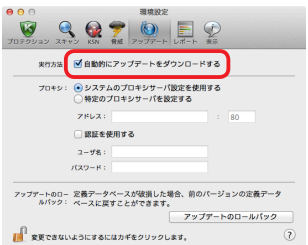
   ロールバックが開始され、進行状況が表示されます。
   ロールバックが終了すると、前回の定義データベースに戻ります。
   もし、定義データベースが最新でなくなった場合は、［アップデートの実行］をクリックして、あらためてアップデートを実行することをおすすめします。



アップデートの自動実行を設定する

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. **メインウインドウの ⚙ ［環境設定］をクリックします。**
2. **［アップデート］をクリックします。**
3. **［自動的にアップデートをダウンロードする］をオンにします。**
4. **（閉じる）をクリックします。**



お知らせ　プロキシサーバを設定する

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

［環境設定］ウインドウの［アップデート］-［プロキシ］で、［システムのプロキシサーバ設定を使用する］または［特定のプロキシサーバを設定する］のどちらかを選択します。

［特定のプロキシサーバを設定する］を選択した場合は、プロキシサーバ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。

スキャンの実行・設定

コンピュータ内にウイルスが潜んでいないか、Mac OS 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 Mac OS の起動時に読み込まれるプログラムなど、コンピュータ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。
- **スキャン**
  ファイルやフォルダ、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。

スキャンを実行する

ファイルをスキャンして、コンピュータ内のウイルスを検知します。
スキャン中は、メインウイ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.28 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] の場合

1. **メインウインドウの （スキャン）をクリックします。**
2. **[完全スキャン] または [簡易スキャン] をクリックします。**
   スキャンが実行されます。

   をクリックすると、プロテクションセンターが表示され、進捗状況や残り時間などが確認できます。[停止] クリックすると、スキャンを中断することもできます。
   さらに、 をクリックすると、レポートウインドウが表示され、より詳細なスキャンの状況を確認できます。
   ▶ レポート

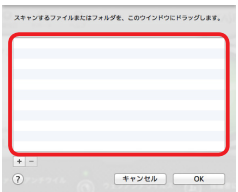
[スキャン] の場合

対象を選択してスキャンするには、次の 3 つの方法があります。

ファイル／フォルダをドラッグ＆ドロップ

1. メインウインドウの （スキャン）をクリックします。
2. [スキャン] をクリックします。
3. 表示されるウインドウに、スキャンしたいファイルやフォルダをドラッグ＆ドロップします。

   スキャンが実行されます。



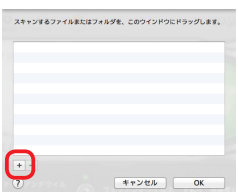
メニューから選択

1. メインウインドウの （スキャン）をクリックします。
2. [スキャン] をクリックします。
3. 表示されるウインドウで、 + をクリックします。
4. 表示されるメニューから、スキャンする対象を選択します。

   一覧に対象が追加されます。

   [ファイルまたはフォルダ] を選んだ場合は、表示される [開く] ウインドウから追加したいファイルまたはフォルダを選び、[開く] をクリックします。

   − をクリックすると、一覧から対象を削除できます。



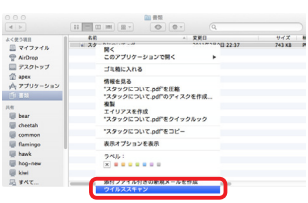
5. [OK] をクリックします。

   スキャンが実行されます。

Finder のコンテキストメニューから実行

1. Finder を起動します。
2. スキャンしたいファイルまたはフォルダを選択し、コンテキストメニューを表示します。
3. [ウイルススキャン] を選択します。

   スキャンが実行されます。



スキャンの対象を設定する

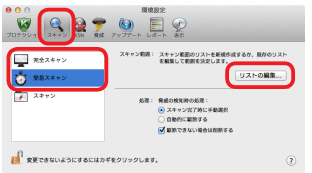
［完全スキャン］または［簡易スキャン］の対象となるファイルやフォルダを設定します。

