ノートン™ アンチウイルス プラス
ノートン™ 360
ノートン™ 360 with LifeLock™
ノートン™ 360 for Gamers

ユーザーマニュアル

Norton™

ノートン™ 360 with LifeLock™ ユーザーマニュアル

NortonLifeLock Inc.
60 East Rio Salado Parkway,
Suite 1000,
Tempe, AZ 85281

https://www.nortonlifelock.com

目次

第 1 章 ノートンLifeLock にようこそ 6

ノートン 360 のシステム要件 6
ノートンLifeLock アカウントへのアクセス 8

第 2 章 保護の設定 9

デバイスセキュリティの設定 9
ノートン パスワード マネージャーの設定 10
クラウドバックアップを設定する 15
LifeLock™ 個人情報盗難保護のセットアップ 15
ダークウェブモニタリング powered by LifeLock** 17
セキュア VPN の設定 17
保護者機能の設定 18
ノートン セーフウェブを使用した銀行情報の保護 22

第 3 章 デバイスセキュリティの管理 23

デバイスがリスクにさらされているときに実行するべき内容 23
ライブアップデートの実行 24
ノートンが検出したデバイスのセキュリティリスクを表示し、修正する 24
検疫済みのリスクまたは脅威を処理する 25
ノートンを使用してパソコンのパフォーマンスを最適化し、改善する 28
パソコンに脅威があるかどうかを確認するためにノートンのスキャンを実行する 31
独自にカスタムのノートンのスキャンを作成する 34
ノートンのスキャンをスケジュール設定する 35
ノートン SONAR によって検出された脅威をリアルタイムで表示する 36
ノートン自動保護、SONAR、ダウンロードインテリジェンススキャンからファイルやフォルダを除外する 37
ノートンのスキャンからシグネチャの危険度が低いファイルを除外する 38
自動タスクのオンとオフを切り替える 38
カスタムタスクを実行する 39

セキュリティとパフォーマンスのスキャンのスケジュールを設定する 40
データプロテクタでパソコンに影響する悪質なプロセスが遮断されるように設定する 41
フィッシングの試行で攻略される恐れのあるスクリプトを削除するようにノートンを設定する 43
ノートン スクリプト制御に関する詳細 46
デバイスをエクスプロイト、ハッカー、ゼロデイ攻撃から保護 48
ノートン ファイアウォールのオンとオフを切り替える 50
プログラムルールをカスタマイズしてプログラムのアクセス設定を変更する 51
ファイアウォールルールの順序を変更する 51
トラフィックルールを一時的にオフにする 52
遮断されたプログラムにインターネットアクセスを許可する 53
ファイアウォール遮断通知をオフにする 54
侵入防止除外リストについて 54
ブラウザ保護をオンにする 55
ノートン ファイアウォールの設定で、攻撃を遮断したときの通知を停止したり再開できます。 56
自動遮断のオンとオフを切り替える 57
ノートン 自動遮断で遮断されたパソコンを遮断解除する 57
デバイスを[デバイスの信頼]に追加する 58
ダウンロードインテリジェンスのオンとオフを切り替える 59
スパムフィルタ処理のオンとオフを切り替える 60
ノートンによるインターネットの使用を定義する 61
データ通信ポリシーのオンとオフを切り替える 62
アプリケーションを監視し、悪質な Web サイトからのパソコンへのアクセスを遮断するようにノートンを設定する 62
ノートン クラウドバックアップを初めて使用する 64
バックアップセットのファイルとフォルダを追加または除外する 65
バックアップに含めるデフォルトのファイルの種類またはファイル拡張子を表示または変更する 66
ノートンバックアップセットから写真、音楽、その他の重要なファイルを復元する 67
クラウドバックアップからのバックアップセットとファイルの削除 68
ノートン製品の設定のカスタマイズ 69
リアルタイム保護設定のカスタマイズ 70
スキャンとリスクの設定について 72
侵入とブラウザ保護の設定について 74
保護されているデバイスをリモートで管理できるようにノートン製品を設定する 75
ノートン デバイスセキュリティ設定を権限がないアクセスから保護する 75

ノートン デバイスセキュリティで情報を検索するショートカットキーを設定する 76
ゲーム オプティマイザーでパソコンをゲーム用に最適化する 76
ゲーム オプティマイザーの詳細 78
[最適化対象のゲーム]リストに手動でゲームを追加する 80

第 4 章 追加の解決策を検索 82

Windows からデバイスセキュリティをアンインストールする 82
免責事項 82

1

ノートンLifeLock にようこそ

この章では以下の項目について説明しています。

- ノートン 360 のシステム要件
- ノートンLifeLock アカウントへのアクセス

ノートン 360 のシステム要件

ノートン デバイスセキュリティ資格のみ

- ノートン™ アンチウイルスプラスは 1 台のパソコンまたは Mac をカバーします

デバイスセキュリティとノートン セキュア VPN 資格

Windows、Mac、Android と iOS で実行されるデバイスをサポートします

- ノートン™ 360 スタンダードは 1 台のデバイスをカバーします
- ノートン™ 360 デラックスは最大 5 台のデバイスをカバーします
- ノートン™ 360 プレミアムは最大 10 台のデバイスをカバーします
- ノートン™ 360 with LifeLock Select は最大 5 台のデバイスをカバーします
- ノートン™ 360 with LifeLock Advantage は最大 10 台のデバイスをカバーします
- ノートン™ 360 with LifeLock Ultimate Plus がカバーするデバイスの台数に制限はありません (制限が適用されます*)
- ノートン™ 360 ゲーマー版は最大 3 台のデバイスをカバーします

メモ: 上記すべてのノートンLifeLock の保護機能を、すべての地域で、またはすべてのパートナー様が使用できるわけではありません。

デバイスセキュリティ

メモ: すべてのプラットフォーム上ですべての機能が利用できるわけではありません。

メモ: 保護者機能、クラウドバックアップ、セーフカムは現在 macOS ではサポートされません。

Windows™ オペレーティングシステム

- Microsoft Windows® 10 (すべてのバージョン)
  - Microsoft Windows® 10 S モード (32 ビット/64 ビット/ARM32) バージョン 1803 以上
  - Microsoft Windows® 8/8.1 (すべてのバージョン)
    一部の保護機能は、Windows 8 のスタート画面から起動するブラウザではご利用いただけません。
  - Microsoft Windows® 7 (32 ビットおよび 64 ビット) Service Pack 1 (SP 1) 以降

  メモ: * ノートン アンチウイルス プラスは Windows 10 S モードに対応していません。

Mac® オペレーティングシステム

- ノートン製品バージョン 8.0 以降を搭載した Mac OS X 10.10.x 以降。

  メモ: ノートン ファミリーの保護者機能とクラウドバックアップは現在 MacOS ではサポートされません。

Android™ オペレーティングシステム

- Android 6.0 以降

  Google Play アプリがインストールされている必要があります。

  Google Play 上のアプリの自動スキャンは、Samsung 社製デバイスを除き、Android 4.1 以降で対応しています。Samsung 社製デバイスでは、Android 4.2 以降が実行されているデバイスに対応しています。以前のバージョンの Android をお使いの場合、Google Play 上のアプリをスキャンするには、Google Play の「共有」機能を使用する必要があります。

iOS オペレーティングシステム

- Apple iOS の現在と以前の 2 つのバージョンを実行する iPhone または iPad

ノートン™ セキュア VPN のシステム要件

Windows™ パソコン、Mac®、iOS、Android™ デバイスで利用可能:

ノートン セキュア VPN は、パソコン、Mac、Android スマートフォンおよびタブレット、iPad、iPhone と互換性があります。ノートン セキュア VPN は指定した数のデバイスで使用できます。有効期間中に使用制限はありません。

Windows™ オペレーティングシステム

- Microsoft Windows® 10 (Windows 10 S を除くすべてのバージョン)
  - Microsoft Windows® 8/8.1 (すべてのバージョン)
  - Microsoft Windows® 7 (32 ビットおよび 64 ビット) Service Pack 1 (SP 1) 以降

  150 MB の空きハードディスク容量。

Mac® オペレーティングシステム

- Mac OS の最新バージョンと 2 つ前までのバージョン。

  300 MB 以上のハードディスク容量。

Android™ オペレーティングシステム

- Android 6.0 以降

  Google Play アプリがインストールされている必要があります。

iOS オペレーティングシステム

- Apple iOS の現在と以前の 2 つのバージョンを実行する iPhone または iPad

ノートンLifeLock アカウントへのアクセス

ノートンLifeLock アカウントから、製品のライセンスの詳細を管理したり、プロダクトキーを見つけたり、ライセンスの延長をアクティブ化したり、その他のサービスにアクセスしたりできます。

アカウントへのアクセス

1. my.Norton.com にアクセスし、[サインイン]をクリックします。
2. ユーザー名/電子メールアドレスとパスワードを入力し、[サインイン]をクリックします。
3. パスワードを忘れた場合は、[パスワードを忘れた場合]をクリックし、電子メールアドレスを入力します。

失敗したログインの試行回数が多すぎるためアカウントが一時的に遮断されているというメッセージが表示される場合は、1 時間待ってからもう一度サインインを試すことを推奨します。

2

保護の設定

この章では以下の項目について説明しています。

- デバイスセキュリティの設定
- ノートン パスワード マネージャーの設定
- クラウドバックアップを設定する
- LifeLock™ 個人情報盗難保護のセットアップ
- セキュア VPN の設定
- 保護者機能の設定
- ノートン セーフウェブを使用した銀行情報の保護

デバイスセキュリティの設定

デバイスを保護するには、ノートン デバイスセキュリティをインストールする必要があります。ノートン デバイスセキュリティは、Windows デスクトップパソコン/ノートパソコン、Mac パソコン、Android および iOS を搭載したモバイルデバイスにインストールできます。

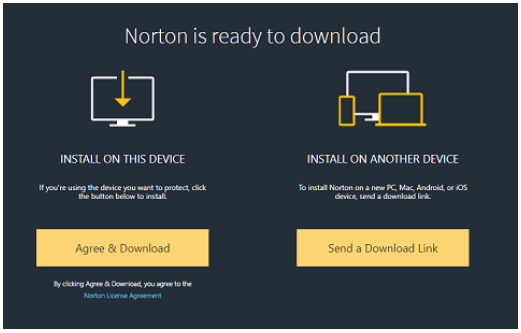
デバイスセキュリティのダウンロードとインストール

1 各パソコン、ラップトップ、スマートフォンでブラウザを開き、次の URL を入力します。

https://norton.com/setup

2 ノートンLifeLock アカウントにサインインします。

3 [ノートンの設定]ウィンドウで[同意してダウンロード]をクリックします。



4 画面の矢印で示されている領域をクリックして、画面に表示される指示に従います。

サービスが自動的にダウンロード、インストール、アクティブ化されます。

メモ: ダウンロードが完了しなかった場合、またはサービスのダウンロード時にエラーが発生した場合は、ダウンロードを再び開始できます。

ノートン パスワード マネージャーの設定

デバイスセキュリティをインストールすると、ブラウザ拡張機能を追加するように指示されます。この機能を動作させるには、Internet Explorer、FireFox、Chrome の各ブラウザに拡張機能をインストールする必要があります。

ブラウザ固有のすべての機能にアクセスするには、ノートンのブラウザ拡張機能を有効にする必要があります。ノートンのブラウザ拡張機能に含まれる内容:

ノートン セーフウェブ	オンラインで安全にネットサーフィン、検索、ショッピングができる安全な検索機能。ノートン セーフウェブは、ユーザーがアクセスする Web サイトを分析して、ウイルス、スパイウェア、マルウェア、またはその他の脅威を検出します。
ノートン セーフサーチ	Ask.com および Yahoo! を使用する安全な検索エンジンによって検索結果が生成されます。ノートン セーフサーチは、サイトの安全性状態とノートン評価に基づいて検索結果をランク表示します。
ノートン ホームページ	ノートン セーフサーチ機能を使用して Web 検索機能を拡張する Web サイト。生成されたそれぞれの検索結果にサイトの安全性状態とノートン評価を表示します。

ノートン パスワード マネージャー	ログイン情報、個人情報、金融情報などのさまざまな重要情報を保存できる安全な場所。保存した情報は、Web サイトへのログイン時、オンラインフォームやオンライン支払いの自動入力で使うことができます。

Internet Explorer

Internet Explorer にノートンのブラウザ拡張機能を追加する

1. ノートンを初めてインストールすると、新しい Internet Explorer セッションを開始したときに新しいウィンドウで[ブラウザ保護]ページが自動的に開きます。
2. [ブラウザ保護]ページで、[ノートン セキュリティツールバー]の[有効にする]オプションをクリックします。
3. 表示された拡張機能のポップアップで[拡張機能を追加する]をクリックします。
4. ノートン セキュリティツールバーを有効にした後に、ブラウザでノートン セーフサーチ拡張機能、ノートン ホームページ拡張機能、ノートン パスワード マネージャー拡張機能を有効にできます。

   [クリックして追加]オプションを使って、画面上の指示に従ってこれらの機能を有効にできます。
5. いずれの拡張機能もインストールしなかった場合、1 週間後以降に Internet Explorer を起動すると[Internet Explorer の保護の警告]という通知が表示されます。

   [今すぐインストール]をクリックして、画面上の指示に従って拡張機能をインストールします。

メモ: ノートン拡張機能を後で有効にする場合は、[後で通知する]をクリックします。この通知警告が表示されないようにするには、[今後確認しない]をクリックします。

Google Chrome

Google Chrome にノートンのブラウザ拡張機能を追加する

メモ: Google Chrome のブラウザ拡張機能をインストールするには、最新バージョンのノートン 360 が必要です。最新バージョンではない場合は、ノートン製品でライブアップデートを実行してください。シマンテック社は Google Chrome ブラウザに次の拡張機能を提供します。

- ノートン セーフウェブ
- ノートン パスワード マネージャー
- ノートン セーフサーチ
- ノートン ホームページ

Chrome のブラウザ拡張機能のインストール手順を次に示します。

1 デバイスセキュリティを初めてインストールすると、新しい Google Chrome セッションを開始したときに新しいウィンドウで[ブラウザ保護]ページが自動的に開きます。

[ブラウザ保護]ページは、[インターネットセキュリティ]メニューの[今すぐ設定]オプションをクリックして起動することもできます。

2 [ブラウザ保護]ページで、[ノートン セーフウェブ]の[クリックして追加]オプションをクリックします。

3 表示された拡張機能のポップアップで[拡張機能を追加する]をクリックします。

4 ノートン セーフウェブを有効にした後に、ブラウザでノートン セーフサーチ、ノートン ホームページ、ノートン パスワード マネージャーの各拡張機能を有効にできます。[クリックして追加]オプションを使用して、画面上の指示に従ってこれらの拡張機能を有効にできます。

Google Chrome ですべてのノートン拡張機能を有効にするには、[ノートンのすべての拡張機能を無料で追加]をクリックして画面上の指示に従います。

- ノートン セーフウェブ拡張機能をインストールしなかった場合、1 週間後に Google Chrome を起動すると[Chrome の保護が削除されました]という警告通知が表示されます。
- いずれの拡張機能もインストールしなかった場合、1 週間後に Google Chrome を起動すると[Google Chrome の保護の警告]という通知が表示されます。

5 [今すぐインストール]をクリックして、画面上の指示に従って拡張機能をインストールします。

メモ: ノートン拡張機能を後で有効にする場合は、[後で通知する]をクリックします。この通知警告が表示されないようにするには、[今後このメッセージを表示しない]をクリックします。

Mozilla Firefox

Mozilla Firefox にノートンのブラウザ機能を追加する

メモ: Mozilla Firefox の Web ベースのスタンドアロンのブラウザ拡張機能をインストールするには、最新バージョンのノートン 360 が必要です。最新バージョンではない場合は、ノートン製品でライブアップデートを実行してください。シマンテック社は Firefox ブラウザに次の拡張機能を提供します。

- ノートン セーフウェブ
- ノートン セーフサーチ
- ノートン ホームページ
- ノートン パスワード マネージャー

Firefox のブラウザ拡張機能のインストールまたはアップグレードの手順を次に示します。

1 デバイスセキュリティを初めてインストールすると、新しい Mozilla Firefox セッションを開始したときに新規ウィンドウまたはタブで[ブラウザ保護]ページが自動的に開きます。

ノートン デバイスセキュリティのアップグレードが完了していたら、[ブラウザ保護]警告ウィンドウで[OK]をクリックし、拡張機能のページをクリックします。

メモ: [ブラウザ保護]ページは、[インターネットセキュリティ]メニューの[今すぐ設定]オプションをクリックして起動することもできます。

2 [ブラウザ保護]ページで、[ノートン セーフウェブ]の[有効にする]オプションをクリックします。

3 表示された拡張機能のポップアップで[許可]をクリックします。

ノートン セーフウェブを有効にした後に、ブラウザでノートン セーフサーチ機能、ノートン ホームページ機能、ノートン パスワード マネージャー機能を有効にできます。[有効にする]オプションを使用して、画面上の指示に従ってこれらの機能を有効にできます。

Firefox ですべてのノートン拡張機能を有効にするには、[ノートンのすべての拡張機能を無料で追加]をクリックして画面上の指示に従います。

拡張機能をインストールしなかった場合、1 週間後に Firefox を起動すると[Firefox の保護の警告]という警告通知が表示されます。ノートン拡張機能を後で有効にする場合は、[後で通知する]をクリックします。この通知警告が表示されないようにするには、[今後このメッセージを表示しない]をクリックします。[後で通知する]を選択した場合、1 週間後に Firefox で保護警告通知が表示されます。通知から[今すぐインストール]オプションをクリックして、画面上の指示に従って拡張機能をインストールします。

Microsoft Edge

Microsoft Edge にノートンのブラウザ拡張機能を追加する

メモ: ノートン パスワード マネージャーは独立した拡張機能です。Microsoft Edge ブラウザでノートン製品をインストールする必要はありません。この拡張機能は Windows 10 Creators Update 以降のバージョンを実行しているパソコンのみと互換性があります。

