ノートン™ セキュリティ

製品マニュアル

Norton LifeLock™

ノートン™ セキュリティ製品マニュアル

ドキュメントバージョン 22.20.1

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

https://www.symantec.com/ja/jp

Made in Singapore.

10 9 8 7 6 5 4 3 2 1

目次

1

ノートンにようこそ

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 セキュリティのシステム要件
- よくあるご質問: ノートン アカウント
- ノートン 早期採用プログラム

ノートン セキュリティのシステム要件

ノートン セキュリティをお使いのパソコン、Mac®、スマートフォン、タブレットにインストールするには、システムの最小要件を満たしていることを確認してください。

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® 8.1 以降 (32 ビットおよび 64 ビット)
- Microsoft Windows® 8 および Windows® 8 Pro (32 ビットおよび 64 ビット)
- Microsoft Windows® 7 (32 ビットおよび 64 ビット) Service Pack 1 以降

ハードウェア

- CPU
  Windows 10/8/7: 1 GHz
- RAM
  Windows 10: 2 GB (回復ツールには最低 512 MB RAM 必要)
  Windows 8/7: 1 GB (32 ビット) (回復ツールには最低 512 MB RAM 必要)
- ハードディスク容量
  300 MB 以上のハードディスク容量

脆弱性保護機能のサポート対象ブラウザ

脆弱性保護機能に対しては次のブラウザがサポートされています。

- Microsoft Internet Explorer® 8.0 以降 (32 ビットおよび 64 ビット)[1, 2]
- Mozilla Firefox® (32 ビットおよび 64 ビット)[2]
- Google Chrome™ (32 ビットおよび 64 ビット)[2]

フィッシング対策、セーフサーチ、パスワード管理のサポート対象ブラウザ

次のブラウザはフィッシング対策、セーフサーチ、パスワード管理をサポートしています。

- Microsoft Internet Explorer® 8.0 以降 (32 ビットおよび 64 ビット)[1, 2]
- Microsoft Edge® (32 ビットおよび 64 ビット)[1, 2]
- Mozilla Firefox® (32 ビットおよび 64 ビット)[2]
- Google Chrome™ (32 ビットおよび 64 ビット)[2]

メモ: セーフサーチ機能は、Microsoft Edge ブラウザでは使用できません。

電子メールクライアント

ノートン セキュリティは、POP3 と互換性のあるすべての電子メールクライアントでの電子メールスキャンをサポートしています。

スパム対策のサポート

次の電子メールクライアントはスパム対策をサポートしています。

- Microsoft Outlook 2003 以降

[1] 一部の保護機能は、Microsoft Internet Explorer 10.0 以降では使えません。

[2] サービス期間内にシマンテック社によってサポートされた場合。

よくあるご質問: ノートン アカウント

次のことを実行するにはノートン アカウントにサインインします。

- 製品のアクティブ化
- バックアップへのアクセス
- クラウド型のデータ保管庫へのアクセスまたは作成
- ノートン製品のライセンスを管理する
- アカウントに保存されたプロダクトキーを使って、ノートン製品を再インストールする
- ストレージを購入してオンラインバックアップの容量を追加する

ノートン アカウントにサインインするにはどうすればよいですか?

https://my.norton.com でいずれかのデバイスからノートン アカウントにアクセスします。

サインインするには、ノートン アカウントの作成時に使用した電子メールアドレスとパスワードを入力します。

メモ: ノートン アカウントへのアクセスに 2 段階認証を選択している場合は、パスワードに加え確認コードを使う必要があります。

ノートン アカウントのパスワードを回復する方法

1. ノートン アカウントのサインインページで[パスワードを忘れた場合]リンクをクリックします。
2. ノートン製品を購入したときやノートン アカウントを作成したときに使った電子メールアドレスを入力します。
3. [続行]をクリックします。
4. パスワードをリセットするリンクが norton@symantec.com から電子メールで送信されます。受信ボックスでその電子メールが見つからない場合は迷惑メールフォルダを調べます。

   リンクをクリックしてもリンク先のページが表示されない場合はこのリンクをコピーして Web ブラウザに直接貼り付けます。

   電子メールが見つからない場合は、入力した電子メールアドレスがノートン製品の購入時やノートン アカウントの作成時に使った電子メールアドレスと同じであることを確認してください。

ノートン アカウントを持っているかどうか不明な場合

以下の情報を基にノートン アカウントを取得しているかどうかを確認できます。

- ノートン製品をインストールまたはアクティブ化している場合は、ほぼ間違いなくノートン アカウントをすでに保有しています。インストールやアクティブ化のプロセスの一環として、名前、電子メールアドレス、パスワードを入力してアカウントを作成する必要があります。
- シマンテックストアで製品を購入した場合やノートン製品のライセンスを延長した場合は、名前、電子メールアドレス、パスワードの入力を求めるメッセージが表示されてノートン アカウントが作成されています。
- ノートン ファミリー、ノートン オンラインバックアップ、ノートン セーフウェブにサインアップした場合はノートン アカウントを保有している可能性があります。ただし、このアカウントが関連付けられたノートン セキュリティライセンスも保有していることを確認してください。