1. メインウインドウの ⚙ ［環境設定］をクリックします。

2. ［スキャン］をクリックします。

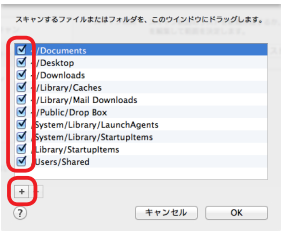
3. ［完全スキャン］または［簡易スキャン］をクリックします。

4. ［リストの編集］をクリックします。



5. 表示されるウインドウの一覧から、スキャンしたい対象をオンにします。

6. 一覧にスキャンしたい対象がない場合は、＋をクリックし、表示されるメニューから選択します。



一覧に対象が追加されます。
［ファイルまたはフォルダ］を選んだ場合は、表示される［開く］ウインドウから追加したいファイルまたはフォルダを選び、［開く］をクリックします。
ファイルやフォルダをウインドウにドラッグ＆ドロップして追加することもできます。
－をクリックすると、一覧から対象を削除できます。

7. ［OK］をクリックします。

8. （閉じる）をクリックします。

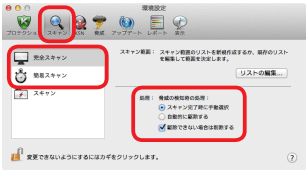
脅威の検知時の処理方法を設定する

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. **メインウインドウの ⚙ ［環境設定］をクリックします。**

2. **［スキャン］をクリックします。**

3. **［完全スキャン］／［簡易スキャン］／［スキャン］のいずれかをクリックします。**



4. **［脅威の検知時の処理］で、処理方法を選択します。**

- **スキャン完了時に手動選択**
  スキャンの完了時までオブジェクトの処理が延期されます。スキャン完了時に通知ウインドウが表示され、検知された危険なオブジェクトの情報、処理方法の選択肢が表示されます。オブジェクトごとに処理方法を指定できます。
- **自動的に駆除する**
  検知されると、通知ウインドウは表示せず、自動的に駆除します。

さらに、［駆除できない場合は削除する］をオンにすると、駆除できなかったファイルは削除されます。

5. **（閉じる）をクリックします。**

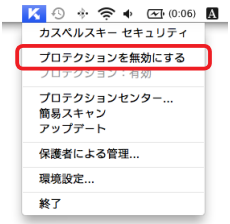
プロテクション機能の停止・再開

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。

プロテクションを停止する



1. **メニューバーにあるカスペルスキーのアイコン をクリックします。**
2. **表示されるメニューから、［プロテクションを無効にする］を選択します。**
   プロテクション機能が停止します。

プロテクションを再開する

1. **メニューバーにあるカスペルスキーのアイコン をクリックします。**
2. **表示されるメニューから、［プロテクションを有効にする］を選択します。**
   プロテクション機能が再開します。

［環境設定］ウインドウの［プロテクション］でもプロテクション機能の停止／再開ができます。［ファイルアンチウイルス］や［ウェブアンチウイルス］のプロテクション機能ごとに停止／再開することもできます。
▶ プロテクション

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自体を終了する方法と、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. **メニューバーにあるカスペルスキーのアイコン をクリックします。**
2. **表示されるメニューから、［終了］を選択します。**
   カスペルスキーが終了します。

カスペルスキーを起動する

1. **Finder の［アプリケーション］から、［カスペルスキー セキュリティ］をダブルクリックします。**
   カスペルスキーが起動します。

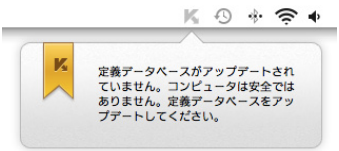
通知ウインドウが表示されたら

カスペルスキーがウイルスなどの脅威を検知すると、ポップアップウインドウと警告音で通知します。通知ウイ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。