1 Microsoft Edge ブラウザを起動します。

2 右上隅にある[...]ボタンをクリックして[拡張機能]を選択します。

3 [拡張機能]ウィンドウで[ストアから拡張機能を取得する]をクリックします。

4 [ストア]ウィンドウの検索ボックスに「ノートン」と入力して、検索結果に表示された[ノートン パスワード マネージャー]をクリックします。

5 インストール先を選択して[続ける]をクリックし、[インストール]をクリックします。

拡張機能をインストールしたら[起動]をクリックします。

6 [新しい拡張機能があります]ポップアップウィンドウで[有効にする]をクリックします。

7 アドレスバーにノートン パスワード マネージャーのアイコンを表示するには、ブラウザの右上隅にある[...]ボタンをクリックして[拡張機能]をクリックします。

8 [拡張機能]ウィンドウで[ノートン パスワード マネージャー]を選択します。

9 [ノートン パスワード マネージャー]ウィンドウの[アドレスバーの横にボタンを表示する]でスライダーを[オン]に移動します。

Chromium に基づく Microsoft Edge 向けのブラウザ拡張機能

Microsoft 社は、Chromium オープンソースプロジェクトに基づく新しいバージョンの Microsoft Edge をリリースしました。ノートンは Microsoft Edge ストアで、この新しいバージョンのブラウザに次のブラウザ拡張機能を提供します。

- ノートン パスワード マネージャー - パスワード、クレジットカード情報、その他の重要なオンライン情報を、より安全に作成、保管、管理するのにかかせないツールを提供します
- ノートン セーフウェブ - ウェブの閲覧中にオンラインの脅威から保護します。

この拡張機能は、Windows と Mac の両方のプラットフォームで利用できます。

Microsoft Edge にノートン セーフウェブ拡張機能を追加する

1 Microsoft Edge ブラウザを起動します。

2 Microsoft Edge Addons ページで、ノートン セーフウェブ拡張機能ページを開きます。

メモ: ノートン パスワード マネージャーの拡張機能がすでにインストールされているかを確認するには、設定アイコンをクリックして[拡張機能]をクリックします。[拡張機能]ページで、[ノートン セーフウェブ]スライダーを移動して拡張機能を有効にします。

3 ノートン セーフウェブ拡張機能ページで、[インストール]をクリックします。

4 [Add "Norton Safe Web" to Microsoft Edge]通知ポップアップで、[Add extension]をクリックし、ノートン セーフウェブ拡張機能をインストールします。

Microsoft Edge にノートン パスワード マネージャー拡張機能を追加する

1 Microsoft Edge ブラウザを起動します。

2 Microsoft Edge Addons ページで、ノートン パスワード マネージャー拡張機能を開きます。

メモ: ノートン パスワード マネージャーの拡張機能がすでにインストールされているかを確認するには、設定アイコンをクリックして[拡張機能]をクリックします。[拡張機能]ページで、[ノートン パスワード マネージャー]スライダーを移動して拡張機能を有効にします。

3 ノートン パスワード マネージャー拡張機能ページで、[インストール]をクリックします。

4 [Add "Norton Password Manager" to Microsoft Edge]通知で、[Add extension]をクリックし、ノートン パスワード マネージャー拡張機能をインストールします。

クラウドバックアップを設定する

クラウドバックアップは、ランサムウェアやマルウェアによって、またはパソコンのハードウェアに発生した重大な問題によって、データを失わないようにするための予防策として機能します。ライセンスにより、指定した容量のノートン クラウドバックアップ領域を利用できます。クラウドストレージの空きボリュームは購入したライセンスによって異なります。

メモ: ノートン クラウドバックアップの機能は、Windows でのみ利用できます。

最初のバックアップを実行する前に、クラウドバックアップをアクティブ化する必要があります。

メモ: クラウドバックアップを使用するには、[ファイアウォールの設定]ウィンドウの[データ通信ポリシー]オプションを[無制限]に設定する必要があります。

[クラウドバックアップ]のアクティブ化

1 ノートンを起動します。

2 [マイノートン]ウィンドウで、[クラウドバックアップ]の横にある[設定する]をクリックします。

3 表示されるウィンドウで[バックアップのアクティブ化]をクリックします。

4 サインイン画面が表示されたら、ノートンLifeLockアカウントの電子メールアドレスとパスワードを入力し、[サインイン]をクリックします。

5 [完了]をクリックします。

LifeLock™ 個人情報盗難保護のセットアップ

LifeLock とノートンが 1 つの企業で協力体制を築くことにより、お客様の ID を保護します。

次の個人情報を LifeLock に追加して監視できます†。

- 運転免許証番号
- 住基ネット個人 ID、生年月日、母親の旧姓
- 5 件までの保険証券番号
- 5 件までの住所
- 5 件までの電話番号

- 10 件までの銀行口座番号
- 10 件までのクレジットカード番号*

電話番号、電子メールアドレス、銀行口座番号などの情報を追加して監視できます。

LifeLock Identity Alert System により、お客様の ID が何者かによって使用された際は警告†されます。このような犯罪者は、お客様の名前に関連付けられた携帯電話のアカウントや自動車ローンの情報を盗み取ろうとしています。

メモ: LifeLock™ 個人情報盗難保護は、事業を対象とするものではありません。当社の技術とサービスは、住基ネット個人 ID やその他の個人を特定できる情報で個人を保護するように設計されています (これらは事業に関連するものではありません)。

* Visa、MasterCard、American Express、Discover などの主要なクレジットカードを追加できます。ただし現時点で、その他の種類のカード (小売業者向けのカードやギフトカードなど) はサポートしていません。

すべての ID 情報の盗難やサイバー犯罪を防ぐことのできる人はいません。

†LifeLock はすべての事業におけるすべてのトランザクションを監視するわけではありません。

LifeLock™ 個人情報盗難保護のセットアップ

1. ノートンを起動します。
2. [マイノートン]ウィンドウで、[個人情報盗難保護]の横にある[セットアップ]をクリックします。
3. [LifeLock メンバーログイン]ページで、[ノートンでサインイン]をクリックします。
4. アカウントの資格情報を入力し、サインインします。
5. 画面の指示に従って操作します。

Android への LifeLock for ノートン 360 アプリのインストール

1. お使いの Android デバイスで[Play ストア]アプリを起動し、LifeLock™ 個人情報盗難保護を検索します。
2. Play ストアでアプリのページが見つかったら、[インストール]をタップして、次に[同意]をタップします。
3. インストールが完了したらアプリを開き、アカウントの資格情報を使用してサインインします。

iOS への LifeLock for ノートン 360 アプリのインストール

1. お使いの iOS デバイスで[App Store]アプリを起動し、LifeLock™ 個人情報盗難保護を検索します。
2. App Store でアプリのページが見つかったら、[入手]をタップして、次に[インストール]をタップします。
3. インストールが完了したらアプリを開き、アカウントの資格情報を使用してサインインします。

ダークウェブモニタリング powered by LifeLock**

ダークウェブモニタリングとは?

シマンテック社は、見つけることが困難なダークウェブサイトやフォーラムで、お客様の個人情報が使用されていないかどうかを監視します。シマンテック社がダークウェブでお客様の情報を検出した場合、お客様に通知します。

監視が重要である理由

ID 情報窃盗犯は、見つけることが困難なダークウェブサイトやフォーラムで、お客様の個人情報を売買している可能性があります。

対策方法

通知にお客様の情報が記載されている場合、次の対策をとるようにしてください。

- デビットカードまたはクレジットカードの侵害: カードを使用停止にした場合は、それ以上のアクションは必要ありません。その口座が現在も使用中であれば、デビットカード会社またはクレジットカード会社に連絡して新しいカードを申請してください。利用明細を詳しく確認してください。
- 電子メールの侵害: 現在の電子メールのパスワードを変更してください。別のアカウントでも同じパスワードを使用している場合は、それらも変更してください。問題が解決しない場合は、新しい電子メールアカウントを作成することも検討します。パスワードを 30 日ごとに変更すると、アカウントの安全性を高めることができます。
- 住基ネット個人 ID の侵害: ID の保護を強化するため、主な 3 つの信用情報機関の 1 つで詐欺警告を設定することを推奨します。
- 名前、住所、電話番号の侵害: これらの情報の流出の場合、より大きなダメージを招く可能性がある情報 (住基ネット個人 ID など) は共有されていないはずです。しかし、何らかの個人情報が漏えいしている可能性があるため、クレジットレポートに不一致がないかをよく確認してください。

シマンテック社は引き続きお客様の個人情報をダークウェブ上で監視します**。お客様の情報を検出した場合、シマンテック社はさらに電子メールを送信します。

メモ: ID 情報の盗難を完全に防ぐことはできません。

** ノートン 360 のダークウェブモニタリングプランは、デフォルトでは電子メールアドレスのみを監視します。監視を目的とするその他の情報を追加できるかを確認するには、ポータルにログインしてください。

セキュア VPN の設定

フリー Wi-Fi は、空港、カフェ、ショッピングモール、ホテルなど多くの場所で提供されています。提供場所も多く便利なため、ユーザーはあまり深く考えずにこうした無料の「ホットスポット」に接続してしまう可能性があります。しかし、メール閲覧や銀行口座の確認、ログインを伴うあらゆるオンライン活動を行う際に、フリー Wi-Fi の使用はリスクを伴います。フリー Wi-Fi を利用すると、第三者にオンラ

イン活動を監視されるおそれがあります。サイバー犯罪者は、ユーザー名、パスワード、場所、チャット、電子メール、口座番号などの個人情報を盗む可能性があります。

セキュア VPN によって、フリー Wi-Fi の使用時に接続を保護できます。これにより、お客様の重要なデータを暗号化する仮想プライベートネットワーク (VPN) が構築されます。

セキュア VPN は、フリー Wi-Fi 経由で送受信するデータを保護し、次のような状況で役立ちます。

- 銀行間通信レベルの強固な暗号化によって、フリー Wi-Fi ホットスポット経由で接続する際でもデータを保護します。
- Web サイトを匿名で閲覧できるので、オンラインプライバシーが保護されます。
- 外出先のどこからでも、お気に入りのアプリやコンテンツに自宅と同じようにアクセスできます。
- ログを記録しない仮想プライベートネットワーク (VPN) でデータを暗号化するため、システム側でオンライン活動が追跡されたりログが保管されることはありません。
- 個人向けオンラインセキュリティ分野をリードするノートンLifeLock の、世界トップクラスのカスタマーサポートを利用できます。

メモ: セキュア VPN の機能は一部のライセンスで利用できます。

次の手順に従って、セキュア VPN を設定します。

セキュア VPN の設定

1. ノートンを起動します。
2. [マイノートン]ウィンドウで、[セキュア VPN]の横にある[セットアップ]をクリックします。
3. Web ページが表示されたら、[サインインする]をクリックします。
4. アカウントの資格情報を入力し、サインインします。
5. ダウンロード画面が表示されたら、[ダウンロード]をクリックします。
6. 画面の指示に従って操作します。

ノートン コミュニティを利用すると、他のデスクトップユーザーとのディスカッションに参加できます。

保護者機能の設定

これで、お子様が安全にインターネットを楽しむことができるように保護者機能をセットアップできます。これは 3 つの手順のみの簡単な作業です。

保護者機能は、インターネット上の危険や不適切なコンテンツから家族のオンライン活動を保護するために必要な機能を提供します。機密性の高い情報がオンラインに流出しないようにするのにも役立ちます。

ノートンLifeLock アカウントにサインインする

1 ノートンを起動します。

2 [マイノートン]ウィンドウで、[保護者機能]の横にある[セットアップ]をクリックします。

3 サインインのメッセージが表示されたら、アカウントの資格情報を入力してサインインします。

4 表示されたページで、[家族]タブをクリックします。

5 利用規約をお読みのうえ、[同意して続行]をクリックしてご家族用に設定してください。

6 画面の指示に従って操作します。

お子様をアカウントに追加する

お子様を追加すると、保護者機能によってそれぞれのお子様の年齢に基づいた定義済みの家族ルールが適用されます。家族ルールは、それぞれのお子様の成熟レベルに合わせていつでもカスタマイズできます。

メモ: アカウントには、お子様を 15 人まで追加できます。お子様をいつでもノートン ファミリーアカウントに追加したりノートン ファミリーアカウントから削除したりできます。

---

1 [お子様の名前]ボックスにお子様の名前を入力します。

メモ: 名前には、&、#、$ などの特殊文字を使うことができません。

---

2 お子様の生年を選択します。

家族ルールは、お子様の年齢に基づいて適用されます。

3 [アバターを選択する]または[写真をアップロードする]を選択して、お子様のプロファイル画像を設定します。

メモ: 最初のお子様の設定が完了した後、アカウントに別のお子様を追加できます。

---

4 [次へ]をクリックします。

子供のデバイスにノートン ファミリーをインストールする

お子様が使用するすべてのデバイスにノートン ファミリーをインストールします。お子様のデバイス上で操作していない場合は、[いいえ]をクリックして、電子メールでダウンロードリンクを送信します。ノートン ファミリーをインストールするデバイスでこの電子メールを開きます。

Windows パソコンにノートン ファミリーをインストールするには

1 [お子様がこのデバイスを使いますか?]という質問に、[はい]をクリックし、[次へ]をクリックします。

2 ダウンロードされたインストーラファイルをクリックするか、または実行します。

3 ノートン ダウンロードマネージャは、デバイスにノートン ファミリーを自動的にインストールします。

4 ユーザー使用許諾契約を読んでから、[同意してインストール]をクリックします。

デバイスが自動的にアカウントにリンクされます。

5 [続行]をクリックします。

6 [デバイスを割り当てる]ウィンドウで、このデバイスを割り当てるお子様の隣の[編集]をクリックします。

7 [指定してサインイン]をクリックして、このデバイスにログオンするのにお子様が使用するアカウントを選択します。お子様が複数のユーザーアカウントを使う場合は、すべてのユーザーアカウントでお子様を選択します。

8 [保存] > [OK]の順にクリックします。

Android にノートン ファミリーアプリをインストールするには

1 [ノートン ファミリーのインストール]ウィンドウで、[はい]をタップし、[続行]をタップします。

2 [ノートン ファミリーアプリのダウンロード]をタップします。

3 メッセージが表示されたら、[Play ストア]を使って操作を完了します。

4 [インストール]をタップして、画面の指示に従います。

5 ノートン ファミリーの保護者機能アプリを開きます。

6 [ノートン製品使用許諾契約]を読んで、[同意して続行]、[開始する]の順にタップします。

7 [サインイン]をクリックし、アカウント資格情報を入力します。

8 [子供]をタップして子供モードに入り、[続行]をタップします。

子供モードでは、このデバイスにお子様を追加して家族ルールを割り当てられます。

9 お子様を追加するには、[子供の追加]をタップし、[プロファイル]ウィンドウでお子様の詳細を入力します。

アバターをタップして、子供のプロファイル用のアバターを選択します。子供のプロファイル用にギャラリーからイメージを選択することも、インスタント写真を撮ることもできます。

10 [続行]をタップし、次に[保存]をタップします。

ノートン ファミリーでは、お子様の生まれた年に基づいてデフォルトの家族ルールが適用されます。[家族ルール]をタップしてお子様に割り当てられたルールを確認できます。

11 このデバイスを割り当てるお子様を選択し、このデバイスを識別するための名前を入力し、[完了]をタップします。

12 メッセージが表示されたら、[アプリの使用状況]と[アクセシビリティ]オプションをオンにします。

13 警告が表示されたら、[アクティブ化]をタップし、デバイスの管理者としてノートン ファミリーを設定します。

iOS にノートン ファミリーアプリをインストールするには

1 [ノートン ファミリーのインストール]ウィンドウで、[はい]をタップし、[続行]をタップします。

2 [ノートン ファミリーアプリのダウンロード]をタップします。

3 [ノートン ファミリー]アプリケーションをタップしてインストールします。

4 [開く]をタップします。

5 [OK]をタップして、ノートン ファミリーによる通知の送信を許可します。

6 ノートン使用許諾契約とプライバシーポリシーを読んで、[同意して続行]をタップします。

7 アカウント資格情報でサインインします。

8 [子供の追加]画面でお子様の詳細を入力して、[追加]をタップします。

別のお子様を追加するには、[新しい子供を追加する]をタップし、[子供の追加]ウィンドウでお子様の詳細を入力してから[追加]をタップします。

アバターをタップして、子供のプロファイル用のアバターを選択します。子供のプロファイル用にギャラリーからイメージを選択することも、インスタント写真を撮ることもできます。

9 このデバイスを割り当てるお子様を選択し、このデバイスを識別するための名前を入力します。

10 [割り当てる]をタップします。

11 [インストール]をタップし、画面の指示に従ってプロファイルをインストールします。

お子様のデバイスでインスタントロックやその他の機能を使用するには、プロファイルをインストールする必要があります。

12 画面の指示に従って、制限を設定します。

親のデバイスにノートン ファミリーをインストールする

セットアップが完了したら、デバイスに次のモバイルアプリをダウンロードしてインストールする必要があります。

- Android デバイス: [ノートン ファミリー保護者機能]アプリ
- iOS デバイス: [保護者用ノートン ファミリー]アプリ

Android に[ノートン ファミリー保護者機能]アプリをダウンロードしてインストールする

1 [Play ストア]アプリを開き、ノートン ファミリー保護者機能を検索します。

2 [ノートン ファミリー保護者機能]アプリを選択し、[インストール]をタップします。

3 インストールが完了したら、アプリを開きます。

4 ノートン製品使用許諾契約とその他のポリシーを読んで、[続行]をタップします。

5 アカウント資格情報でサインインします。

6 [保護者デバイス]をタップします。デバイスをお子様と共有する場合は、お子様にデバイスを手渡す前に子供モードに切り替えてください。

iOS に[保護者用ノートン ファミリー]アプリをダウンロードしてインストールする

1 [App Store]アプリを開き、保護者用ノートン ファミリーを検索します。

2 保護者用ノートン ファミリーを選択し、[入手]をタップします。

3 インストールが完了したら、アプリを開きます。

4 ノートン製品使用許諾契約とその他のポリシーを読んで、[続行]をタップします。

5 アカウント資格情報でサインインします。

家族で相談する

コミュニケーションを取ることは、家族のオンライン活動を保護するうえで重要です。話し合いの場を設け、インターネットを適切に使うことの重要性についてお子様に説明してください。