ノートン 早期採用プログラム

ノートン 早期採用プログラムを利用すると、ノートンのプレリリースソフトウェアをダウンロードして、新しい機能を試す最初のユーザーになることができます。プレリリースソフトウェアにアップグレードするために、別のノートン アカウントを作成したり、ノートンをアンインストールしたりする必要はありません。

ノートン 早期採用プログラムに参加すると、ノートン ライブアップデートがお使いのパソコンに最新のプレリリースソフトウェアをダウンロードします。

ノートン 早期採用プログラムに参加するメリットは何ですか?

- 最新のノートン セキュリティの機能をプレビューすることができます。
- 製品の最終バージョンの開発に役立つフィードバックを行うことができます。

ノートン 早期採用プログラムに参加する資格があるのは誰ですか?

限られた数の課金ユーザーまたはアクティブユーザーに、製品内でノートン 早期採用プログラムの招待が送信されます。これが最初にプログラムに参加する唯一の方法です。

ノートン 早期採用プログラムに登録するにはどうすれば良いですか?

製品内でノートン 早期採用プログラムの招待を受け取った場合、登録できます。

ノートン 早期採用プログラムはいつでもやめることができます。

ノートン 早期採用プログラムをやめた場合、以前のバージョンにロールバックできますか?

ノートン 早期採用プログラムはいつでもやめられますし、ノートン製品の以前のバージョンにロールバックできます。

ノートン 早期採用プログラムを選択する前に、ノートンのローカルバックアップドライブをバックアップする必要がありますか?

データをバックアップする必要はありません。ノートン ライブアップデートがノートンの最新プレリリースソフトウェアをインストールします。ただし、ノートン 早期採用プログラムをやめると、ノートンのローカル設定は失われます。

ノートン 早期採用プログラムに関するフィードバックをお知らせください。

フィードバックを提供する

ノートン 早期採用プログラムに参加する

製品内でノートン 早期採用プログラムに参加する招待を受け取った場合、登録できます。

ノートン 早期採用プログラムはいつでもやめることができます。

招待からノートン 早期採用プログラムに参加する

1. ノートン 早期採用プログラムの招待で、[詳細]をクリックします。
2. [ノートン 早期採用プログラムについて]ページを読み、[参加する]をクリックします。
3. ノートン製品使用許諾契約を読んでから、[同意する]をクリックします。

4 ノートン アカウントのパスワードを入力して、[サインイン]をクリックします。

5 [登録完了]ウィンドウで[閉じる]をクリックします。ノートンが次のライブアップデートセッションでパソコンにプレリリースソフトウェアをダウンロードします。

ノートンの[管理の設定]ウィンドウからノートン 早期採用プログラムに参加する

製品内の招待を拒否したか無視した場合、ノートン製品を使用してノートン 早期採用プログラムに参加できます。

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、[管理の設定]をクリックします。

4 [管理の設定]ウィンドウの[ノートン 早期採用プログラム]行で[参加する]をクリックします。

5 [ノートン 早期採用プログラムについて]ページを読み、[参加する]をクリックします。

6 ノートン製品使用許諾契約を読んでから、[同意する]をクリックします。

7 ノートン アカウントのパスワードを入力して、[サインイン]をクリックします。

8 [登録完了]ウィンドウで[閉じる]をクリックします。ノートンが次のライブアップデートセッションでパソコンにプレリリースソフトウェアをダウンロードします。

ノートン 早期採用プログラムをやめる

ノートン 早期採用プログラムは、ノートンの[管理の設定]ウィンドウからいつでもやめることができます。

ノートン 早期採用プログラムをやめる

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 [管理の設定]ウィンドウの[ノートン 早期採用プログラム]行で[登録解除]をクリックします。