通知ウインドウには、検知された脅威の種類や状況によって、次のような処理方法の選択肢が表示されます。

項目	説明
スキップ	処理は行われません。
削除	ウイルスを含んだファイルごと削除します。
駆除	検知したウイルスを駆除します。
ブロック	ダウンロードしようとしたファイルにウイルスが検知された場合、ダウンロードを中止します。
許可	ダウンロードしようとしたファイルにウイルスが検知された場合、ダウンロードを許可します。
選択した処理を常に実行	クリックしてオンにしたあとで、上記のいずれかの選択肢をクリックすると、以降同じ処理を実行します。
詳細	検知した脅威の詳細を確認できる Web ページが表示されます。

また、メニューバーのアイコンの近くにメッセージが表示される場合があります。



ご注意　通知の設定

［環境設定］ウインドウの［表示］では、通知の有効／無効や通知の種類の設定ができますが、初期設定どおりに、すべて有効に設定してお使いになることをおすすめします。

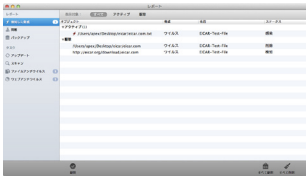
処理結果の確認（レポート）

レポート機能を使って、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、一覧で確認できます。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することもできます。また、アップデートやスキャンの実行履歴を確認して、テキストファイルに保存することも可能です。

レポートを表示して確認する

1. **メインウインドウの [レポート] をクリックします。**

2. **表示される［レポート］ウインドウで、項目を選択して内容を確認します。**



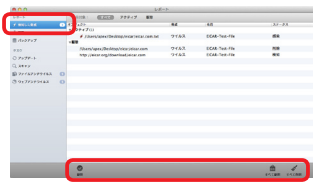
確認できる内容は、次のとおりです。

- **レポート**
  検知された脅威や、隔離／バックアップされたオブジェクトが表示されます。駆除や削除などの処理を行うこともできます。
  ▶ P.36 検知された脅威を処理する
  ▶ P.37 隔離されたオブジェクトを操作する
  ▶ P.38 バックアップされたオブジェクトを処理する
- **タスク**
  アップデート、スキャン、ファイルアンチウイルス、ウェブアンチウイルスの実行履歴が表示されます。
  ▶ P.38 タスクの実行履歴を確認する・保存する

レポートに注目すべきイベントが記録されると、メインウインドウの情報表示部やプロテクションセンターに が表示されている場合があります。このアイコンをクリックすると、[レポート] ウインドウが起動し、該当する内容が表示されます。

検知された脅威を処理する

1. **［レポート］ウインドウで、［検知した脅威］をクリックします。**



2. **表示される一覧から、処理したいオブジェクトを選択します。**

3. **実行したい処理をクリックします。**

実行できる処理は次のとおりです。

駆除	選択したオブジェクトを駆除します。
すべて駆除	一覧に表示されているすべてのオブジェクトを駆除します。
すべて削除	一覧に表示されている検知の記録をすべて削除します。オブジェクトは削除されません。

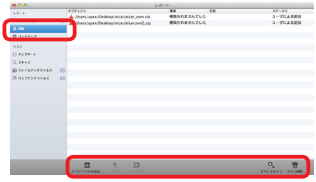
隔離されたオブジェクトを操作する

隔離とは、危険な可能性があるオブジェクトを、安全な状態にして特殊な領域（隔離フォルダ）に保存する処理です。隔離されたオブジェクトはシステムへアクセスできなくなり、脅威を拡散できなくなります。
脅威が検知されなかったが危険な可能性があるファイルは、手動で隔離できます。定義データベースが更新されたあと、あらためてスキャンを実行して駆除したり、安全が確認されたら元の場所に復元したり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、コンピュータ全体の感染を招く恐れがあります。