ノートン セーフウェブを使用した銀行情報の保護

銀行取引 Web サイトでの取引の際に、ノートン セーフウェブを使用するとセキュリティを強化できます。Google Chrome、Mozilla Firefox、または Microsoft Edge ブラウザを使用して銀行取引 Web サイトにアクセスすると、ノートン セーフウェブ拡張機能をインストールまたは有効にする通知が表示されます。通知の[インストール]または[有効にする]をクリックして、画面上の指示に従ってノートン セーフウェブ拡張機能をインストールまたは有効化します。

通知の[今後この画面を表示しない]をクリックするか、[設定]ウィンドウに移動して、銀行取引保護通知の警告をオフにすることができます。

銀行取引保護通知のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [侵入とブラウザの保護]タブの[銀行取引保護通知]行で、[オン/オフ]スライダーを[オフ]または[オン]に移動します。

5 [設定]ウィンドウで、[適用]をクリックしてから[閉じる]をクリックします。

3

デバイスセキュリティの管理

この章では以下の項目について説明しています。

- デバイスがリスクにさらされているときに実行するべき内容
- ノートンを使用してパソコンのパフォーマンスを最適化し、改善する
- パソコンに脅威があるかどうかを確認するためにノートンのスキャンを実行する
- デバイスをエクスプロイト、ハッカー、ゼロデイ攻撃から保護
- アプリケーションを監視し、悪質な Web サイトからのパソコンへのアクセスを遮断するようにノートンを設定する
- ノートン クラウドバックアップを初めて使用する
- ノートン製品の設定のカスタマイズ
- ゲーム オプティマイザーでパソコンをゲーム用に最適化する

デバイスがリスクにさらされているときに実行するべき内容

ノートンのメインウィンドウで、[セキュリティ]、[インターネットセキュリティ]、[バックアップ]、[パフォーマンス]タイルの色により、次のように、各カテゴリの状態がわかります。

- 緑: 保護されています。
- オレンジ: パソコンは注意が必要です。
- 赤: パソコンは危険な状態です。

メモ: バックアップカテゴリを利用できるのは、デラックス、プレミアム、ノートン 360 のライセンスがある場合のみです。

保護またはシステムパフォーマンスの低下を招くほとんどの問題は、ノートンで自動的に解決され、メインウィンドウの状態が[保護]として表示されます。注意する必要がある問題は[リスクあり]または[注意]として表示されます。

[注意]または[リスクを伴う]の状態インジケータに対応する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[リスクを伴う]または[注意]を示しているカテゴリ内の赤いタイルまたはオレンジのタイルをクリックします。

3 [今すぐ解決]をクリックして画面上の指示に従います。

それでも問題が解決しない場合は、[ヘルプ] > [サポート情報]をクリックして、診断ツールを実行します。

パソコンに重大な感染が発生している可能性がある場合は、ノートン レスキューツールを使用することもできます。

ライブアップデートの実行

ノートンLifeLock 社は、次のような場合にライブアップデートを定期的に実行することを推奨します。

- [自動ライブアップデート]をオフにしている場合
- パソコンが長時間インターネットに接続されていない場合

メモ: ライブアップデートを実行するには、ライセンスとインターネット接続が必要です。

ライブアップデートを手動で実行する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで、[セキュリティ]をダブルクリックしてから[ライブアップデート]をクリックします。

3 [ノートン ライブアップデート]ウィンドウで、ライブアップデートが正常に完了したら、[OK]をクリックします。

ノートンが検出したデバイスのセキュリティリスクを表示し、修正する

ノートンがセキュリティリスクを検出したときに、リスクの解決方法に関するユーザーからの指示が不要な場合、そのリスクは自動的に削除されます。指示が必要な場合は、[脅威を検出しました]警告またはセキュリティリスク警告が表示され、そのセキュリティリスクへの対応方法が提案されます。

スキャン中に自動的に解決されたリスクを表示する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで[解決したセキュリティリスク]を選択します。

4 リストでリスクを選択し、[詳細]ウィンドウで、実行した処理を表示します。

スキャン中に検出された未解決のリスクを解決する

場合によっては、ノートンで自動的にリスクを解決できないことがありますが、リスクを解決するために実行する必要がある処理が推奨されます。

スキャン中に検出された未解決のリスクを解決する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで[未解決のセキュリティリスク]を選択します。

4 未解決のリスクが表示される場合は、リストでリスクを選択します。

5 [詳細]ペインの[推奨する処理]に従います。

メモ: ノートンがセキュリティリスクを削除した後で、パソコンの再起動が必要になることがあります。パソコンの再起動を求めるメッセージが表示されたら、開いているファイルを保存してからパソコンを再起動する必要があります。

メモ: システムが感染していると思う場合はノートン パワーイレイサーを実行します。ノートン パワーイレイサーは、削除が困難なセキュリティリスクを除去する強力なマルウェア駆除ツールです。詳しくは、p.31 の「パソコンに脅威があるかどうかを確認するためにノートンのスキャンを実行する」を参照してください。

検疫済みのリスクまたは脅威を処理する

検疫項目はパソコンの他の部分から隔離されているため、感染が広がったりパソコンに感染する可能性はありません。ノートン製品ではリスクと識別されないものの、感染していると考えられる項目がある場合は、項目を検疫に手動で入れることができます。項目のリスクが低いと考えられる場合は、検疫から項目を復元することもできます。ノートンは復元された項目を修復しません。ただし、ノートンは復元された項目を後続のスキャンで駆除できます。

検疫から項目を復元する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで[検疫]カテゴリを選択します。

4 管理する項目を選択します。

5 [詳細]ペインで[オプション]をクリックします。

[その他のオプション]リンクを使って、項目に対する処理を選択する前にその項目についての詳細を表示できます。このリンクで、リスクに関する詳しい情報を含む[ファイルインサイト]ウィンドウが開きます。

6 [脅威が検出されました]ウィンドウで次のいずれかのオプションを選択します。

- [復元する]: 項目をパソコンの元の場所に戻します。このオプションは手動で検疫した項目に対してのみ利用できます。
- [復元してこのファイルを除外する]: 項目を修復せずに元の場所に戻し、今後のスキャンでこの項目が検出されないように除外します。このオプションは検出されたウイルス性脅威と非ウイルス性脅威に対して利用できます。
- [履歴から削除する]: 選択した項目を[セキュリティ履歴]ログから削除します。

7 復元する場合は、[検疫の復元]ウィンドウで[はい]をクリックします。

8 [フォルダの参照]ダイアログボックスで、ファイルの復元先のフォルダまたはドライブを選択し、[OK]をクリックします。

誤ってセキュリティリスクであると識別されたファイルを復元する

デフォルトでは、ノートンはパソコンからセキュリティリスクを削除して検疫します。ファイルが誤って削除されたと思う場合は、ファイルを検疫から元の場所に戻して今後のスキャンから除外できます。

検疫からファイルを復元する

メモ: プログラムは安全であると確信する場合にのみノートンのスキャンからプログラムを除外します。たとえば、別のプログラムが機能するのにセキュリティリスクプログラムを使う場合には、パソコンにそのプログラムを残すことにする場合があります。

---

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]、[履歴]の順にクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンメニューで[検疫]を選択します。

4 復元したいファイルを選択します。

5 [詳細]ペインで[オプション]をクリックします。

6 [脅威が検出されました]ウィンドウで[このファイルを復元して除外]をクリックします。

7 [検疫の復元]ウィンドウで[はい]をクリックします。

8 [フォルダの参照]ダイアログボックスで、ファイルの復元先のフォルダまたはドライブを選択し、[OK]をクリックします。

ノートンによる評価に項目を提出する

セキュリティリスクと考えられるファイルを提出することで、ノートン製品の有効性に貢献できます。ノートン セキュリティレスポンスがファイルを分析し、リスクである場合は、今後の保護定義に追加します。

メモ: 個人の身元を特定する情報が提出物に含まれることは決してありません。

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで[検疫]カテゴリを選択します。

4 管理する項目を選択します。

5 [詳細]ペインで[オプション]をクリックします。

[その他のオプション]リンクを使って、項目に対する処理を選択する前にその項目についての詳細を表示できます。このリンクで、リスクに関する詳しい情報を含む[ファイルインサイト]ウィンドウが開きます。

6 [脅威が検出されました]ウィンドウで、[ノートンLifeLock に提出する]をクリックします。

7 表示される画面で[OK]をクリックします。

項目を手動で検疫する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで[検疫]カテゴリを選択します。

4 [検疫に追加]をクリックします。

5 [手動検疫]ウィンドウで検疫するファイルを追加して、参照用に説明を入力します。

メモ: いずれかの実行中のプロセスに関連付けられているファイルを検疫した場合は、プロセスが終了されます。そのため、ファイルを検疫に追加する前に、開いているファイルと実行中のプロセスをすべて閉じてください。

ノートンを使用してパソコンのパフォーマンスを最適化し、改善する

パソコンの動作が遅くなり簡単なタスクに長い時間がかかると、いらいらするのはよくわかります。ユーザーの中には、ノートンをインストールしてからパソコンのパフォーマンスが落ちていると感じている方もいらっしゃいます。しかし、実際には、ノートンはパフォーマンスを損なうことなく世界レベルの保護を保証するよう合理化されています。

ノートンは、毎日の作業を高速化するパフォーマンス管理ツールと最適化ツールによって、お使いのパソコンの速度を加速することもできます。

パソコンの起動時間の高速化

多くのアプリケーションは、パソコンの起動時に設定されます。これには、使用しないプログラム、ほとんど使用しないプログラム、インストールされていることを知らなかったプログラムも含まれています。パソコンの起動時に立ち上げるプログラムが増えれば、かかる時間は長くなります。ノートン起動マネージャを使用すると、起動プログラムを無効にしたり延期したりして、迅速にパソコンを起動して実行できます。

起動項目を無効または延期する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[パフォーマンス]をダブルクリックしてから[起動マネージャ]をクリックします。

3 [起動マネージャ]ウィンドウで、次の内容を実行します。

- [オン/オフ]列で、使用しないプログラムのチェックマークをはずし、パソコンの起動時に開始されないようにします。
- [起動の延期]列で、起動完了後にのみロードしたいプログラムを選択します。

4 [適用]をクリックしてから[閉じる]をクリックします。

プログラムとファイルのロードにかかる時間の改善

ディスクの最適化ツールは、時間の経過とともにパソコンに広がるファイルの断片を再編集します。このツールによってパソコンのパフォーマンスが改善され、作業効率が向上します。

ディスクの最適化の実行

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[パフォーマンス]をダブルクリックしてから[ディスクの最適化]をクリックします。

3 完了したら[閉じる]をクリックします。

パソコンの動作を遅くする一時ファイルとフォルダを削除する

ファイルを閲覧したりダウンロードしたりするたびに、パソコンは一時ファイルを格納します。保存する必要がなくても、時間の経過とともに一時ファイルは蓄積され、パソコンの動作を遅くする可能性があります。ファイルのクリーンアップツールは、不要なファイルを削除して、パソコンの動作を高速化します。

一時ファイルとフォルダを削除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[パフォーマンス]をダブルクリックしてから[ファイルのクリーンアップ]をクリックします。

3 完了したら[閉じる]をクリックします。

ブートボリュームを最適化する

ブートボリュームの最適化では隣接し、連続するクラスタにファイルの断片を再整理することで、使用可能な空き領域が最大になります。ハードディスクのヘッドがファイルのすべてのデータに 1 カ所でアクセスすれば、メモリへのファイルの読み込みが高速になります。

ブートボリュームを最適化する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[パフォーマンス]をダブルクリックしてから[グラフ]をクリックします。

3 [グラフ]ウィンドウのセキュリティの状態グラフの上部で[最適化]をクリックします。

ゲームをしたり映画を視聴するときのパフォーマンスの改善

ゲームをしたり映画を視聴したりしているときにセキュリティソフトウェアが動作を開始して、最悪の場合で画面がフリーズしたことがありますか? 全画面表示の検出ツールを設定すると、中断を避けたいプログラムを実行しているときを識別できます。これによって、ユーザーを保護するバックグラウンドタスクの実行前に、該当のアプリでの作業が完了するまでノートンが待機します。

全画面表示の検出がオンになっていることを確認する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[管理の設定]をクリックします。

4 [サイレントモードの設定]の[全画面表示の検出]行で、スイッチを[オン]の位置に移動します。

5 [適用]をクリックしてから[閉じる]をクリックします。

お気に入りのアプリ使用時の中断の停止

お気に入りのプログラムの動作がノートンによって遅くなっていると考えられる場合、クワイエットモードによって、プログラム使用中、ノートンを実行しないように設定できます。これによって、ユーザーを保護するバックグラウンドタスク開始前に、これらのプログラムの使用完了までノートンが待機します。

お気に入りのプログラムのクワイエットモードでの実行

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[管理の設定]をクリックします。

4 [サイレントモードの設定]の[ユーザー指定のプログラム]行で、[設定]をクリックします。

5 [クワイエットモードプログラム]ウィンドウで[追加]をクリックします。

6 [プログラムを追加する]ダイアログボックスでそのプログラムまで移動します。

7 ファイルを選択して[開く]をクリックして、[OK]をクリックします。

リソースを消費して動作を遅くするプログラムの表示

ノートンは、パソコンを監視して、プログラムやプロセスが異常なリソース量を使用していると考えられる場合に警告します。それらのプログラムを使用していない場合は、シャットダウンしてパフォーマンスを改善できます。

リソースを消費するプロセスの特定

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[パフォーマンス]をダブルクリックしてから[グラフ]をクリックします。

3 [グラフ]ウィンドウの左ペインで[使用率]をクリックします。

4 次のいずれかの操作をします。

- CPU グラフを表示するには、[CPU]ページをクリックします。

- メモリグラフを表示するには、[メモリ]ページをクリックします。

5 グラフの任意の点をクリックして、リソースを消費するプロセスのリストを取得します。

プロセスの名前をクリックして、[ファイルインサイト]ウィンドウでプロセスについての追加の情報を取得します。

パソコンに脅威があるかどうかを確認するためにノートンのスキャンを実行する

ノートンでは、ウイルス定義を自動的に更新し、パソコン上のさまざまな脅威を定期的にスキャンします。パソコンをオフラインで使用していた場合や、ウイルスが存在することが疑われる場合は、以下の機能を手動で実行できます。

- クイックスキャン: 脅威に対して最も脆弱なパソコン上の領域を分析します。
- システムの完全スキャン: クイックスキャンで検出されるアプリケーション、ファイル、実行中のプロセスよりも脆弱性が低い、アプリケーション、ファイル、実行中のプロセスを含む、システム全体を分析します。
- カスタムスキャン 個別のファイル、フォルダまたはドライブがリスクにさらされていると疑われる場合に、これらを分析します。

メモ: ノートンをインストールした後の最初のスキャンは、システム全体を分析するため 1 時間以上かかる場合があります。

クイックスキャン、システムの完全スキャン、またはカスタムスキャンを実行する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。

3 [スキャン]ウィンドウの[スキャンとタスク]の横にある次のいずれかを選択します。

- [クイックスキャン] > [実行]
- [システムの完全スキャン] > [実行]
- [カスタムスキャン] > [実行]を選択した後、[ドライブスキャン]、[フォルダスキャン]または[ファイルスキャン]の横にある[実行]をクリックして、スキャンするコンポーネントに移動します。

4 [結果の概略]ウィンドウで[完了]をクリックします。

確認が必要な項目がある場合には[脅威を検出しました]ウィンドウでリスクを確認します。

システムの完全スキャン

システムの完全スキャンは、パソコンの詳細スキャンを実行し、ウイルスとその他のセキュリティの脅威を削除します。ユーザーがアクセスするすべてのブートレコード、ファイル、実行中のプロセスを検査します。パソコン全体がスキャンされるため、時間がかかります。

メモ: 管理者権限を持つユーザーがシステムの完全スキャンを実行すると、管理者権限を持っていないユーザーがスキャンを実行する場合よりも多くのファイルがスキャンされます。

システムの完全スキャンを実行する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。
3. [スキャン]ウィンドウの[スキャンとタスク]で[システムの完全スキャン]をクリックします。
4. [実行]をクリックします。

カスタムスキャン

場合によっては特定のファイル、リムーバブルドライブ、パソコンの任意のドライブ、パソコン上の任意のフォルダまたはファイルを個々にスキャンすると便利です。たとえば、リムーバブルメディアを使っていてウイルス感染の疑いがあるとき、その特定のディスクをスキャンできます。また、電子メールで圧縮ファイルを受信したときにウイルス感染の疑いがある場合には、その特定の要素をスキャンできます。

個々の要素をスキャンする

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。
3. [スキャン]ウィンドウの[スキャンとタスク]で、[カスタムスキャン]をクリックします。
4. [実行]をクリックします。
5. [スキャン]ウィンドウで次のいずれかの操作をします。
   - 特定のドライブをスキャンするには[ドライブスキャン]の横にある[実行]をクリックしてスキャンするドライブを選択し、[スキャン]をクリックします。
   - 特定のフォルダをスキャンするには[フォルダスキャン]の横にある[実行]をクリックしてスキャンするフォルダを選択し、[スキャン]をクリックします。

- 特定のファイルをスキャンするには[ファイルスキャン]の横にある[実行]をクリックしてスキャンするファイルを選択し、[追加]をクリックします。また、Ctrl キーを押しながらスキャン対象として複数のファイルを選択することもできます。

6 [結果の概略]ウィンドウで[完了]をクリックします。

確認が必要な項目がある場合には確認し、推奨する処理を行います。

ノートン パワーイレイサースキャン

ノートン パワーイレイサーは、削除が困難なセキュリティリスクの除去に役立つ強力なマルウェア駆除ツールです。ノートン パワーイレイサーでは、通常のスキャンプロセスよりさらに強力な技法が使われるため、正当なプログラムが削除対象としてフラグ付けされる危険性があります。ノートン パワーイレイサーを使ってファイルを削除する前に、スキャン結果を慎重に確認してください。

ノートン パワーイレイサーをダウンロードしてスキャンを実行する (Windows 10/8/7 の場合)