5 ノートン製品がノートン 削除/再インストールツールを開始して、以前のノートン製品のバージョンにロールバックします。

6 使用許諾契約を読んで[同意]をクリックします。

7 ［削除と再インストール］をクリックします。

8 ［今すぐ再起動］をクリックします。

パソコンを再起動したら、画面上の指示に従ってノートン製品の以前のバージョンを再インストールします。

2

ノートンのダウンロードとインストール

この章では以下の項目について説明しています。

ノートンのダウンロードとインストール

お使いのデバイスを保護してノートン製品を管理するのは、ノートンアカウントに新しいデバイスを追加するのと同じくらい簡単です。

お使いのパソコンにノートンをダウンロードしてインストールするには

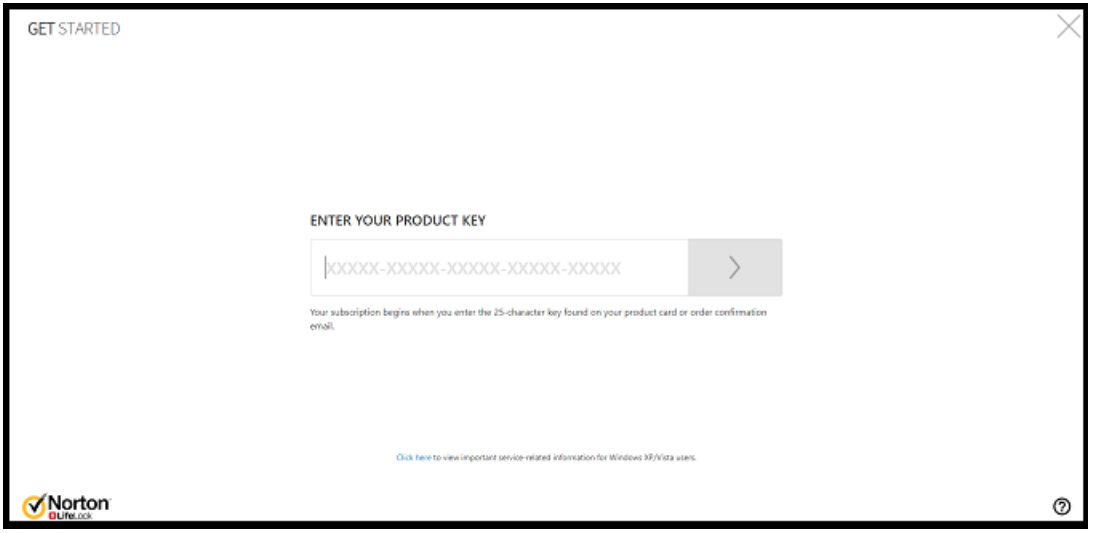
1. ノートンにサインインします。
2. アカウントにサインインしていない場合は、電子メールアドレスとパスワードを入力して、[サインイン]をクリックします。

   アカウントを持っていない場合は、[アカウントを作成する]をクリックして、サインアッププロセスを完了します。

3 [開始する]ウィンドウで、[ノートンをダウンロードする]をクリックします。

ノートン アカウントにまだ登録されていない新しい製品をインストールするには、[新しいプロダクトキーを入力]をクリックします。

プロダクトキーを入力して、「次へ」(>) アイコンをクリックします。



4 [同意してダウンロードする]をクリックします。

5 画面の青い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。

- Internet Explorer または Microsoft Edge ブラウザの場合は、[実行]をクリックします。
- Firefox または Safari の場合は、ブラウザの右上隅にある[ダウンロード]オプションをクリックしてダウンロードされたファイルを表示し、ダウンロードしたファイルをダブルクリックします。
- Chrome の場合は、左下隅に表示されるダウンロードしたファイルをダブルクリックします。

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

7 ノートン製品がダウンロード、インストールされ、アクティブ化されます。

追加デバイスへのノートンのインストール

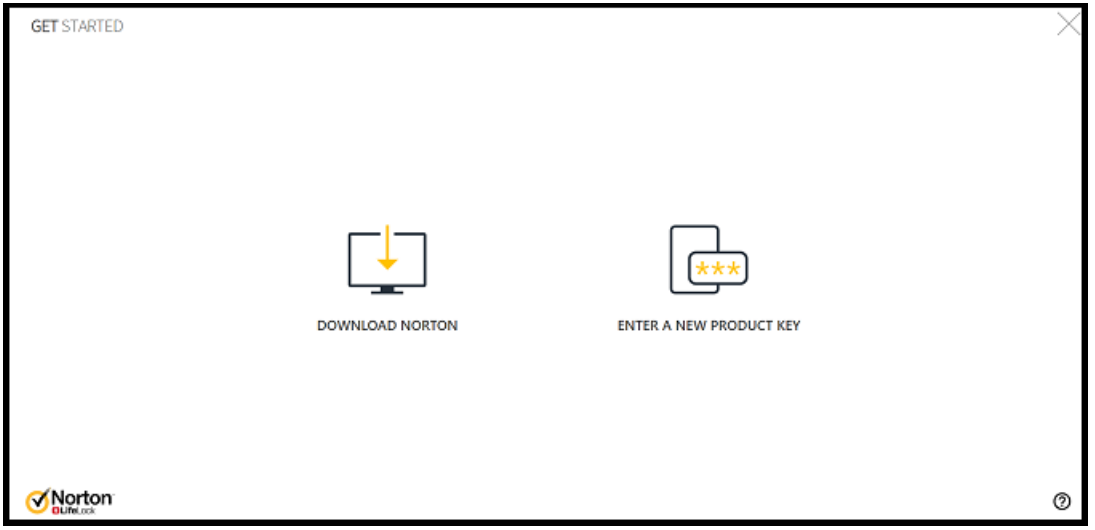
ノートン アカウントから追加デバイスに電子メールを送信して、そのデバイスにノートンをインストールできます。電子メールにはノートンをインストールするためのインストールリンクと説明が記載されています。