1. ［レポート］ウインドウで、［隔離］をクリックします。
2. 隔離にオブジェクトを追加する場合は、［オブジェクトの追加］をクリックして、ファイルを選択します。
3. オブジェクトを処理する場合は、表示される一覧から、処理したいオブジェクトを選択します。

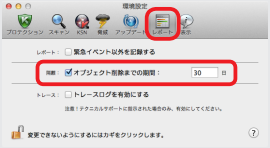


4. 実行したい処理をクリックします。
   実行できる処理は次のとおりです。

項目	説明
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	オブジェクトを削除します。
すべてスキャン	隔離に格納されている、すべてのオブジェクトをスキャンします。 隔離後に定義データベースが更新され、駆除できるようになることがあります。
すべて削除	隔離に格納されている、すべてのオブジェクトを削除します。

お知らせ　隔離の保存期間を設定する

［環境設定］ウインドウの［レポート］-［隔離］で、隔離にオブジェクトを保存しておく期間を設定できます。



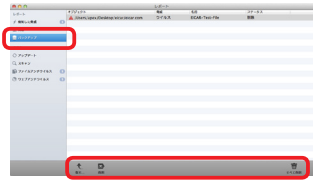
バックアップされたオブジェクトを処理する

ウイルスが検知されると、駆除または削除が行われます。駆除・削除されたオブジェクトは、特殊な領域に安全な状態でバックアップコピーが保存されます。
バックアップは、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。バックアップに格納されたオブジェクトはシステムへアクセスできなくなり、特殊な領域の外へ脅威を拡散できなくなります。バックアップに格納されたファイルは、あとから削除や復元などの操作ができます。

ご注意　復元には十分に注意してください

バックアップ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、コンピュータ全体の感染を招く恐れがあります。

1. **［レポート］ウインドウで、［バックアップ］をクリックします。**
2. **表示される一覧から、処理したいオブジェクトを選択します。**



3. **実行したい処理をクリックします。**

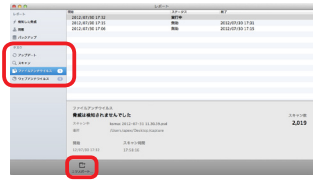
   実行できる処理は次のとおりです。

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	オブジェクトを削除します。
すべて削除	隔離に格納されている、すべてのオブジェクトを削除します。

タスクの実行履歴を確認する・保存する

各タスク（アップデート／スキャン／ファイルアンチウイルス／ウェブアンチウイルス）の実行履歴を確認できます。表示された実行履歴は、テキストファイルに保存することも可能です。

1. **［レポート］ウインドウで、［アップデート］／［スキャン］／［ファイルアンチウイルス］／［ウェブアンチウイルス］のいずれかをクリックします。**
2. **表示される一覧で、各タスクの実行履歴が確認できます。**



3. **ファイルに保存する場合は、保存したい対象を一覧から選択して、［エクスポート］をクリックします。**
4. **保存する場所とファイル名を指定し、［保存］をクリックします。**

   「txt」形式でファイルが保存されます。

保護者によるコンピュータ利用の制限

保護者による管理は、コンピュータ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。
Mac OS のユーザアカウント単位で設定できるため、ログイ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。

保護者による管理を有効にする

制限したいユーザ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。

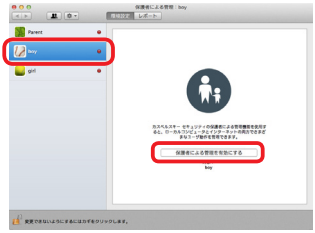
1. メインウインドウの［保護者による管理］をクリックします。

コンピュータに登録されているアカウントが一覧で表示されます。

> ウインドウ左下のカギマークが 🔒 になっている場合は、設定変更を可能にするため、🔒 をクリックしてロックを解除します。その際、認証画面が表示されるので、管理者のアカウント名とパスワードを入力してください。