1 ノートン パワーイレイサーをダウンロードします。

2 ブラウザで Ctrl + J キーを押して、[ダウンロード]ウィンドウを開き、NPE.exe ファイルをダブルクリックします。

[ユーザーアカウント制御]ウィンドウが表示されたら、[はい]または[続行]をクリックします。

3 使用許諾契約を読み、[同意]をクリックします。

すでに使用許諾契約に同意している場合は、再度プロンプトが表示されることはありません。

ノートン パワーイレイサーは新しいバージョンの有無を調べ、新しいバージョンがある場合は自動でダウンロードします。

4 ノートン パワーイレイサーのウィンドウで、[システムの完全スキャン]を選択し、[今すぐ実行]をクリックします。

5 ルートキットスキャンを含める場合は、[設定]をクリックし、[スキャンとログの設定]で、[ルートキットスキャンを含める (コンピュータの再起動が必要)]オプションに切り替え、[適用]をクリックします。

6 パソコンの再起動を求めるメッセージが表示されたら、[再起動]をクリックします。

スキャンが完了するまで待ちます。画面の指示に従って操作します。

ノートン パワーイレイサーをダウンロードしてスキャンを実行する (Windows XP/Vista の場合)

1 ノートン パワーイレイサーをダウンロードします。

2 ブラウザで Ctrl + J キーを押して、[ダウンロード]ウィンドウを開き、NPE.exe ファイルをダブルクリックします。

[ユーザーアカウント制御]ウィンドウが表示されたら、[はい]または[続行]をクリックします。

3 使用許諾契約を読んで[同意]をクリックします。

ノートン パワーイレイサーは新しいバージョンの有無を調べ、新しいバージョンがある場合はダウンロードを促すメッセージを表示します。

4 [ノートン パワーイレイサー]ウィンドウで[リスクのスキャン]アイコンをクリックします。

5 デフォルトでは、ノートン パワーイレイサーによってルートキットスキャンが実行され、システムを再起動する必要があります。パソコンの再起動を求めるメッセージが表示されたら、[再起動]をクリックします。

ルートキットスキャンを含めない場合は、[設定]に移動し、[ルートキットスキャンを含める(パソコンの再起動が必要)]オプションのチェックマークをはずします。

6 スキャンが完了するまで待ちます。画面の指示に従って操作します。

独自にカスタムのノートンのスキャンを作成する

デフォルトのノートンの自動スキャン設定は、ほとんどのユーザーに適した設定ですが、選択したスケジュールで特定のドライブ、フォルダまたはファイルをスキャンするようオプションをカスタマイズすることもできます。

カスタムスキャンを作成する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。

3 [スキャン]ウィンドウの[スキャンとタスク]で、[カスタムスキャン]をクリックし、次に[実行]をクリックします。

4 [スキャン]ウィンドウで、[スキャンの作成]をクリックします。

5 [新しいスキャン]ウィンドウの[スキャン名]の横にカスタムスキャンの名前を入力し、次のように設定を追加します。

- [スキャン項目]タブで、[ドライブを追加する]、[フォルダを追加する]または[ファイルを追加する]をクリックし、スキャンに含めるコンポーネントに移動します。
- [定期スキャン]タブの[どのタイミングでスキャンを実行しますか?]で間隔を選択し、タイミングのオプションを選択します。
  [スキャンの実行]で、オプションを選択します。ほとんどのユーザーの場合、すべてのボックスをオンにしたままにすることを推奨します。このようにすると、パソコンを使用していないときや、バッテリ電源を使用していないときにだけスキャンが実行されるため、スキャン中にパソコンがスリープ状態になるのを防ぐことができます。
- [スキャンオプション]タブで、スイッチを移動して圧縮ファイルや危険度が低い脅威に対する動作をカスタマイズします。

6 [保存]をクリックします。

ノートン カスタムスキャンを編集または削除する

カスタムスキャンの名前の変更、ファイルの追加や削除、またはスケジュールの変更を行うために、作成したカスタムスキャンを編集できます。スキャンを実行する必要がなくなった場合は、削除できます。

カスタムスキャンを編集または削除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。

3 [スキャン]ウィンドウの[スキャンとタスク]で、[カスタムスキャン]をクリックし、次に[実行]をクリックします。

4 [スキャン]ウィンドウの[スキャンの編集]列で、修正したいカスタムスキャンの横で次のいずれかを行います。

- 編集アイコンをクリックし、[スキャンの編集]ウィンドウで、スイッチを移動してスキャンオプションをオンまたはオフにします。ほとんどのユーザーの場合、デフォルトの設定が適しています。[デフォルト設定を使う]をクリックして、カスタム設定を削除します。
- ごみ箱アイコンをクリックし、[はい]をクリックし、カスタムスキャンを削除します。

5 [保存]をクリックします。

ノートンのスキャンをスケジュール設定する

ノートンは、システム上の脅威を定期的に監視するために、ユーザーがパソコンから離れていることを検知すると自動的にスキャンを実行します。ユーザー独自のクイックスキャン、システムの完全スキャン、またはカスタムスキャンのスケジュールを設定し、選択した時間に実行することもできます。

ノートン クイックスキャン、システムの完全スキャン、またはカスタムスキャンのスケジュールを設定する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。

3 [スキャン]ウィンドウの[スキャンとタスク]で、[カスタムスキャン]をクリックします。

4 [実行]をクリックします。

5 [スキャン]ウィンドウの[スキャンの編集]列で、以前に作成したクイックスキャン、システムの完全スキャン、またはカスタムスキャンの横にある編集アイコンをクリックします。

6 [スキャンの編集]ウィンドウの[スキャンスケジュール]ページで次のいずれかの操作をします。

- [どのタイミングでスキャンを実行しますか?]で間隔を選択し、タイミングのオプションを選択します。
- [スキャンの実行]で、オプションを選択します。ほとんどのユーザーの場合、すべてのボックスをオンにしたままにすることを推奨します。このようにすると、パソコンを使用していないときや、バッテリ電源を使用していないときにだけスキャンが実行されるため、スキャン中にパソコンがスリープ状態になるのを防ぐことができます。

7 [次へ]をクリックします。

8 [スキャンオプション]ウィンドウで[保存]をクリックします。

ノートン SONAR によって検出された脅威をリアルタイムで表示する

SONAR は脅威からリアルタイム保護し、未知のセキュリティリスクをプロアクティブに検出します。SONAR は、アプリケーションの動作に基づいて新種の脅威を識別します。この方法は、従来のシグネチャベースの脅威検出より迅速です。ライブアップデートでウイルス定義を入手するよりも早く、悪質なコードからパソコンを保護するように支援します。

メモ: SONAR 保護は常時オンにしてください。自動保護をオフにすると SONAR 保護も無効になり、パソコンは新種の脅威から保護されなくなります。

SONAR によって検出されたリスクを表示する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウのドロップダウンリストで[SONAR 活動]を選択します。

4 リスクが表示される場合、リストでリスクを選択します。

5 [詳細]ペインの[推奨する処理]に従います。

このカテゴリには、パソコンの構成や設定を修正するすべての活動のリストも表示されます。このカテゴリの[詳細]オプションには、活動によって影響を受けたリソースの詳細情報が表示されます。

[SONAR 保護]がオンになっていることを確認する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [自動保護]タブの[リアルタイム保護]で、[SONAR 保護]スイッチを[オン]に動かします。

5 [適用]をクリックします。

6 [設定]ウィンドウで[閉じる]をクリックします。

ノートン自動保護、SONAR、ダウンロードインテリジェンススキャンからファイルやフォルダを除外する

Auto-Protect スキャンと SONAR スキャンから特定のプログラムを除外するようにノートンを設定できます。[スキャンの除外]ウィンドウと[リアルタイム除外]ウィンドウを使用して、ウイルスとその他の危険度が高いセキュリティの脅威をスキャンから除外できます。ファイルまたはフォルダを除外リストに追加すると、ノートンでセキュリティリスクをスキャンするときにそのファイルまたはフォルダは無視されます。

ダウンロードインテリジェンスからファイルを除外するには、フォルダを選択し、選択したフォルダにファイルをダウンロードする必要があります。たとえば、安全ではない実行可能ファイルをこのフォルダにダウンロードすると、ファイルのダウンロードが許可され、パソコンから削除されません。ダウンロードインテリジェンスの除外項目用の新しいフォルダを作成する必要があります。

メモ: ノートンのスキャンからファイルを除外すると、パソコンの保護レベルが低下するので、明確な必要性がある場合にのみ使用してください。項目は未感染という確信がある場合にのみ除外してください。

危険度が高いセキュリティの脅威をスキャンから除外する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[ウイルス対策]をクリックします。
4. [ウイルス対策]設定ウィンドウで、[スキャンとリスク]タブをクリックします。
5. [除外 / 低危険度]で次のいずれかの操作をします。
   - [スキャンから除外する項目]行で[設定]をクリックします。
   - [自動保護、スクリプト制御、SONAR、ダウンロードインテリジェンスの検出から除外する項目]行で[設定]をクリックします。
6. 表示されるウィンドウで[フォルダの追加]または[ファイルの追加]をクリックします。

   ローカルドライブ、フォルダ、ファイルのグループ、単一のファイル、ネットワークドライブを除外項目に割り当てることができます。ただし、ノートンはネットワーク上のファイルの除外をサポートしません。除外リストにネットワークドライブを追加する場合は、そのドライブがパソコンに接続されていることを確認してください。
7. [項目の追加]ダイアログボックスで参照アイコンをクリックします。
8. 表示されるダイアログボックスで、スキャンから除外したい項目を選択します。

   フォルダを追加する際、サブフォルダを含めるか除外するかを指定できます。
9. [OK]をクリックします。

10 [項目の追加]ダイアログボックスで[OK]をクリックします。

11 表示されるウィンドウで、[適用]をクリックしてから[OK]をクリックします。

ノートンのスキャンからシグネチャの危険度が低いファイルを除外する

ノートンのシグネチャの除外を使用するとノートンのスキャンから除外する特定の既知のセキュリティリスクを選択できます。たとえば、無料のゲームなどの正当なアプリを利用するためにアドウェアのような別のプログラムが必要な場合には、リスクにさらされてもパソコンにそのアドウェアを残すことを判断する場合があります。またその場合、将来のスキャンでそのプログラムに関する通知を受け取る必要はないでしょう。

メモ: 保護が低下するので、除外は明確な必要性があり、ノートンのスキャンから既知の脅威を除外することに伴う潜在的なリスクを十分理解した場合にのみ使用してください。

[シグネチャの除外]に危険度が低いシグネチャを追加する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [ウイルス対策]設定ウィンドウで、[スキャンとリスク]タブをクリックします。

5 [除外 / 低危険度]の[すべての検出から除外するシグネチャ]行で、[設定]をクリックします。

6 [シグネチャの除外]ウィンドウで、[追加]をクリックします。

7 [セキュリティリスク]ウィンドウで、除外したいセキュリティリスクをクリックしてから[追加]をクリックします。

8 [シグネチャの除外]ウィンドウで、[適用]をクリックしてから、[OK]をクリックします。

自動タスクのオンとオフを切り替える

ノートンは自動タスクの実行時に、バックグラウンドで動作させてパソコンを保護します。この自動タスクにはウイルスのスキャン、インターネット接続の監視、保護情報の更新版のダウンロード、その他の重要なタスクがあります。このような活動はパソコンに電源が入っているときにバックグラウンドで実行されます。

注意を要する項目がある場合、ノートンは現在の状態に関する情報が記載されたメッセージを表示し、対策を採るように促します。メッセージが表示されない場合、パソコンは保護されています。

ノートンをいつでも開いてパソコンの状態を一目で確認したり保護の詳細を表示したりすることができます。

バックグラウンド活動の実行中、ノートンは、タスクバーの右端にある通知領域にメッセージを表示します。最新の活動の結果は、次回ノートンのメインウィンドウを開いたときに確認できます。

自動タスクのオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[タスクスケジュール]をクリックします。

4 [タスクスケジュール]ウィンドウの[自動タスク]ページで次のいずれかの操作をします。

- 自動的に実行したい機能にチェックマークを付けます。
  [タスク]チェックボックスにチェックマークを付けて、すべての機能に一度にチェックマークを付けます。
- 自動的には実行したくない機能のチェックマークをはずします。
  [タスク]チェックボックスのチェックマークをはずして、すべての機能のチェックマークを一度にはずします。

5 [適用]をクリックしてから[閉じる]をクリックします。

カスタムタスクを実行する

ノートンはシステムを自動的に検査してシステムの安全性確保に最良の設定を選択します。ただし、いくつかの特定のタスクを実行することができます。[カスタムタスク]ウィンドウで利用可能なオプションを使って実行したい特定のタスクを選択できます。

1 回限りのスキャンに固有の組み合わせでタスクを選択できます。ライブアップデートの実行、データのバックアップの作成、ブラウザ履歴の消去、ディスククラッター上に散乱するファイルのクリーンアップによるディスク容量の解放、ディスクの最適化を行うことができます。

カスタムタスクを実行する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[スキャン]をクリックします。

3 [スキャン]ウィンドウの[スキャンとタスク]で、[カスタムタスク]をクリックし、次に[実行]をクリックします。

4 [カスタムタスク]ウィンドウで、実行したいタスクにチェックマークを付けます。

すべてのタスクを選択するには、[タスク]にチェックマークを付けます。

5 [実行]をクリックします。

セキュリティとパフォーマンスのスキャンのスケジュールを設定する

タスクスケジュールの設定を使うと、セキュリティとパフォーマンスの問題がないかノートンでシステムを自動的に検査できます。このような検査をノートン製品が実行するタイミングと頻度を指定できます。

セキュリティとパフォーマンスのスキャンのスケジュールには次のオプションがあります。

[自動 (推奨)]	アイドル状態のときにいつでもパソコンを検査してセキュリティとパフォーマンスの問題がないか調べます。 この設定で最大限の保護が得られます。
[週単位]	パソコンを週に 1 回以上検査してセキュリティとパフォーマンスの問題がないか調べます。 スキャンを実行する曜日と時刻を選択できます。
[月単位]	パソコンを月に 1 回検査してセキュリティとパフォーマンスの問題がないか調べます。 スキャンを実行する日と時刻を選択できます。
[手動スケジュール]	パソコンでセキュリティとパフォーマンスの定時スキャンを実行しません。 このオプションを選択した場合、保護状態を維持するためにパソコンでセキュリティとパフォーマンスの手動スキャンを定期的に実行してください。

パソコンがアイドル状態の間に重要な操作が実行されるようにスケジュール設定すると、パソコンのパフォーマンスは最大になります。スキャンを週単位または月単位でスケジュール設定して[アイドル時にのみ実行]オプションにチェックマークを付けている場合、ノートンはパソコンがアイドルのときにパソコンをスキャンします。[アイドル時にのみ実行]にチェックマークを付けてパソコンのパフォーマンスを上げることを推奨します。

セキュリティとパフォーマンスのスキャンのスケジュールを設定する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[タスクスケジュール]をクリックします。
4. [スケジュール]ページの[スケジュール]でオプションを選択します。

   [週単位]または[月単位]をクリックした場合には自動タスクを実行する日時を選択する必要があります。自動タスクをパソコンがアイドルのときにのみ実行することを指定するオプションもあります。
5. [適用]をクリックしてから[閉じる]をクリックします。

データプロテクタでパソコンに影響する悪質なプロセスが遮断されるように設定する

データプロテクタは、パソコンを不安定にし、データを壊したり盗んだりし、悪質な動作をその他の正常なプロセスに伝播することを意図する悪質なプロセスからパソコンを保護します。ノートンの評価技術を使用して、プロセスを安全、悪質、または不明に識別します。状況に応じて、追加のフォルダや拡張機能を追加したり、プロセスをスキャンや保護の対象から除外したりできます。

警告:この機能をオフにすると、パソコンに対する保護機能が低下します。そのため、常にこの機能をオンのままにすることを推奨します。この機能をオフにする場合は、一時的にオフにし、確実に再びオンにしてください。

データプロテクタのオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定] > [ウイルス対策]をクリックします。

3 [ウイルス対策]ウィンドウで、[データプロテクタ]タブをクリックします。

4 [データプロテクタ]行で、[オン/オフ]スイッチを[オン]または[オフ]の位置に動かします。

5 [通知を表示する]行で次のいずれかの操作をします。

- データプロテクタが脅威を遮断するたびに通知する場合はスイッチを[オン]の位置に動かします。
- 通知を表示しない場合は、スイッチを[オフ]の位置に動かします。その場合でも、[セキュリティ履歴]ウィンドウで、遮断した脅威の詳細を確認できます。
  [セキュリティ履歴]ウィンドウにアクセスするには、ノートンのメインウィンドウで[セキュリティ]をダブルクリックし、[履歴] > [データプロテクタ]を選択します。

6 [適用]をクリックします。

7 要求された場合は、データプロテクタ機能をオフにするまでの期間を選択し、[OK]をクリックします。

データプロテクタ保護対象のフォルダを追加または編集する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定] > [ウイルス対策]をクリックします。

3 [ウイルス対策]ウィンドウで、[データプロテクタ]タブをクリックします。

4 [データプロテクタ]行で、[オン/オフ]スイッチを[オン]の位置に動かします。

5 フォルダを追加または編集するには、以下を実行します。

- [保護されているフォルダ]の横にある[設定]をクリックします。
- [保護されているフォルダ]ウィンドウで、以下を実行します。
  - 新しい項目を含めるには、[追加]をクリックします。
  - 既存の項目を変更するには、項目を選択してから、[編集]をクリックして修正します。

  メモ: 事前設定されているフォルダを編集することはできません。

- [項目を追加する]ウィンドウまたは[項目を編集する]ウィンドウで、フォルダを参照して選択します。
- チェックボックスをクリックし、サブフォルダを含めます。
- [OK]をクリックします。

6 [適用]をクリックしてから[OK]をクリックします。

データプロテクタ保護対象の拡張機能を追加する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定] > [ウイルス対策]をクリックします。

3 [ウイルス対策]ウィンドウで、[データプロテクタ]タブをクリックします。

4 [データプロテクタ]行で、[オン/オフ]スイッチを[オン]の位置に動かします。

5 拡張機能を追加するには、以下を実行します。

- [保護されたファイルの種類]の横にある[設定]をクリックします。
- [保護されたファイルの種類]ウィンドウで、[追加]をクリックします。
- [項目を追加する]ウィンドウで、保護する拡張機能を入力します。たとえば、実行可能ファイルを保護する場合、ボックスに「.exe」と入力します。すると、パソコン上のあらゆる場所にある、拡張子が「.exe 」のファイルはすべて保護されます。
- [OK]をクリックします。