2. 保護者による管理を有効にしたいアカウントを選択し、［保護者による管理を有効にする］をクリックします。

アカウント名に表示される 🔴 が 🟢 に変わります。



3. 制限したい項目を有効にします。

［Web 管理］／［時間管理］／［個人情報管理］／［SNS 管理］のそれぞれを選択して、［有効にする］をクリックします。

制限する内容を設定する

アカウントの項目ごとに、制限する内容を設定します。

1. ［保護者による管理］ウインドウで、制限内容を設定したいアカウントと項目をクリックします。

2. ［環境設定］をクリックします。

設定できる内容は、次のとおりです。

項目	説明
Web 管理	［Web 管理］では、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、［特定のサイト］をクリックして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。 ［セーフサーチ］では、検索エンジンが提供するセーフサーチ機能を強制的にオンにします。検索エンジンのセーフサーチによるフィルタリングが、常に検索結果に反映されます。 ［ダウンロードの管理］では、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ダウンロードをブロックできます。
時間管理	インターネットを使用できる時間を制限します。 1 日の使用時間を制限したり、使用可能な時間帯を平日と週末で指定したりできます。
個人情報管理	設定した個人情報の送信を制限します。 送信されるデータの中に、設定した情報が含まれているのを見つけると、送信をブロックして履歴を残します。
SNS 管理	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。

設定が終わったら、ウインドウ左下のカギマーク をクリックして、設定を変更されないようにロックしておくことをおすすめします。

お知らせ　同じ制限設定を他のアカウントにコピーする

同様の設定内容を他の複数のアカウントにも設定したい場合、設定内容をコピーできます。

［保護者による管理］ウインドウの をクリックして表示されるメニューから［設定のコピー］を選択します。コピーしたいアカウントを選択して、もう一度 のメニューから［設定のペースト］を選択します。

使用状況を確認する

保護者による管理を有効にすると、アカウント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］ウインドウで、制限内容を確認したいアカウントをクリックします。**

2. **［レポート］クリックします。**

   設定した項目の使用状況が一覧で表示されます。

3. **項目または［詳細］をクリックすると、項目ごとにより詳細な使用状況が確認できます。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 管理では、ユーザがアクセスした 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。

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。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。

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、ブラウザでパスワードなどの入力欄にカーソルを置くと、自動的に表示されます。

対応するブラウザは、Safari、Mozilla Firefox、Google Chrome です。
Safari では標準で設定されていますが、Mozilla Firefox や Google Chrome で同様に利用できるようにするには、次の設定が必要です。

1. **Mozilla Firefox または Google Chrome をインストールします。**
2. **メインウインドウの ⚙ ［環境設定］をクリックします。**
3. **［環境設定］ウインドウの［KSN］をクリックします。**
4. **［機能拡張］で、［セキュリティキーボード］のチェックをオンにします。**
5. **（閉じる）をクリックして、［環境設定］ウインドウを終了します。**

お知らせ **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。

お知らせ **ブラウザのアイコンから手動でセキュリティキーボードを起動する**

Safari、Mozilla Firefox、Google Chrome のツールバーにあるアイコン 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。

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、フィッシングサイトなどの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出された場合、リンクの横に危険を示すアイコンが表示されます。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。

危険サイト診断を設定する

対応するブラウザは、Safari、Mozilla Firefox、Google Chrome です。
Safari では標準で設定されていますが、Mozilla Firefox や Google Chrome で同様に利用できるようにするには、次の設定が必要です。

1. Mozilla Firefox または Google Chrome をインストールします。
2. メインウインドウの ［環境設定］をクリックします。
3. ［環境設定］ウインドウの［KSN］をクリックします。
4. ［機能拡張］で、［危険サイト診断］のチェックをオンにします。
5. （閉じる）をクリックして、［環境設定］ウインドウを終了します。