6 [適用]をクリックしてから[OK]をクリックします。

データプロテクタからフォルダまたは拡張機能を削除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定] > [ウイルス対策]をクリックします。

3 [ウイルス対策]ウィンドウで、[データプロテクタ]タブをクリックします。

4 [データプロテクタ]行で、[オン/オフ]スイッチを[オン]の位置に動かします。

5 [保護されているフォルダ]または[保護されたファイルの種類]の横にある[設定]をクリックします。

6 [保護されているフォルダ]ウィンドウ、または[保護されたファイルの種類]ウィンドウで、削除する項目を選択します。

メモ: 事前設定されているフォルダまたは拡張機能を削除することはできません。

7 [削除]をクリックします。

8 [適用]をクリックしてから[OK]をクリックします。

データプロテクタ除外対象に対してプロセスを追加または削除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定] > [ウイルス対策]をクリックします。

3 [ウイルス対策]ウィンドウで、[データプロテクタ]タブをクリックします。

4 [データプロテクタ]行で、[オン/オフ]スイッチを[オン]の位置に動かします。

5 [プロセスの除外]行で[設定]をクリックし、以下を実行します。

- データプロテクタ除外対象のプロセスを追加するには、[追加]をクリックしてから、プロセスを選択します。
- データプロテクタ除外対象からプロセスを削除するには、プロセスをクリックしてから[削除]をクリックします。

6 [適用]をクリックしてから[OK]をクリックします。

フィッシングの試行で攻略される恐れのあるスクリプトを削除するようにノートンを設定する

[スクリプト制御]は、ダウンロードしたり、フィッシング電子メールの添付ファイルとして受け取ったマルウェアからの保護に役立ちます。これにより、デフォルトでファイルから一般的でないスクリプトを削除したり、ファイルをサニタイズできます。**ただし、スクリプトが存在する元のファイルを復元して、スクリプトが埋め込まれたドキュメントをノートンが処理する方法を設定できます。

メモ: ** Chrome、Edge、Internet Explorer ブラウザでは、Windows 10 RS2 以降のバージョンでのみこの機能を使用できます。

また、埋め込まれたスクリプトで一般的でない動作が検出された場合、ノートンはスクリプトが埋め込まれたプログラムの実行を遮断します。ただし、スクリプトが埋め込まれたプログラムをノートンが処理する方法を設定できます。

スクリプトは、動的な、対話型のドキュメントを作成するのに使用されます。スクリプトの本来の目的はドキュメントの使い勝手を向上させることにありますが、サイバー犯罪者はそれらを使用してユーザーのパソコンにマルウェアを潜ませることができます。一般的には、スクリプトはドキュメントの機能にとって重要ではないため、多くのソフトウェアプログラムはデフォルトでこれらを無効にします。

疑わしいコンテンツが含まれていないことがわかっている場合は、[スクリプト制御]から特定のファイルを除外するようにノートンを設定できます。詳しくは、p.37 の「ノートン自動保護、SONAR、ダウンロードインテリジェンススキャンからファイルやフォルダを除外する」を参照してください。 を参照してください。サニタイズしたファイルを置き換えることにより、元のファイルを復元できます。疑わしいコンテンツが含まれていないことがわかっている場合にのみファイルを除外してください。

スクリプト制御は、ファイルの動作に基づいて潜在的な脅威を特定します。スクリプトが埋め込まれたドキュメントまたはプログラムを開いたときにノートンが潜在的に危険な活動を検出すると、ノートンはアプリケーションによるスクリプトの実行を遮断します。スクリプトが埋め込まれたドキュメントまたはプログラムを開いたときに、ノートンがスクリプトを処理する方法を設定できます。

元のファイルに戻すには

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]行の[開く]をクリックします。

2 ノートンのメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストから、[スクリプト制御]を選択します。

4 [スクリプト制御]ビューで、復元する項目を選択します。

5 右側のペインで、[詳細]にある[復元する]をクリックします。

6 [スクリプト制御の復元]ウィンドウで、[はい]をクリックします。

7 プロンプトが表示されたら、[はい]を選択します。

8 [セキュリティ履歴]ウィンドウで[閉じる]をクリックします。

[スクリプト制御]のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]行の[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [ウイルス対策]設定ウィンドウで、[スクリプト制御]タブをクリックします。

5 [ドキュメントのダウンロードしたときにスクリプトを削除する]行で、[オン/オフ]スイッチを[オン]または[オフ]に切り替え、[適用]をクリックします。

オフにした場合は、次のように操作します。

- [セキュリティ要求]ウィンドウの[期間を選択してください]ドロップダウンリストで、オプションをオフにしておきたい期間の長さを選択し、[OK]をクリックします。

6 [ドキュメントを開くときにスクリプトを遮断する]行で、[オン/オフ]スイッチを[オン]または[オフ]に切り替え、[適用]をクリックします。

オフにした場合は、次のように操作します。

- [セキュリティ要求]ウィンドウの[期間を選択してください]ドロップダウンリストで、オプションをオフにしておきたい期間の長さを選択し、[OK]をクリックします。

7 [設定]ウィンドウで[閉じる]をクリックします。

すべてのスクリプト制御項目を永久に削除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]行の[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストから、[スクリプト制御]を選択します。

4 [スクリプト制御]ビューで、[エントリの消去]をクリックします。

5 エントリの消去ウィンドウで、[はい]をクリックします。

6 確認ダイアログボックスで[はい]をクリックします。

7 [セキュリティ履歴]ウィンドウで[閉じる]をクリックします。

スクリプトが埋め込まれたドキュメントとプログラムをノートンが処理する方法の設定

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]行の[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [ウイルス対策]設定ウィンドウで、[スクリプト制御]タブをクリックします。

5 [ドキュメントを開くときにスクリプトを遮断する]の[Microsoft Office]行で、[設定]をクリックします。

6 [Microsoft Office 設定]ウィンドウの[処理]で、各アプリケーションに対してノートンに実行させる処理を選択します。

次のオプションがあります。

- [遮断する]
- [許可する]

- ［確認］

アプリケーションごとに異なる処理を選択できます。

7 表示される確認ウィンドウで［OK］をクリックします。

8 ［Microsoft Office 設定］ウィンドウで、［適用］をクリックしてから［OK］をクリックします。

9 ［Adobe ドキュメント］行で、PDF ドキュメントに対してノートンに実行させる処理を選択します。

10 ［一般的でない動作のスクリプトを遮断する］行で、スクリプトが埋め込まれたプログラムに対してノートンに実行させる処理を選択します。

次のオプションがあります。

- ［遮断する］
- ［許可する］
- ［確認］

11 ［設定］ウィンドウで、［適用］をクリックしてから［閉じる］をクリックします。

ノートン スクリプト制御に関する詳細

スクリプトは、動的な、対話型のドキュメントを作成するのに使用されます。また、スクリプトによって特定のタスクを自動化する機能も利用できるようになります。スクリプトには、ActiveX コントロール、アドイン、データ接続、マクロ、リンクされたオブジェクトリンクと埋め込まれた OLE ファイル、カラーテーマファイルなどがあります。

スクリプト制御は、ダウンロードしたり、フィッシング電子メールの添付ファイルとして受け取ったりしたマルウェアからの保護に役立ちます。

これにより、デフォルトでファイルから安全でないスクリプトを削除したり、ファイルをサニタイズできます。ただし、スクリプトが存在する元のファイルを復元して、スクリプトが埋め込まれたドキュメントをノートンが処理する方法を設定できます。

以降のセクションは、スクリプト制御の設定の構成に役立ちます。

スクリプトが埋め込まれた元のファイルを復元する

サニタイズしたファイルを置き換えることにより、元のファイルを復元できます。疑わしいコンテンツが含まれていないことがわかっている場合にのみ元のファイルを復元してください。

1 ノートンを起動します。

［マイノートン］ウィンドウが開いたら、［デバイスセキュリティ］行の［開く］をクリックします。

2 ノートンのメインウィンドウで、［セキュリティ］をダブルクリックしてから［履歴］をクリックします。

3 ［セキュリティ履歴］ウィンドウの［表示］ドロップダウンリストから、［スクリプト制御］を選択します。

4 ［スクリプト制御］ビューで、復元するアクティブコンテンツ項目を選択します。

5 右側のペインで、［詳細］にある［復元する］をクリックします。

6 [スクリプト制御の復元]ウィンドウで、[はい]をクリックします。

7 プロンプトが表示されたら、[はい]を選択します。

8 [セキュリティ履歴]ウィンドウで[閉じる]をクリックします。

スクリプトが埋め込まれたドキュメントとプログラムを処理するようにノートンを設定する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]行の[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [ウイルス対策]設定ウィンドウで、[スクリプト制御]タブをクリックします。

5 [ドキュメントを開くときにスクリプトを遮断する]の[Microsoft Office]行で、[設定]をクリックします。

6 [Microsoft Office 設定]ウィンドウの[処理]で、各アプリケーションに対してノートンに実行させる処理を選択します。

次のオプションがあります。

- [遮断する]
- [許可する]
- [確認]

アプリケーションごとに異なる処理を選択できます。

7 表示される確認ウィンドウで[OK]をクリックします。

8 [Microsoft Office 設定]ウィンドウで、[適用]をクリックしてから[OK]をクリックします。

9 [Adobe ドキュメント]行で、PDF ドキュメントに対してノートンに実行させる処理を選択します。

10 [一般的でない動作のスクリプトを遮断する]行で、スクリプトが埋め込まれたプログラムに対してノートンに実行させる処理を選択します。

次のオプションがあります。

- [遮断する]
- [許可する]

- ［確認］

11 ［設定］ウィンドウで、［適用］をクリックしてから［閉じる］をクリックします。

スクリプト制御をオフにする

メモ: スクリプト制御をオフにすることにより、保護のレベルが下がり、特定のニーズがある場合にのみ保護を行うことが可能になります。［スクリプト制御］によってスクリプトの削除とドキュメントのサニタイズが行われ、セキュリティがさらに強化されます。セキュリティを強化するため、ノートンLifeLock は、［スクリプト制御］を常にオンにしておくことを推奨します。

1 ノートンを起動します。

［マイノートン］ウィンドウが開いたら、［デバイスセキュリティ］行の［開く］をクリックします。

2 ノートンのメインウィンドウで［設定］をクリックします。

3 ［設定］ウィンドウで、［ウイルス対策］をクリックします。

4 ［ウイルス対策］設定ウィンドウで、［スクリプト制御］タブをクリックします。

5 ［ドキュメントをダウンロードしたときにスクリプトを削除する］行で、［オン/オフ］スイッチを［オフ］に切り替えます。

6 ［ドキュメントを開くときにスクリプトを遮断する］行で、［オン/オフ］スイッチを［オフ］に切り替えます。

7 ［設定］ウィンドウで、［適用］をクリックします。

8 ［セキュリティ要求］ウィンドウの［期間を選択してください］ドロップダウンリストで、機能をオフにしておきたい期間の長さを選択し、［OK］をクリックします。

9 ［設定］ウィンドウで［閉じる］をクリックします。

デバイスをエクスプロイト、ハッカー、ゼロデイ攻撃から保護

ゼロデイ攻撃とは、ハッカーがプログラムの脆弱性を利用して、パソコンで悪質な行為を実行するために使用する技術のことです。パソコンの速度が低下したり、プログラムの不具合の原因になったりする以外に、これらの攻撃によって、個人データや機密情報がハッカーにさらされてしまいます。

ノートン製品の未知の脆弱性保護機能は、エクスプロイト攻撃を受けやすいアプリケーションやファイルを保護します。デフォルトでは、ノートン脆弱性保護はオンになっており、脆弱なプログラムを終了してプログラムに対する攻撃を遮断します。ノートンは、プログラムをシャットダウンするときに「遮断された攻撃」通知を送信して、攻撃に関する情報へのリンクを提供します。

未知の脆弱性保護のオンとオフを切り替える

メモ: 未知の脆弱性保護をオフにした場合、パソコンはゼロデイ攻撃やその他のエクスプロイトに対して脆弱な状態になります。

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[未知の脆弱性保護]をクリックします。

4 [未知の脆弱性保護]行で、[オン/オフ]スイッチを[オフ]または[オン]の位置に動かします。

5 [設定]ウィンドウで、[適用]をクリックしてから[閉じる]をクリックします。

未知の脆弱性保護の技術

ノートンは、未知の脆弱性保護の技術を使用して、最新のゼロデイ攻撃からパソコンを保護します。[設定]ウィンドウで個別の技術のオンとオフを切り替えることができます。デフォルトでは、すべての技術はオンになっています。

メモ: ノートンでは、すべての脆弱性保護技術をオンにして、幅広い攻撃から保護することを推奨します。

未知の脆弱性保護には次の技術が含まれます。

- Java プロセス保護
  リモートのハッカーが Java プロセスを通じて悪質なコードを利用するのを防ぎ、信頼できる Java プロセスのみ実行を許可します。
- SEH (Structured Exception Handler) Overwrite 防止
  例外ハンドラのポインタを攻撃者が制御するアドレスで上書きすることによってアプリケーションに不正アクセスする、構造化例外を利用したエクスプロイトから保護します。
- スタックピボットの検出
  スタックのポインタを攻撃者が制御するメモリで変更して、ROP (Return Oriented Programming) によって製作された攻撃コードを実行するエクスプロイト攻撃を遮断します。
- データ実行防止のエンフォースメント
  パソコンのスタックやヒープメモリからの攻撃者による悪質なコードの実行を遮断します。
- メモリ配置のランダム化のエンフォースメント
  攻撃者から保護するため、動的にロードされたアプリケーションの DLL やモジュールが常にランダムな場所にロードされるように強制します。
- ヒープスプレー攻撃防止

エクスプロイトや攻撃者がヒープスプレー攻撃技術を使用してシェルコードを割り当てるときに標的となりやすいメモリの場所を保護します。

- メモリ配置のランダム化の拡張
  アプリケーションの重要なメモリの場所を割り当てるときに、オペレーティングシステムの ASLR (アドレス空間配置のランダム化) の動作を改善します。これによって、メモリの場所を攻撃者が予測しにくくなります。
- Null ページ攻撃防止
  Null メモリの場所を事前に割り当てます。これによって、攻撃者が、Null ポインタ逆参照の脆弱性を利用しにくくなります。
- リモート DLL インジェクションの検出
  リモートのハッカーが、パブリック IP アドレスやドメインなどの外部ネットワークを経由して悪質な実行可能コードを挿入するのを防ぎます。
- スタック実行防止、疑わしい API 呼び出しの検出、ヒープペイロードの検出技術は、アドレス空間配置のランダム化やデータ実行防止などのエクスプロイト緩和技術を回避する ROP (Return-Oriented Programming) 攻撃からパソコンを保護します。

ノートン ファイアウォールのオンとオフを切り替える

スマートファイアウォールは、インターネット上の他のパソコンとの間の通信を監視します。さらに一般的なセキュリティの問題からパソコンを保護します。スマートファイアウォールをオフにした場合、パソコンはインターネットの脅威とセキュリティリスクから保護されません。

スマートファイアウォールをオフにする必要がある場合は、特定の期間のみオフにしてください。その期間が過ぎると、スマートファイアウォールは自動的にオンに戻ります。

ノートン ファイアウォールのオンとオフを切り替える

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[ファイアウォール]をクリックします。
4. [一般の設定]ページの[スマートファイアウォール]行で、オン/オフスイッチ[オフ]または[オン]の位置に動かします。
5. [適用]をクリックします。
6. 要求された場合は、ファイアウォール機能をオフにするまでの期間を選択し、[OK]をクリックします。

Windows 通知領域でノートン ファイアウォールを無効または有効にする

1 タスクバーの通知領域でノートンのアイコンを右クリックして[スマートファイアウォールを無効にする]または[スマートファイアウォールを有効にする]をクリックします。

2 要求された場合は、ファイアウォール機能をオフにするまでの期間を選択し、[OK]をクリックします。

プログラムルールをカスタマイズしてプログラムのアクセス設定を変更する

ノートンをしばらく使うと、一定のプログラムのアクセス設定を変更する必要が出てくる場合があります。

プログラムルールをカスタマイズする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [プログラム制御]ページの[プログラム]列で、変更したいプログラムを選択します。

5 変更したいプログラムの横にあるドロップダウンリストでそのプログラムに設定したいアクセスレベルを選択します。次のオプションがあります。

[許可する]	このプログラムによるすべてのアクセスの試みを許可します。
[遮断する]	このプログラムによるすべてのアクセスの試みを拒否します。
[カスタム]	このプログラムがインターネットにどうアクセスするかを制御するルールを作成します。

6 [適用]をクリックします。

ファイアウォールルールの順序を変更する

リストごとに上から下にファイアウォールルールが処理されます。ファイアウォールルールの順序を変更することにより、これらのルールをどう処理するかを調整できます。

メモ: 詳しい知識のあるユーザー以外はデフォルトのトラフィックルールの順序を変更しないでください。デフォルトのトラフィックルールの順序を変更するとファイアウォールの機能に影響し、パソコンのセキュリティが低下することがあります。

トラフィックルールの順序を変更する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [トラフィックルール]ページで移動したいルールを選択します。

5 次のいずれかの操作をします。

- このルールをその上にあるルールの前に移動するには[上に移動]をクリックします。
- このルールをその下にあるルールの後ろに移動するには[下に移動]をクリックします。

6 ルールの移動が終わったら[適用]をクリックします。

プログラムルールの順序を変更する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [プログラム制御]ページで移動したいルールを含むプログラムを選択します。

5 [修正]をクリックします。

6 [ルール]ウィンドウで移動したいルールを選択します。

7 次のいずれかの操作をします。

- このルールをその上にあるルールの前に移動するには[上に移動]をクリックします。
- このルールをその下にあるルールの後ろに移動するには[下に移動]をクリックします。

8 ルールの移動が終わったら[OK]をクリックします。

9 [ファイアウォール]設定ウィンドウで、[適用]をクリックします。

トラフィックルールを一時的にオフにする

パソコンまたはプログラムへの特定のアクセスを許可する場合、トラフィックルールを一時的にオフにできます。変更を必要としたプログラムまたはパソコンの操作が終わったら忘れずにルールを再びオンにしてください。