全般的なプロテクション設定

プロテクションの有効／無効を切り替えます。

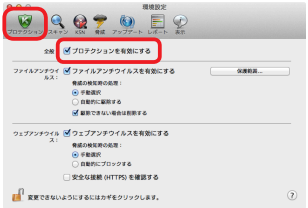
プロテクションの有効・無効を切り替える

各プロテクション機能は、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. メインウインドウの ⚙ ［環境設定］をクリックします。
2. ［プロテクション］の［全般］で、［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。
3. ⊗（閉じる）をクリックして、［環境設定］ウインドウを終了します。



メニューバー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.34 プロテクション機能の停止・再開

プロテクションごとに有効・無効を切り替える

1. メインウインドウの ⚙ ［環境設定］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を有効にする］または［ウェブアンチウイルスを有効にする］をオン／オフして、機能の有効／無効を切り替えます。
3. ⊗（閉じる）をクリックして、［環境設定］ウインドウを終了します。

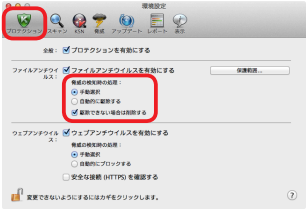
ファイルアンチウイルス
（ファイルからの感染を検知）

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を保護する機能です。Mac OS 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。

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、［手動選択］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。

1. **メインウインドウの ⚙ ［環境設定］をクリックします。**
2. **［プロテクション］をクリックします。**
3. **［ファイルアンチウイルス］の［脅威の検知時の処理］で、処理方法を次から選択します。**



- **手動選択**
  感染した、または疑わしいオブジェクトが検知されると、通知ウイ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。
  ▶ P.35 通知ウインドウが表示されたら
- **自動的に駆除する**
  感染したオブジェクトが検知されると、最も適切な方法ですぐに駆除が行われ、感染したオブジェクトはバックアップにコピーされます。
  ▶ P.38 バックアップされたオブジェクトを処理する
  感染が疑わしいオブジェクトが検知された場合は、ファイルへのアクセスがブロックされ、隔離へ移動されます。
  ▶ P.37 隔離されたオブジェクトを操作する
- **駆除できない場合は削除する**
  駆除できなかった場合の処理を指定します。オブジェクトごと削除する場合にオンにします。

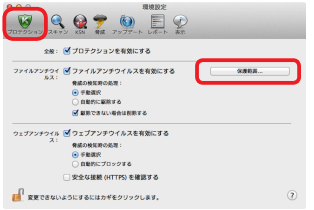
4. **（閉じる）をクリックして、［環境設定］ウインドウを終了します。**

検知の履歴や駆除結果は、［レポートの］［検知した脅威］で確認できます。
▶ P.36 処理結果の確認（レポート）

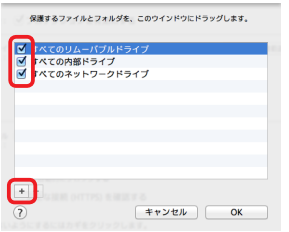
保護範囲を設定する

ファイルアンチウイルスによる保護の対象となるファイルやフォルダを設定します。初期設定では、ハードディスクドライブ、リムーバブルドライブ、およびネットワークドライブなど、コンピュータに接続されているすべてのデバイスのオブジェクトが対象に含まれています。通常は初期設定のまま変更する必要はありませんが、状況に応じて変更できます。

1. **メインウインドウの ⚙ ［環境設定］をクリックします。**
2. **［プロテクション］をクリックします。**
3. **［保護範囲］をクリックします。**



4. **表示されるウインドウの一覧から、保護の対象とする項目のオン／オフを切り替えます。**
5. **一覧に対象とする項目がない場合は、＋ をクリックし、表示されるメニューから選択します。**



一覧に対象が追加されます。
［ファイルまたはフォルダ］を選んだ場合は、表示される［開く］ウインドウから追加したいファイルまたはフォルダを選び、［開く］をクリックします。
ファイルやフォルダをウインドウにドラッグ＆ドロップして追加することもできます。
－ をクリックすると、一覧から対象を削除できます。

6. **［OK］をクリックします。**
7. **（閉じる）をクリックして、［環境設定］ウインドウを終了します。**

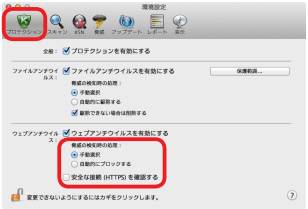
ウェブアンチウイルス
（Web ページからの感染を検知）

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ます。

検知時の処理方法を設定する

Web サイトからウイルスに感染したファイルをダウンロードするなど、Web トラフィックに脅威が検知された場合、ウェブアンチウイルスは、あらかじめ設定された方法に従って脅威を未然にブロックします。初期設定では、［手動選択］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。

1. **メインウインドウの ⚙ ［環境設定］をクリックします。**
2. **［プロテクション］をクリックします。**
3. **［ウェブアンチウイルス］の［脅威の検知時の処理］で、処理方法を次から選択します。**



- **手動選択**
  感染した、または疑わしいオブジェクトが Web トラフィックに検知されると、通知ウイ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。
  ▶ P.35 通知ウインドウが表示されたら
- **自動的にブロックする**
  感染したオブジェクトが Web トラフィックに検知されると、すぐにブロックされます。

4. **暗号化された Web トラフィック（HTTPS 接続）をスキャンする場合は、［安全な接続（HTTPS）を確認する］をオンにします。**
5. **（閉じる）をクリックして、［環境設定］ウインドウを終了します。**

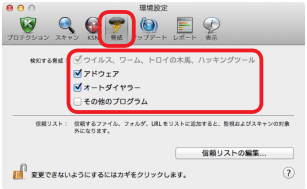
検知の履歴や駆除結果は、［レポートの］［検知した脅威］で確認できます。
▶ P.36 処理結果の確認（レポート）

検知する対象の設定

コンピュータ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、どのような悪意のあるソフトウェアからコンピュータを保護するか選択できます。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. メインウインドウの ⚙ ［環境設定］をクリックします。
2. ［脅威］をクリックします。



3. ［検知する脅威］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。

- **ウイルス、ワーム、トロイの木馬、ハッキングツール**
  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。オフにすることはできません。
- **アドウェア**
  危険なふるまいの発生源となるプログラムです。ユーザの望まない広告を表示するなど、潜在的に危険なプログラムを含みます。
- **オートダイヤラー**
  通話料金が高額なサービスに自動的に電話するプログラムです。
- **その他のプログラム**
  侵入者がコンピュータやデータに危害を加えるために、悪用する可能性のあるプログラムです。

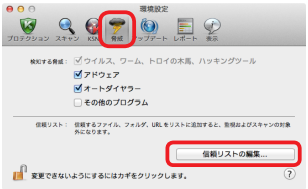
4. （閉じる）をクリックして、［環境設定］ウインドウを終了します。

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 Web サイトのリストです。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「信頼するファイルとフォルダ」と、Web サイトの URL を登録する「信頼する URL」があります。

信頼するファイルとフォルダを追加する

1. メインウインドウの ⚙ ［環境設定］をクリックします。
2. ［脅威］をクリックします。
3. ［信頼リスト］の［信頼リストの編集］をクリックします。

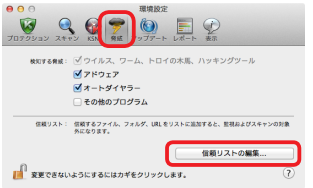


4. 表示されるウインドウで、［信頼するファイルとフォルダ］をクリックします。
5. ＋ をクリックします。
6. ［開く］ウインドウで信頼リストに追加したいファイルまたはフォルダを選択します。
   ［信頼するファイルとフォルダ］の一覧に追加したファイルが表示されます。
   － をクリックすると、一覧から削除できます。