メモ: リストに表示されるデフォルトのファイアウォールルールには、オフにできないものがあります。[表示]オプションを使ってこれらのルールの設定の表示のみを行うことができます。

トラフィックルールを一時的にオフにする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [トラフィックルール]ページでオフにしたいルールの隣にあるチェックボックスのチェックマークをはずします。

5 [適用]をクリックします。

遮断されたプログラムにインターネットアクセスを許可する

デフォルトでは、スマートファイアウォールは特定のプログラムのインターネットアクセスを遮断します。このようなプログラムには特定のストリーミングメディアプログラム、ネットワークゲーム、雇用者が持ち込んだカスタムビジネスアプリケーションが含まれる可能性があります。プログラムのインターネット活動がセキュリティの脅威にならないことがわかっている場合にはそのプログラムのインターネットアクセスを遮断解除できます。

遮断されたプログラムにインターネットアクセスを許可する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [プログラム制御]タブでインターネットアクセスを許可したいプログラムを選択します。

5 プログラムエントリの[アクセス]ドロップダウンリストで[許可する]をクリックします。

6 [適用]をクリックします。

デフォルトでは、ノートン ファイアウォールは Web 対応プログラムの最初の実行時に、そのプログラムに対するインターネットアクセスを自動的に設定します。プログラムが最初にインターネットにアクセスしようとするとき、プログラムの自動制御によりこのプログラム用のルールが作成されます。

ただし、プログラムのインターネットアクセスを手動で設定することもできます。

プログラムのインターネットアクセスを設定する

プログラムの自動制御をオフにする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [ファイアウォール]設定ウィンドウで、[拡張プログラム制御]をクリックします。

5 [プログラムの自動制御]行で、オン/オフスイッチを[オフ]の位置に動かします。

6 確認のウィンドウで、[はい]をクリックします。

7 [設定]ウィンドウで、[適用]をクリックしてから[閉じる]をクリックします。

プログラムのインターネットアクセスを設定する

1 プログラムを起動します。

プログラムがインターネットにアクセスしようとすると、ノートンのファイアウォール警告と確認メッセージが表示されます。

2 [ファイアウォール警告]ウィンドウの[オプション]ドロップダウンリストで、処理を選択します。

許可、遮断、プログラムルールの手動作成が可能です。

3 [OK]をクリックします。

ファイアウォール遮断通知をオフにする

[プログラムの自動制御]がオンになっていると、悪質なアプリケーションや低評価のアプリケーションによるインターネットへの接続やネットワーク上の他のパソコンとの通信がスマートファイアウォールによって自動的に遮断されます。

アプリケーションによるネットワークへの接続がスマートファイアウォールによって遮断されるとノートンから通知されます。この通知が表示されないようにするには、[拡張プログラム制御]を使ってこの通知をオフにします。

ファイアウォール遮断通知をオフにする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [プログラムの拡張制御]タブで、[ファイアウォール遮断通知を表示]スイッチを[オフ]の位置に動かします。

侵入防止除外リストについて

ネットワーク上のデバイスが安全であるという確信がある場合は、そのデバイスの信頼レベルを[完全な信頼]に変更できます。[ネットワークの設定]の[デバイスの信頼]を使用して、デバイスの信頼レベルを設定できます。これらの信頼できるデバイスは侵入防止スキャンから除外できます。[完全な信頼]デバイスを侵入防止スキャンから除外すると、スキャン時間が節約されてパソコンのネットワーク速度が改善されます。[完全な信頼]に設定されているデバイスを除外すると、ノートン製品はこのデバ

イスから受信する情報をスキャンしません。侵入防止スキャンから除外された[完全な信頼]デバイスは侵入防止除外リストに追加されます。

侵入防止スキャンから除外したデバイスのいずれかが感染していることがわかった場合は、保存されている除外リストをリセットできます。除外リストをリセットすると、ノートン製品は IPS で除外されるすべてのデバイスを除外リストから削除します。

保存されている除外リストは、次の状況でリセットできます。

- 侵入防止スキャンから除外したデバイスのいずれかが感染している。
- 侵入防止スキャンから除外したデバイスのいずれかがパソコンを感染させようとしている。
- ホームネットワークが感染している。

侵入防止除外リストからすべてのデバイスを削除する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[ファイアウォール]をクリックします。
4. [侵入防止とブラウザ保護]タブをクリックします。
5. [侵入防止]の[除外リスト]行で[リセット]をクリックします。
6. 確認ダイアログボックスで[はい]をクリックします。
7. [設定]ウィンドウで[閉じる]をクリックします。

ブラウザ保護をオンにする

悪質な Web サイトはブラウザの脆弱性を検出して悪用し、マルウェアをダウンロードします。[ブラウザ保護]をオンにすれば、ノートンがマルウェアを攻撃してくる前に遮断します。重要な情報の保護に役立ち、攻撃者がパソコンにアクセスできないようにします。

デフォルトでは、[ブラウザ保護]はオンになっています。悪質な Web サイトに対して確実に保護するには、[ブラウザ保護]をオンにしたままにしておいてください。

メモ: ブラウザ保護機能は、Google Chrome、Microsoft Internet Explorer、Mozilla Firefox、Microsoft Edge ブラウザで利用できます。

[ブラウザ保護]をオンにする方法

ブラウザ保護機能は、悪質な Web サイトからブラウザを保護するためにデフォルトではオンになっています。ただし、何らかの理由でオフにした場合はオンに戻すことができます。

[ブラウザ保護]をオンにする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [ブラウザ保護]行で、オン/オフスイッチを[オフ]の位置に動かします。

6 [適用]をクリックします。

7 [設定]ウィンドウで[閉じる]をクリックします。

ノートン ファイアウォールの設定で、攻撃を遮断したときの通知を停止したり再開できます。

攻撃の疑いのある通信をノートン製品の侵入防止システムが遮断した場合に通知を表示するかどうかを選択できます。

通知の受信を選択しなかった場合も、セキュリティ履歴でノートンが遮断した攻撃を確認できます。

侵入防止の通知のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[通知]行で、[オン/オフ]スイッチを[オフ]または[オン]の位置に動かします。

6 [設定]ウィンドウで、[適用]をクリックしてから[閉じる]をクリックします。

個々の侵入防止の通知のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[侵入シグネチャ]行で[設定]をクリックします。

6 [侵入シグネチャ]ウィンドウで、個々のシグネチャに対応する[通知する]にチェックマークを付けるかチェックマークをはずします。

7 [OK]をクリックします。

8 [侵入シグネチャ]ウィンドウで、[適用]をクリックしてから[OK]をクリックします。

9 [設定]ウィンドウで[閉じる]をクリックします。

自動遮断のオンとオフを切り替える

ノートン侵入自動遮断は、ネットワークのデバイスとそのデバイスを悪用しようとする他のパソコンの間のすべてのトラフィックを停止します。これには悪質ではないと考えられるトラフィックが含まれるため、自動遮断は、脅威が検出されてから一定期間のみ接続を停止します。ノートン製品が攻撃側のパソコンからの接続を遮断する期間を指定できます。デフォルトでは、ノートン製品は自分のパソコンと攻撃側のパソコン間のすべてのトラフィックを 30 分間遮断します。

アクセスする必要のあるパソコンを自動遮断が遮断している場合には自動遮断を無効にできます。

自動遮断のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[侵入自動遮断]行で[設定]をクリックします。

6 [侵入自動遮断]ウィンドウの[自動遮断]で次のいずれかの操作をします。

- 侵入自動遮断をオフにするには[オフ]をクリックします。
- 侵入自動遮断をオンにするには、[オン (推奨)]をクリックしてから、[自動遮断で攻撃側パソコンを遮断する期間]ドロップダウンリストで自動遮断をオンにする期間を選択します。

7 [侵入自動遮断]ウィンドウで[OK]をクリックします。

8 [設定]ウィンドウで[閉じる]をクリックします。

ノートン 自動遮断で遮断されたパソコンを遮断解除する

ノートン ファイアウォールが安全であることがわかっているパソコンへのネットワークトラフィックを停止している場合、ノートン ファイアウォール設定の自動遮断リストから削除して、パソコンへの接続を回復できます。

自動遮断で遮断しているパソコンの遮断を解除する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[侵入自動遮断]行で[設定]をクリックします。

6 [侵入自動遮断]ウィンドウの[現在自動遮断が遮断しているパソコン]で、パソコンの IP アドレスを選択します。

7 [処理]列の下で、ドロップダウンリストから[遮断しない]を選択します。

8 [侵入自動遮断]ウィンドウで[OK]をクリックします。

9 [設定]ウィンドウで[閉じる]をクリックします。

デバイスを[デバイスの信頼]に追加する

[デバイスの信頼]に手動でデバイスを追加できます。次の情報を指定してデバイスを追加できます。

- デバイスの名前または説明
- デバイスの IP アドレスまたは物理アドレス

メモ: 自分のネットワーク上にないデバイスを信頼する場合、パソコンは潜在的なセキュリティリスクに対して無防備になる可能性があります。

デバイスを[デバイスの信頼]に追加する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [一般の設定]タブの[デバイスの信頼]行で、[設定]をクリックします。

5 [デバイスの信頼]ウィンドウで、[追加]をクリックします。

6 [デバイスの追加]ウィンドウの[名前]ボックスにネットワークに追加するデバイスの名前を入力します。

デバイス名の最大長は 15 文字以下にする必要があります。

7 [IP アドレスまたは物理アドレス]ボックスにデバイスの信頼に追加するデバイスの IP アドレスまたは物理アドレスを入力します。

[IP アドレスまたは物理アドレス]フィールドでは次の形式が使えます。

IPv4 アドレス	172.16.0.0
IPv6 アドレス	fe80::12ac:fe44:192a:14cc
物理アドレス	11-22-c3-5a-fe-a4
解決可能なホスト	ftp.myfiles.com

指定したアドレスはそのデバイスがネットワーク上で物理的に見つかるまで検証されません。

8 [信頼レベル]ドロップダウンメニューから任意のオプションを選択します。次のオプションがあります。

[完全な信頼]	デバイスを[完全な信頼]リストに追加します。 [完全な信頼]のデバイスは既知の攻撃と感染についてのみ監視されます。この設定はデバイスが完全に安全であるという確信があるときのみ選択してください。
[制限]	デバイスを[制限]リストに追加します。 制限デバイスはこのパソコンにアクセスできません。

9 デバイスを侵入防止スキャンから除外する場合は、[IPS スキャンから除外]にチェックマークを付けます。

10 [デバイスの追加]をクリックします。

ダウンロードインテリジェンスのオンとオフを切り替える

ダウンロードインサイトは、サポート対象の ブラウザを使ってダウンロードした後に実行される可能性がある安全でないファイルから、パソコンを保護します。デフォルトでは、[ダウンロードインテリジェンス]オプションはオンになっています。この場合、ダウンロードインサイトはダウンロードした実行可能ファイルの評価レベルを通知します。ダウンロードインサイトが提供する評価の詳細には、ダウンロードしたファイルをインストールして安全かどうかが示されます。

場合によっては、ダウンロードインサイトをオフにしたいことがあります。たとえば、安全でないファイルをダウンロードする場合です。この場合、ファイルをダウンロードしてもノートン製品がそのファイルをパソコンから削除しないようにダウンロードインサイトをオフにする必要があります。

[ダウンロードインテリジェンス]オプションを使って、ダウンロードインサイトをオフまたはオンにできます。

ダウンロードインテリジェンスのオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [ダウンロードインテリジェンス]行で、[オン/オフ]スイッチを[オフ]または[オン]の位置に動かします。

6 [適用]をクリックします。

7 要求された場合は、ダウンロードインテリジェンス機能をオフにするまでの期間を選択し、[OK]をクリックします。

8 [設定]ウィンドウで[閉じる]をクリックします。

スパムフィルタ処理のオンとオフを切り替える

電子メールの使用が増加するにつれ、多くのユーザーがスパムと呼ばれる不要で迷惑な営利目的の電子メールメッセージを大量に受け取っています。スパムは有効な電子メールメッセージを識別しにくくするだけでなく、一部のスパムは不快なメッセージやイメージを含みます。

これらのスパムメールを制御するには、スパムフィルタ処理を使います。デフォルトではスパム防止は有効な状態のままです。何らかの理由で無効にしたい場合にはプログラム自体の内部からオフにできます。

メモ: ノートン アンチスパムをオフにすると、迷惑メールメッセージを受信する機会が増加します。

スパムフィルタ処理のオンとオフを切り替える

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[スパム対策]をクリックします。

4 [フィルタ]タブの[スパム対策]行で、[オン/オフ]スイッチを[オフ]または[オン]の位置に動かします。

5 スパムフィルタ処理をオフにする場合は、次の操作を実行します。

- [セキュリティ要求]ウィンドウの[期間を選択してください。]ドロップダウンリストでスパムフィルタ処理をオフにする期間を選択します。

6 [適用]をクリックします。

7 [OK]をクリックします。

8 [設定]ウィンドウで[閉じる]をクリックします。

ノートンによるインターネットの使用を定義する

[データ通信ポリシー]を使うと、ノートン製品が使うネットワーク帯域幅を制御できます。デフォルトでは、[データ通信ポリシー]はオンになっており、[自動]に設定されています。Windows 7 以前の場合のデフォルト設定は[無制限]です。インターネット接続の速度が低下している場合は、ノートン製品が使う帯域幅を減らすことができます。[データ通信ポリシー]の設定を変更すると、パソコンが使うすべてのネットワーク接続の通信ポリシーを設定することもできます。

ノートンによるインターネットの使用を定義する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ファイアウォール]をクリックします。

4 [一般の設定]タブの[データ通信ポリシー]行で[設定]をクリックします。[設定]オプションが無効な場合は、オン/オフスイッチを[オン]の位置に動かします。

5 [データ通信ポリシー]設定ウィンドウの[ポリシー]列で、ポリシーを設定するネットワーク接続の横にあるドロップダウンリストをクリックします。

6 次のいずれかを選択します。

- [自動]: ノートンは Windows のデータ通信ポリシーに基づいてすべての製品とウイルス定義の更新を受信できます。

  メモ: [自動]オプションは Windows 8 以降でのみ利用できます。

- [無制限]: ノートンは必要なネットワーク帯域幅を使って、すべての製品とウイルス定義の更新を受信します。Windows 7 以前を使っている場合、デフォルトポリシーは[無制限]です。
- [節約]: ノートン製品は、重要な製品のアップデートやウイルス定義を受信する場合にのみインターネットにアクセスできます。インターネット接続が制限されている場合は、[節約]を設定すると、致命的なセキュリティの脅威から保護されます。
- [トラフィックなし]: ノートンによるインターネットへの接続を遮断します。このポリシーを選択した場合、ノートンは重要なウイルス定義とプログラムの更新を受信できません。そのため、潜在的な危険とウイルス攻撃にさらされる可能性があります。

7 [適用]をクリックしてから[OK]をクリックします。

8 [設定]ウィンドウで[閉じる]をクリックします。

データ通信ポリシーのオンとオフを切り替える

ノートン製品のインターネット使用率を制限するポリシーを設定できます。ノートン製品のインターネット使用率を制限しない場合は、[データ通信ポリシー]をオフにします。

ノートン製品が使うネットワーク帯域幅が大きすぎると考えられる場合は、[データ通信ポリシー]をオンにします。次に、ノートン製品のインターネット使用率を制限するポリシーを設定します。ノートン製品は、[データ通信ポリシー]設定ウィンドウで設定されているポリシーに基づいてインターネットに接続します。デフォルトでは、[データ通信ポリシー]はオンになっています。

データ通信ポリシーのオンとオフを切り替える

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[ファイアウォール]をクリックします。

   ノートン アンチウイルスをインストールしている場合、[ネットワーク]をクリックします。
4. [一般の設定]タブの[データ通信ポリシー]行で、[オン/オフ]スイッチを[オフ]または[オン]の位置に動かします。
5. [設定]ウィンドウで、[適用]をクリックしてから[閉じる]をクリックします。

アプリケーションを監視し、悪質な Web サイトからのパソコンへのアクセスを遮断するようにノートンを設定する

フリーウェアやシェアウェアアプリケーションをインストールして起動したとき、悪質な Web サイトがデバイス情報への権限がないアクセスを試みる場合があります。悪質な Web サイトは脆弱性を検出して攻略し、デバイス情報をサイバー犯罪者に公開できるクリプトマイニングマルウェアなどのマルウェアをダウンロードします。

[アプリ URL の監視]をオンにすると、ノートンはパソコンにインストールされたすべてのアプリケーションを監視し、悪質な Web サイトからのパソコンへのアクセスを遮断します。ノートンは悪質な Web サイトを遮断したときに警告を表示します。[セキュリティ履歴]ウィンドウで、攻撃に関する情報を確認できます。

メモ: [アプリ URL の監視]は、ブラウザアプリケーションは監視しません。ブラウザアプリケーションを悪質な Web サイトから保護するには、ノートンのブラウザ拡張機能を追加する必要があります。

アプリ URL の監視をオンにして悪質な Web サイトを遮断する

デフォルトでは、[アプリ URL の監視]はオンになっています。悪質な Web サイトに対して確実に保護するには、[アプリ URL の監視]をオンのままにしてください。

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[アプリ URL の監視]行で、オン/オフスイッチを[オン]の位置に動かします。

URL またはドメインを監視から除外する

侵入防止は攻撃シグネチャのリストを使用し、疑わしい Web サイトを検出して遮断します。場合によっては、安全な Web サイトが類似の攻撃シグネチャを持つために、疑わしいと識別されることがあります。潜在的な攻撃の通知を受け取って、通知をトリガする Web サイトまたはドメインが安全であるとわかっている場合は、そのシグネチャを監視から除外することができます。

URL またはドメインを警告通知から除外する

1 警告通知で[詳細を表示する]をクリックします。

2 [セキュリティ履歴 - 詳細]ウィンドウで、[URL の遮断解除]をクリックします。

ノートンを使用して URL またはドメインを除外する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで[ファイアウォール]または[ネットワーク]をクリックします。