7. ［OK］をクリックします。
8. ⊗（閉じる）をクリックして、［環境設定］ウインドウを終了します。

信頼する URL を追加する

1. メインウインドウの ⚙ ［環境設定］をクリックします。
2. ［脅威］をクリックします。
3. ［信頼リスト］の［信頼リストの編集］をクリックします。



4. 表示されるウインドウで、［信頼する URL］をクリックします。
5. ＋ をクリックします。
6. URL を入力します。
   ［信頼する URL］の一覧に表示されます。
   － をクリックすると、一覧から削除できます。

7. ［OK］をクリックします。
8. （閉じる）をクリックして、［環境設定］ウインドウを終了します。

トラブルシューティング

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。詳しくは、18 ページの「アクティベーション」を参照してください。

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でアクティベーションしたあと、残りの台数のコンピュータ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、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。詳しくは、17 ページの「ライセンス」を参照してください。

[定義データベースが破損しています]、[ライセンス情報のブラックリストが破損しています]と表示され、定義データベースがアップデートできない

➡ 定義データベースの一部が不正になっている可能性があります。
カスペルスキーをアンインストールし、再インストールしてください。

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、隔離フォルダに、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
コンピュータに侵入し、ユーザの操作を記録したり、情報を盗んだりするプログラム。

ダイヤラー
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開けたりする悪質なウイルス。

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。安心ネットセキュリティは、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。

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。

- **ユーザー登録のご案内：**
  https://kasperskylabs.jp/users/

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、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）が挙げられます。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

CPU 10
Finder 31
Kaspersky Lab 56
Kaspersky Security Network 13, 21
KSN 24
OS 10
SNS 管理 40
Web 管理 40

あ

アクティベーション 11, 14, 18
アクティベーションコード 11, 14, 18
アクティベーションの実行 18
アップデート 24, 28
アンインストール 11, 16
インジケータ 23, 27
インストール 11
ウェブアンチウイルス 47
お問い合わせ 55
主な機能 19

か

隔離 37
カスタマイズ 13
画面構成 22
簡易スキャン 30
環境設定 22
環境設定ウインドウ 24
完全スキャン 30
管理者アカウント 11
キーロガー 20
危険サイト診断 20, 43
起動する 34
脅威 24
脅威の検知時の処理 33, 45, 47
駆除 35, 36
警告音 35
検知した脅威 36
検知する脅威 48
個人情報管理 40

さ

サウンド 10
削除 35
サポートサービス 53
時間管理 40
システム要件 10
自動実行 29
終了する 34
信頼する URL 50
信頼するファイルとフォルダ 49
信頼リスト 49
スキャン 24, 30, 31
スキャンの対象 32
スケジュール 29
セキュリティキーボード 20, 42
ソーシャルネットワークサービス 40
ソフトウェア使用許諾契約 12

た

タスク 38
通知ウインドウ 35
通知の設定 35
定義データベース 28
ディスプレイ 10
テクニカルサポート 54
トラブルシューティング 51

は

ハードディスク 10
バックアップ 38
表示 24
ファイルアンチウイルス 45
フィッシングサイト 19
復元 37, 38
複数台用ライセンス 11
プラグイン 10
プロキシサーバ 29
プログラム 28
プロテクション 24, 34
プロテクションセンター 30
プロテクションの再開 34
プロテクションの停止 34
プロテクションを有効にする 44
保護者による管理 20, 39
保護状態 27
保護範囲 46

ま

マイカスペルスキーアカウント..... 54
メインウインドウ 22
メニューバーアイコン 26

や

有効期限..... 17, 18
ユーザー登録 53

ら

ライセンス..... 17, 23
ライセンスの更新 18
ライセンスの購入 17
レポート..... 22, 24, 36
レポートウインドウ 25
ロールバック 29

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® Security、カスペルスキー セキュリティ、Kaspersky®、iArc™、iChecker™、iCure™、iStream™、iSwift™ は、Kaspersky Lab の商標または登録商標です。
- Mac、Mac OS、Apple、Safari は、米国 Apple Inc. 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。
- Intel 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 は、Google 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 セキュリティ

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。