4 [侵入防止とブラウザ保護]タブをクリックします。

5 [侵入防止]の[アプリ URL の監視除外]で[設定]をクリックします。

6 [追加]ボタンをクリックし、監視から除外する URL またはドメインを入力します。

7 URL またはドメインを編集または削除する場合は、次の手順を実行します。

- リストから URL またはドメインを選択し、[編集]ボタンをクリックします。URL またはドメイン名を変更します。
- 削除する URL またはドメインを選択し、[削除]ボタンをクリックします。

遮断された URL に関する情報を表示する

警告通知の情報を表示する

1 警告通知で[詳細を表示する]をクリックします。

2 [セキュリティ履歴 - 詳細]ウィンドウで、遮断された URL に関する詳細を確認できます。

[セキュリティ履歴]ウィンドウで情報を表示する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートン製品のメインウィンドウで、[セキュリティ]をダブルクリックしてから[履歴]をクリックします。
3. [セキュリティ履歴]ウィンドウの[表示]ドロップダウンリストで、リストから[侵入防止]を選択します。
4. 行をクリックして項目の詳細を表示します。
5. 行をダブルクリックするか[その他のオプション]をクリックし、[セキュリティ履歴 - 詳細]を開いて、活動に関する詳細を表示し、必要に応じて活動に対するアクションを実行します。

ノートン クラウドバックアップを初めて使用する

クラウドバックアップにより、ハードディスクドライブの障害、デバイスの盗難、さらにはランサムウェアによるデータ損失への予防対策として、重要なファイルと文書を保存して保護できます。

メモ: ノートン クラウドバックアップは Windows でのみ利用できます。

ノートン クラウドバックアップを実行する前に、バックアップを作成するファイルの種類を指定するバックアップセットを作成する必要があります。ファイルをバックアップする場所とバックアップを実行するタイミングも指定できます。ファイルのバックアップは、ノートン クラウドバックアップを使用してクラウドに作成したり、外付けドライブに作成したりできます。

メモ: 初めてバックアップを実行するときは、ノートンがパソコンのすべてのファイルを確認してコピーするのに、少し時間がかかる可能性があります。インターネット接続が遅い場合、処理時間が長くなる可能性があります。

バックアップ先がローカルバックアップである場合、ノートンはファイルのバックアップを自動的には行いません。ローカルストレージデバイスにバックアップする場合は、ユーザーの操作が必要になります。

バックアップセットを作成します

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[バックアップ]をダブルクリックしてから[バックアップセット]をクリックします。
3. [バックアップの設定]ウィンドウで、[新しいセットの作成]をクリックします。
4. 表示されるウィンドウでバックアップセット名を入力してから[OK]をクリックします。

5 [対象]ページの[ファイルの種類]で、バックアップを作成する 1 つ以上のファイルカテゴリを選択します。

6 [場所]タブの[バックアップ先]列で、[セキュアクラウドストレージ]を選択します。

クラウドバックアップをアクティブ化したら[無料でアクティブ化する]リンクをクリックして、表示される手順を実行します。

7 [タイミング]タブで、[スケジュール]リストを使用して必要なバックアップに最も合うバックアップスケジュールを選択します。

8 [設定を保存する]をクリックします。

ノートン クラウドバックアップを実行する

メモ: バックアップを初めて実行したとき、ノートンは、認証のためにアカウント資格情報を入力するように求めることがあります。

---

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[バックアップ]をダブルクリックしてから[バックアップを実行する]をクリックします。

3 [バックアップを実行する]ウィンドウで、画面上の指示に従います。

4 [閉じる]をクリックします。

メモ: バックアップが完了しない場合、ノートンは、ストレージ容量が不十分、速度制限など、可能性のある原因を提示します。バックアップ時は、インターネットに接続されていて、ストレージデバイスが接続され、電源がオンになっていることを必ず確認してください。

バックアップセットのファイルとフォルダを追加または除外する

ノートンを使うと、写真、音楽、ビデオなど、さまざまな種類のファイルをバックアップセットにバックアップできます。通常はバックアップセットに含まれる種類のファイルやそのようなファイルが含まれたフォルダを指定し、それらをバックアップから除外できます。

通常はデフォルトのファイルの種類となっているファイル拡張子を追加または削除することもできます。詳しくは次を参照してください。p.66 の「バックアップに含めるデフォルトのファイルの種類またはファイル拡張子を表示または変更する」を参照してください。

バックアップセットのファイルとフォルダを追加または除外する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[バックアップ]をダブルクリックしてから[バックアップセット]をクリックします。
3. [バックアップの設定]ウィンドウの[バックアップセット]ドロップダウンリストで、設定するバックアップセットを選択します。
4. [対象]タブで[ファイルまたはフォルダを追加または除外する]をクリックします。
5. 表示されるウィンドウで次の操作を実行します。
   - バックアップセットにファイルを追加する場合は、[含めるファイル]をクリックして追加するファイルに移動します。
   - バックアップセットにフォルダを追加する場合は、[含めるフォルダ]をクリックして追加するフォルダに移動します。
   - バックアップセットからファイルを削除する場合は、[除外するファイル]をクリックして削除するファイルに移動します。
   - バックアップセットからフォルダを削除する場合は、[除外するフォルダ]をクリックして削除するフォルダに移動します。
6. [バックアップの設定]ウィンドウで、[設定を保存する]をクリックします。

メモ: ファイルまたはフォルダを右クリックして、ショートカットメニューの[ノートン セキュリティ] > [バックアップに追加する]または[バックアップから除外する]を選択してファイルまたはフォルダをバックアップに追加したりバックアップから除外することもできます。

ショートカットメニューの[バックアップに追加する]と[バックアップから除外する]オプションは、バックアップの設定後や、[バックアップの設定]または[ファイルを復元する]ウィンドウを閉じるときにのみ表示されます。

バックアップに含めるデフォルトのファイルの種類またはファイル拡張子を表示または変更する

デフォルトでは、ノートン バックアップはバックアップを実行する前に、写真、音楽、ビデオなどの特定のファイルの種類に属するファイルを探します。デフォルトのファイルの種類の設定では、バックアップセットを作成してバックアップを実行すると、ほとんどのユーザーが重要と考えるデータが自動的にバックアップされます。バックアップでデータを含めるか除外する場合は、バックアップファイルの種類のデフォルト、または各ファイルの種類に含まれる拡張子を変更できます。

バックアップに含めるデフォルトのファイルの種類またはファイル拡張子を表示または変更する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[バックアップ]をダブルクリックしてから[バックアップセット]をクリックします。
3. [バックアップの設定]ウィンドウの[バックアップセット]ドロップダウンリストで、設定するバックアップセットを選択します。
4. [対象]タブで[ファイルの種類を編集する]にチェックマークを付け、写真、音楽、ビデオなどのファイルの種類に該当する拡張子を変更します。
5. [ファイルの種類]で、ファイルの種類の横にある[設定する]をクリックします。
6. 表示されるウィンドウで次の操作を実行して[保存]をクリックします。
   - ファイル拡張子を削除する場合は、リストからファイル拡張子を選択して[削除]をクリックする
   - リストに拡張子を追加する場合は、[新規追加する]をクリックします。
7. [バックアップの設定]ウィンドウで、[設定を保存する]をクリックします。

ノートンバックアップセットから写真、音楽、その他の重要なファイルを復元する

ランサムウェアまたは他のマルウェアの被害に遭った場合や、回復不能なハードウェアの問題が発生した場合、ノートン バックアップデータを簡単に復元できます。バックアップセット全体またはバックアップセットの特定のファイルの復元を選択できます。また、バックアップされているファイルの復元先を指定することもできます。

メモ: 復元は、設定済みのバックアップセットに従って実行されます。新しいデバイスに復元する場合、古いデバイスの希望するフォルダ構造のとおりにファイルが復元されることは期待できません。

ノートンのバックアップファイルまたはバックアップセット全体を復元する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[バックアップ]をダブルクリックしてから[ファイルを復元する]をクリックします。
3. [ファイルの復元]ウィンドウの[復元元]で[すべてを表示]をクリックします。

   バックアップセットをクリックしてから、[OK]をクリックします。

4 [ファイルの復元]ウィンドウの[ファイル]で[ファイルやフォルダを参照する]をクリックします。

復元したいファイルにチェックマークを付けてから、[OK]をクリックします。

5 [ファイルの復元]ウィンドウの[復元先]で、[元の場所]をクリックします。

元の場所に復元しない場合は[変更する]をクリックして、手順に従います。

6 [ファイルを復元する]をクリックしてから、[閉じる]をクリックします。

クラウドバックアップからファイルをダウンロードする

1 https://my.Norton.com に移動します。

2 [サインイン]をクリックします。

3 ノートンLifeLock アカウントの電子メールアドレスとパスワードを入力し、[サインイン]をクリックします。

4 [マイノートン]ページの[クラウドバックアップ]タイルで、[バックアップセットを表示する]をクリックします。

5 ダウンロードするファイルが含まれたバックアップセットを選択します。

6 ダウンロードするファイルがある場所に移動します。

ファイル名がわかっている場合は、検索機能を使用してその特定のファイルを検索できます。

[フィルタ]オプションを使用して、画像やドキュメントをフィルタできます。

7 マウスのポインタをファイル名の上に合わせ、[ダウンロード]をクリックします。

クラウドバックアップからのバックアップセットとファイルの削除

不要になったバックアップセットを削除できます。利用可能なバックアップセットが 1 つのみの場合、バックアップセットは削除できません。ただし、古いバックアップセットを削除する前に新しいバックアップセットを作成できます。

メモ: バックエンドサービスの停止またはサーバーメンテナンスのため、バックアップデータを削除できない場合があります。このような場合は、しばらく経ってから削除してみてください。サービスの停止が発生しているかどうかを、ノートン サービスの状態ページで確認できます。

バックアップセットを削除すると、そのバックアップセットに含まれるファイルのバックアップの詳細も変わります。たとえば、ファイルのバックアップ状態アイコンとファイルのプロパティの[バックアップ]ページは表示されなくなります。

バックアップセットの削除は、セキュアクラウドストレージの領域の解放に特に役立ちます。

メモ: クラウドバックアップからバックアップセットを削除するには、[ファイアウォールの設定]ウィンドウの[データ通信ポリシー]オプションを[無制限]に設定する必要があります。

詳しくは次を参照してください。p.61 の「ノートンによるインターネットの使用を定義する」を参照してください。

バックアップセットを削除する

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートンのメインウィンドウで、[バックアップ]をダブルクリックしてから[バックアップセット]をクリックします。
3. [バックアップの設定]ウィンドウの[バックアップセット]ドロップダウンリストで、削除するバックアップセットを選択します。
4. [削除]をクリックします。
5. [バックアップセットを削除する]ウィンドウで次のいずれかの操作を実行します。
   - 現在のバックアップセットを削除する場合は、[バックアップセットを削除する]を選択する
   - 現在のバックアップセットとすでにバックアップが作成されているファイルを削除する場合は、[バックアップセットとファイルを削除する]を選択する
6. [はい]をクリックします。

アカウントからバックアップセットを削除する

1. アカウントにサインインします。
2. [マイノートン]ページで、[クラウドバックアップ]をクリックします。

   使用中の既存のバックアップセットが表示されます。
3. バックアップセットを削除するには、削除したいバックアップセットのごみ箱アイコンを選択します。
4. [バックアップセットを削除する]確認ウィンドウで、[削除]をクリックします。

   [キャンセル]をクリックすると、バックアップセットを削除しないで[バックアップ]ページが表示されます。

ノートン製品の設定のカスタマイズ

[設定]ウィンドウでは次のクイック制御サービスのオンとオフを切り替えることができます。

- [サイレントモード]
- [バックアップ]

- ［バックアップ状態マーク］
- ［自動ライブアップデート］
- ［スマートファイアウォール］
- ［ノートン製品の改ざん対策］

［サイレントモード］以外のすべてのサービスをオンのままにしてください。

クイック制御サービスをオンまたはオフにする

1 ノートンを起動します。

［マイノートン］ウィンドウが開いたら、［デバイスセキュリティ］の横にある［開く］をクリックします。

2 ノートンのメインウィンドウで［設定］をクリックします。

3 ［設定］ウィンドウの［クイック制御］で次のいずれかの操作をします。

- サービスをオンにするにはそのチェックボックスにチェックマークを付けます。
- サービスをオフにするにはそのチェックボックスのチェックマークをはずします。
  警告またはメッセージが表示されたら、ドロップダウンメニューから期間を選択して［OK］をクリックします。

リアルタイム保護設定のカスタマイズ

リアルタイム保護は、パソコン上の未知のセキュリティリスクを検出します。リスクが検出された場合、実行するべき対策を決定できます。

メモ: ほとんどのユーザーにはデフォルト設定を推奨します。機能を一時的にオフにしたい場合でもできるだけ早くオンにしてください。危険度が低いアイテムを自動的に削除したい場合は SONAR 拡張モードを設定します。自動保護はパソコン上のプログラムが実行されるたびに、ウイルスとその他のセキュリティリスクの有無を調べます。自動保護は常にオンにしておいてください。

自動保護でリムーバブルメディアスキャンを設定する

リムーバブルメディアにアクセスする際に、ブートウイルスの有無を調べます。ブートウイルスをスキャンした後、そのリムーバブルメディアは再挿入またはフォーマットするまで再スキャンされません。依然としてリムーバブルメディアでブートウイルスの感染が疑われる場合は、リムーバブルメディアを再スキャンするため、［自動保護］をオンにします。次に、リムーバブルメディアを挿入して、［マイコンピュータ］からそのメディアを開くと、自動保護によってメディアが再スキャンされます。手動でリムーバブルメディアをスキャンして感染していないと確認することもできます。

自動保護の設定をカスタマイズする

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [リムーバブルメディアスキャン]でスライダーを[オン]に設定します。

SONAR で脅威の自動削除を設定する

SONAR は、脅威からパソコンをリアルタイム保護し、未知のセキュリティリスクをパソコン上でプロアクティブに検出します。SONAR はアプリケーションの動作に基づいて新種の脅威を識別します。SONAR 拡張モードの設定で SONAR が脅威を削除する方法を設定できます。

SONAR で脅威の自動削除を設定する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [リスクを自動的に削除]で、スライダーを[常時]に設定します。

5 [操作がないときにリスクを削除]で、スライダーを[常時]に設定します。

6 [適用]をクリックします。

自動保護でノートンのスキャンからの既知の良好なファイルの除外を設定する

ノートンが有効なアプリケーションをセキュリティリスクとして識別してしまう場合にノートンのスキャンからファイルを除外できます。

ノートンのスキャンからファイルを除外する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートンのメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[ウイルス対策]をクリックします。

4 [ウイルス対策]設定ウィンドウで、[スキャンとリスク]タブをクリックします。

5 [除外 / 低危険度]で次のいずれかの操作をします。

- [スキャンから除外する項目]行で[設定]をクリックします。

- ［自動保護、SONAR、ダウンロードインテリジェンスの検出から除外する項目］行で［設定］をクリックします。

6 表示されるウィンドウで［フォルダの追加］または［ファイルの追加］をクリックします。

7 ［項目の追加］ダイアログボックスで参照アイコンをクリックします。表示されるダイアログボックスで、スキャンから除外する項目を選択します。

8 ［OK］をクリックします。

スキャンとリスクの設定について

［スキャンとリスク］の設定を使うとノートンがパソコン上で実行するスキャンをカスタマイズできます。パソコン上のファイルのデジタル署名と信頼レベルに基づいてスキャンを設定できます。電子メールメッセージのスキャン時にノートンがどのように動作するかを定義できます。

次のスキャンとリスクの設定があります。

［パソコンスキャン］

さまざまな種類のスキャンを実行し、パソコン上のウイルスを検出して感染を防止できます。スキャンには、クイックスキャン、システムの完全スキャン、カスタムスキャンがあります。［パソコンスキャン］の各種オプションを使ってノートンがパソコン上で実行するスキャンをカスタマイズできます。圧縮ファイルのスキャンを指定することもできます。

［パソコンスキャン］オプションでは、ルートキット、その他のステルス項目、cookie による追跡、未知のセキュリティの脅威を検出するスキャンを指定することもできます。次のオプションがあります。

- ［圧縮ファイルスキャン］
  圧縮ファイル内部のファイルをスキャンして修復します。
  この機能をオンにすると、ノートンは圧縮ファイル内のファイルのウイルスとその他のセキュリティリスクを検出して圧縮ファイルを削除します。
- ［ルートキットとステルス項目のスキャン］
  パソコン上に隠れている可能性があるルートキットやその他のセキュリティリスクをスキャンします。
- ［ネットワークドライブスキャン］
  パソコンに接続されているネットワークドライブをスキャンします。
  ノートンはシステムの完全スキャン中とカスタムスキャン中にネットワークドライブスキャンを実行します。デフォルトでは、［ネットワークドライブスキャン］オプションはオンになっています。このオプションをオフにすると、ノートンはネットワークドライブをスキャンしません。
- ［ヒューリスティック保護］
  パソコンをスキャンして未知のセキュリティの脅威から保護します。
  ノートンはヒューリスティック技術を使ってファイルの疑わしい特性を調べ、感染ファイルとして分類します。ファイルの特性は既知の感染ファイルと照合されます。ファイルに明らかに疑わしい特性がある場合、ノートンはそのファイルを脅威が存在する感染ファイルとして識別します。
- ［cookie による追跡のスキャン］

パソコン処理活動を追跡するためにプログラムがパソコンに配置した可能性のある小さいファイルをスキャンします。

- ［システムの完全スキャン］
  システムの完全スキャンはパソコン全体を検査してウイルス、スパイウェア、さまざまなセキュリティの脆弱性を調べます。［設定］オプションを使ってシステムの完全スキャンをスケジュール設定できます。

保護ポート

［保護ポート］の設定によって、電子メールプログラムの POP3 ポートと SMTP ポートを保護できます。

このオプションを使うと、電子メール保護をするように POP3 と SMTP の電子メールポートを手動で設定できます。使っている電子メールプログラムに対してインターネットサービスプロバイダ (ISP) が提供している SMTP ポート番号と POP3 ポート番号がデフォルトの SMTP ポート番号と POP3 ポート番号と異なる場合は、これらのポートを保護するようにノートンを設定する必要があります。

電子メールウイルススキャン

［電子メールウイルススキャン］は電子メールの添付ファイルで送受信される脅威から保護します。

［電子メールウイルススキャン］オプションを使うと、電子メールメッセージをスキャンするときのノートンの動作を定義できます。ノートンは選択したオプションに基づいて送受信する電子メールメッセージを自動的にスキャンします。

除外/低危険度

［除外］オプションでは、ノートンのスキャンから除外するフォルダ、ファイル、ドライブなどの項目を指定します。スキャンから除外できるのは、スキャンシグネチャや危険度が低い項目です。

［除外］オプションでは、ノートンで検出するリスクのカテゴリを選択することもできます。次のオプションがあります。

- ［低危険度］
  パソコンで見つかった危険度の低い項目を管理できます。
  ノートンで危険度の低い項目にどう応答するかを指定できます。
- ［スキャンから除外する項目］
  リスクスキャンから除外したいディスク、フォルダ、ファイルを決定できます。
  新しい除外項目を追加したり、除外項目リストに追加した項目を編集したりできます。項目を除外項目リストから削除することもできます。
- ［自動保護、SONAR、ダウンロードインテリジェンスの検出から除外する項目］
  自動保護スキャンと SONAR スキャンから除外したいディスク、フォルダ、ファイルを決定できます。
  除外する必要がある項目を新しく追加したり、すでに除外した項目を修正できます。項目を除外項目リストから削除することもできます。
- ［すべての検出から除外するシグネチャ］

名前で既知のリスクを選択したり、除外項目リストからリスク名を削除することができます。
また、パフォーマンス、プライバシー、削除、ステルスの影響に基づくリスクの影響を表示できます。

- ［スキャン時に除外されるファイル ID を消去］
  スキャンから除外されるファイルの評価情報を削除できます。
  ［すべてクリア］オプションを使って、スキャンから除外されるファイルの評価情報を消去できます。

メモ: 保護レベルが低下するので、除外は明確な必要性がある場合にのみ使用してください。

侵入とブラウザ保護の設定について

侵入防止はパソコンに出入りするすべてのネットワークトラフィックをスキャンしてこの情報を攻撃シグネチャのセットと照合し調べます。攻撃シグネチャには攻撃者が既知のオペレーティングシステムまたはプログラムの脆弱性を悪用する試みを識別する情報が含まれます。 侵入防止は一般的なインターネット攻撃のほとんどからパソコンを保護します。

情報が攻撃シグネチャに一致する場合、侵入防止はパケットを自動的に破棄してそのデータを送信したパソコンとの接続を切断します。この処理でパソコンはいずれの影響からも保護されます。

侵入防止は攻撃シグネチャのリストに基づいて疑わしいネットワーク活動の検出と遮断をします。ノートン製品は、攻撃シグネチャのリストを最新にしておくためにライブアップデートを自動的に実行します。自動ライブアップデートを使わない場合、1 週間に 1 回ライブアップデートを実行してください。

また、ノートン製品はブラウザ保護機能によって、悪質なプログラムからブラウザを守ります。

メモ: ブラウザ保護機能は、Google Chrome、Microsoft Internet Explorer、Mozilla Firefox、Microsoft Edge ブラウザで利用できます。

インターネットを使う機会が増えるにつれて、ブラウザは悪質な Web サイトから攻撃されやすくなります。悪質なサイトは、Web ブラウザの脆弱性を検出してそれを悪用し、ユーザーの同意なく、知らないうちにマルウェアプログラムをシステムにダウンロードします。このようなマルウェアプログラムは、ドライブバイダウンロードとも呼ばれます。また、ノートン製品は、悪質な Web サイトによるドライブバイダウンロードからブラウザを保護します。

［侵入防止とブラウザ保護］の設定には、ダウンロードした安全でないファイルからパソコンを保護する［ダウンロードインテリジェンス］オプションも含まれます。ダウンロードインテリジェンスは、ブラウザを使ってダウンロードした実行可能ファイルの評価レベルに関する情報を提供します。ダウンロードインテリジェンスは、HTTPS プロトコル、Internet Explorer 6.0 以降、Edge 40.15063 以降、Chrome 10.0 以降、Firefox 3.6 以降のブラウザを使用したダウンロードのみをサポートしています。ダウンロードインテリジェンスが提供する評価の詳細には、ダウンロードしたファイルをインストールして安全かどうかが示されます。これらの詳細を使って実行可能ファイルをインストールするかどうかを決定できます。

保護されているデバイスをリモートで管理できるようにノートン製品を設定する

ノートンのリモート管理では、デバイスの健全性状態とその他の情報が Windows 用ノートン スタジオアプリに送信されます。このアプリを使用して、ノートン製品を表示、管理、または探索したり、デバイスの保護に関する問題をリモートで解決したりできます。デフォルトでは、[リモート管理]はオフです。

[リモート管理]をオンにする

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートン製品のメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[管理の設定]をクリックします。
4. [リモート管理]行で、スイッチを[オン]の位置に動かします。
5. [適用]をクリックしてから[閉じる]をクリックします。

ノートン デバイスセキュリティ設定を権限がないアクセスから保護する

ノートン デバイスセキュリティ設定の不正な変更を防ぐには、[設定のパスワード保護]と[ノートン製品の改ざん対策]をオンにします。

- [設定のパスワード保護]をオンにすると、デバイスセキュリティ設定を表示または変更するためのパスワードを設定できます。
- [ノートン製品の改ざん対策]をオンにすると、未知または疑わしいアプリによる設定に対する変更が検証されます。

[設定のパスワード保護]と[ノートン製品の改ざん対策]のオンとオフを切り替える

1. ノートンを起動します。

   [マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。
2. ノートン製品のメインウィンドウで[設定]をクリックします。
3. [設定]ウィンドウで、[管理の設定]をクリックします。
4. [製品セキュリティ]で以下の操作を行います。
   - [設定のパスワード保護]行で、スイッチを[オン]または[オフ]の位置に動かします。
   - [ノートン製品の改ざん対策]行で、スイッチを[オン]または[オフ]の位置に動かします。要求された場合は、機能を無効にする期間を選択し、[OK]をクリックします。
5. [適用]をクリックします。
6. [パスワードの設定]ウィンドウが表示されたら、パスワードを入力して確定します。この機能を有効または無効にするたびにパスワードを設定する必要があります。

7 [OK]をクリックします。

8 [設定]ウィンドウで[閉じる]をクリックします。

ノートン設定のパスワード保護のパスワードを紛失または忘れた場合のリセット

設定にアクセスして新しいパスワードを設定するには、ノートンを再インストールする必要があります。

ノートン デバイスセキュリティで情報を検索するショートカットキーを設定する

ノートン デバイスセキュリティアプリの検索アイコンを使用して、ノートンの機能とサポート情報、一般的なトピックをオンラインで検索できます。デフォルトのキーボードショートカット Ctrl+F を使用してすばやく検索したり、ショートカットを設定できます。

検索ショートカットキーを設定する

1 ノートンを起動します。

[マイノートン]ウィンドウが開いたら、[デバイスセキュリティ]の横にある[開く]をクリックします。

2 ノートン製品のメインウィンドウで[設定]をクリックします。

3 [設定]ウィンドウで、[管理の設定]をクリックします。

4 [検索ショートカットキー]行でスイッチを[オン]の位置に移動します。

5 矢印をクリックして、製品内検索に割り当てるキーを選択します。

6 次のいずれかの操作をします。

- ノートン製品がフォーカスしたときのみショートカットキーを動作させるには、[グローバル]オプションのチェックマークをはずします。
- ノートン製品がフォーカスしないときにショートカットキーを動作させるには、[グローバル]オプションにチェックマークを付けます。

7 [適用]をクリックしてから[閉じる]をクリックします。

ゲーム オプティマイザーでパソコンをゲーム用に最適化する

ゲーム オプティマイザー[1]は、マルチコアの CPU を搭載したパソコン向けの特許取得済み技術です。コンピュータのセキュリティを維持しながら、パフォーマンスの低下を防ぐことで、没入型のゲーム体験を提供します。必須ではないアプリを単一の CPU コアに分離することで、残りの CPU をゲームに割り当てることができます。

メモ: ゲーム オプティマイザーを機能させるには、パソコンのプロセッサが 4 コア以上である必要があります。

ゲーム オプティマイザーは、次のようにしてゲーム体験を改善します。

- CPU のパフォーマンスを最適化してゲームをスムーズに実行
- 必須ではないアプリを単一の CPU コアに分離し、残りの CPU をゲームに割り当ててパフォーマンスを改善
- ゲームを自動的に検出[2]
- ゲームを追加したり、最適化が不要なゲームを選択することが可能
- 1 秒あたりのフレーム数 (FPS) を増加し、遅延を削減
- ゲームのパフォーマンスを最適化するために必要な CPU を占有できるため、ウイルス対策保護をオフにする必要性を排除
- CPU コアをゲーム用に占有することで、ゲームの速度を低下させる可能性のあるランダムな CPU スパイクを削減

詳しくは、p.78 の「ゲーム オプティマイザーの詳細」を参照してください。を参照してください。

メモ: ウイルスとその他のセキュリティの脅威からのパソコンの保護に関連する重要なノートン プロテクション機能は、すべてバックグラウンドで実行され、ゲーム体験を妨げることはありません。

ゲーム体験を最適化するようにノートン製品を設定する

1. ノートンを起動します。
2. [マイノートン]ウィンドウの中央ペインで、稲妻のアイコンをクリックします。
3. [ゲームダッシュボード]で、[最適化の管理]をクリックします。
4. [ゲーム オプティマイザー]ウィンドウで、次の設定を構成します。
   - [ユーザープロセスのリソース使用率を制限]: このオプションをオンにすると、ユーザーが開始したすべてのプロセスの CPU 使用率が制限されます。
   - [システムプロセスのリソース使用率を制限]: このオプションをオンにすると、オペレーティングシステムが開始したすべてのプロセスの CPU 使用率が制限されます。
   - [電源プランを自動的に高パフォーマンスに設定する]: このオプションをオンにすると、Windows の高パフォーマンス電源プラン設定に切り替わります。ゲーム オプティマイザーは、ゲームのパフォーマンスを最大化するためにカスタムの Windows 電源プラン設定を作成します。この電源プランは、ゲームセッションが進行中の場合にのみ利用できます。ゲームセッションが終了すると、電源プランは元の設定に戻ります。
     優れたゲーム体験を実現するには、このオプションを常にオンにすることを推奨します。

- ［最適化対象のゲーム］: ゲーム オプティマイザーによって最適化されるゲームを一覧表示します。

ゲーム オプティマイザーをオンにする

デフォルトで、ゲーム オプティマイザーはオンになっています。ゲームユーザー向け機能を強化する必要がない場合は、ゲーム オプティマイザーをオフにできます。優れたゲーム体験を実現するには、この機能を常にオンにすることを推奨します。

ゲーム オプティマイザーのオンとオフを切り替える

1. ノートンを起動します。
2. ［マイノートン］ウィンドウの左ペインで、［ゲーム オプティマイザー］スイッチをスライドして、この機能を有効または無効にします。

通知領域から［ゲーム オプティマイザー］のオンとオフを切り替える

- Windows タスクバーの通知領域でノートンのアイコンを右クリックし、次のいずれかの操作を実行します。
  - ゲーム オプティマイザーをオフにするには、［ゲーム オプティマイザー をオフにする］をクリックします。
  - ゲーム オプティマイザーをオンにするには、［ゲーム オプティマイザー をオンにする］をクリックします。

[1]ゲーム オプティマイザー は、4 つ以上のコアプロセッサを搭載した Windows で利用できます (Windows 10 の S モード、および ARM プロセッサで動作する Windows を除く)。

[2]ユーザーによって手動でゲームが追加された場合、または以前にゲームが検出された場合は、ゲームランチャー[3]の使用と同様に、CPU 使用率の高い全画面検出モードに基づいてゲームを自動的に検出します。

[3] 2021 年 4 月の時点で監視しているゲームランチャーは、Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam、Uplay です。

ゲーム オプティマイザーの詳細

ゲーム オプティマイザー[1]は、マルチコアの CPU を搭載したパソコン向けの特許取得済み技術です。コンピュータのセキュリティを維持しながら、パフォーマンスの低下を防ぐことで、没入型のゲーム体験を提供します。必須ではないアプリを単一の CPU コアに分離することで、残りの CPU をゲームに割り当てることができます。

ゲーム オプティマイザーは、次のようにしてゲーム体験を改善します。

- CPU のパフォーマンスを最適化してゲームをスムーズに実行
- 必須ではないアプリを単一の CPU コアに分離し、残りの CPU をゲームに割り当ててパフォーマンスを改善

- ゲームを自動的に検出[2]
- ゲームを追加したり、最適化が不要なゲームを選択することが可能
- 1 秒あたりのフレーム数 (FPS) を増加し、遅延を削減
- ゲームのパフォーマンスを最適化するために必要な CPU を占有できるため、ウイルス対策保護をオフにする必要性を排除
- CPU コアをゲーム用に占有することで、ゲームの速度を低下させる可能性のあるランダムな CPU スパイクを削減

バックグラウンドで行われる活動を最小限に抑えると、パソコンのパフォーマンスも向上し、ゲームをプレイするには理想的です。ゲームセッションが終了すると、ノートン 360 for Gamers は一時停止していたすべての活動の実行をバックグラウンドで再開します。

メモ: ゲーム オプティマイザーを機能させるには、パソコンのプロセッサが 4 コア以上である必要があります。

ゲームアプリケーションを開始すると、ゲーム オプティマイザーは最適化を開始し、ゲームを終了するまで最適化を続けます。ゲームセッションがアクティブなときに全画面モードを終了すると、最適化は一時停止されます。たとえば、Alt + Tab を押して他の実行中のプログラムにアクセスすると、ゲームの最適化を終了し、制限を解除します。ただしゲームに戻るとゲームの最適化を続行し、制限対象のプログラムは CPU を使用できなくなります。

メモ: ウイルスとその他のセキュリティの脅威からのパソコンの保護に関連する重要なノートン プロテクション機能は、すべてバックグラウンドで実行され、ゲーム体験を妨げることはありません。

タスクバーの通知領域でゲーム オプティマイザーの状態を確認できます。ゲーム オプティマイザーが有効になっていると、通知領域のノートン製品のアイコンに緑の稲妻アイコンが表示されます。ゲーム オプティマイザーをオフにすると、この色がグレーに変わります。

[ゲームダッシュボード]には、ゲーム オプティマイザーの状態、最近プレイしたゲームの最適化の状態、ゲーム オプティマイザーの設定へのアクセスが表示されます。切り替えスイッチを使用して、最近プレイしたゲームの最適化を有効または無効にできます。

メモ: ゲーム オプティマイザー機能は、ノートン 360 for Gamers でのみ利用できます。

---

[1]ゲーム オプティマイザーは、4 つ以上のコアプロセッサを搭載した Windows で利用できます (Windows 10 の S モード、および ARM プロセッサで動作する Windows を除く)。

[2]ユーザーによって手動でゲームが追加された場合、または以前にゲームが検出された場合は、ゲームランチャー[3]の使用と同様に、CPU 使用率の高い全画面検出モードに基づいてゲームを自動的に検出します。

[3] 2021 年 4 月の時点で監視しているゲームランチャーは、Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam、Uplay です。

[最適化対象のゲーム]リストに手動でゲームを追加する

ゲーム オプティマイザー[1]は、マルチコアの CPU を搭載したパソコン向けの特許取得済み技術です。コンピュータのセキュリティを維持しながら、パフォーマンスの低下を防ぐことで、没入型のゲーム体験を提供します。必須ではないアプリを単一の CPU コアに分離することで、残りの CPU をゲームに割り当てることができます。既知のゲームの内部リストをチェックして、ゲームアプリケーションを検出します。[1、2] ただし、特定のゲームが自動的に検出されなかった場合は、[最適化対象のゲーム]リストに手動でゲームを追加できます。

また、ノートン 360 for Gamers にゲームのパフォーマンスを強化させる必要がない場合は、[最適化対象のゲーム]リストからそのゲームを削除することもできます。

メモ: [最適化対象のゲーム]リストから特定のゲームを削除すると、そのゲームは最適化されなくなり、そのゲームのパフォーマンスに影響する可能性があります。

[最適化対象のゲーム]リストにゲームを追加する

1. ノートンを起動します。
2. [マイノートン]ウィンドウの中央ペインで、稲妻のアイコンをクリックします。
3. [ゲームダッシュボード]で、[最適化の管理]をクリックします。
4. [ゲーム オプティマイザー]ウィンドウで、[最適化対象のゲーム]の横にある[追加]をクリックします。
5. ノートンで最適化するゲームプログラムに移動して選択します。

[最適化対象のゲーム]リストからゲームを削除する

1. ノートンを起動します。
2. [マイノートン]ウィンドウの中央ペインで、稲妻のアイコンをクリックします。
3. [ゲームダッシュボード]で、[最適化の管理]をクリックします。
4. [ゲーム オプティマイザー]ウィンドウの[最適化対象のゲーム]で、削除するゲームプログラムの横にあるスイッチを無効にします。

[1]ゲーム オプティマイザーは、4 つ以上のコアプロセッサを搭載した Windows で利用できます (Windows 10 の S モード、および ARM プロセッサで動作する Windows を除く)。

[2]ユーザーによって手動でゲームが追加された場合、または以前にゲームが検出された場合は、ゲームランチャー[3]の使用と同様に、CPU 使用率の高い全画面検出モードに基づいてゲームを自動的に検出します。

[3] 2021 年 4 月の時点で監視しているゲームランチャーは、Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam、Uplay です。

4

追加の解決策を検索

この章では以下の項目について説明しています。

- Windows からデバイスセキュリティをアンインストールする
- 免責事項

Windows からデバイスセキュリティをアンインストールする

以下の手順を実行して、パソコンからデバイスセキュリティアプリをアンインストールします。

Windows からデバイスセキュリティをアンインストールする

1. Windows+R を押して、[ファイル名を指定して実行]ダイアログボックスを開きます。
2. `appwiz.cpl` と入力し、Enter を押します。
3. 現在インストールされているプログラムのリストで、ノートン製品を選択して[アンインストールと変更]をクリックします。
4. 画面の指示に従って操作します。

   パソコンを再起動するまでデバイスセキュリティは完全にはアンインストールされません。

免責事項