別のデバイスにノートンをインストールするには

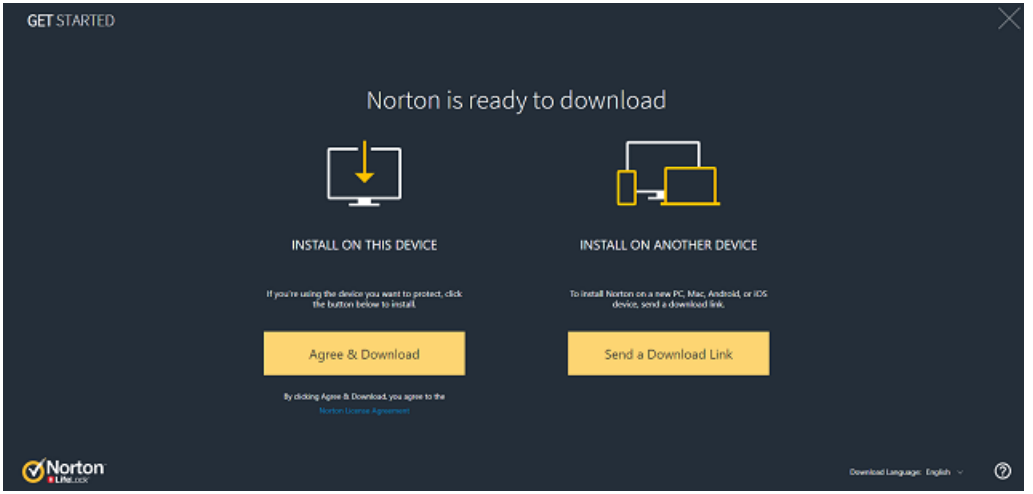
1 ノートンにサインインします。

2 ノートン アカウントにサインインしていない場合は、電子メールアドレスを入力して[サインイン]をクリックします。

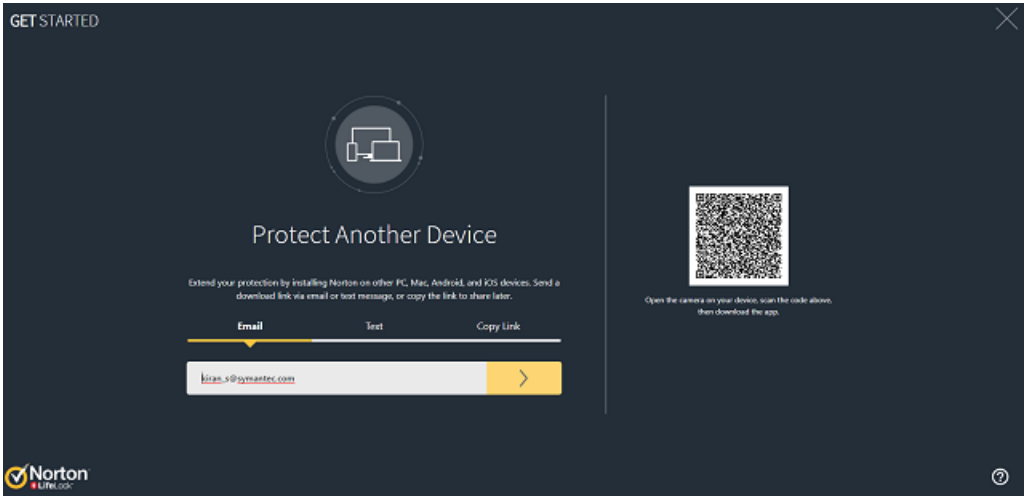
3 [開始する]ウィンドウで、[ノートンをダウンロードする]をクリックします。



4 表示されるページで[ダウンロードリンクを送信]をクリックします。



5 追加デバイスでアクセスできる電子メールアドレスを入力して、[送信する]ボタンをクリックし、[完了]ボタンをクリックします。



ノートン製品のインストール方法を記載した電子メールが電子メールアドレスに送信されます。

6 ノートンをダウンロードするデバイスで、ノートンチーム (The Norton Team) から受信した電子メールを探して開きます。

7 [今すぐダウンロード]をクリックします。

8 [同意してダウンロードする]をクリックします。

9 パソコンにファイルを保存し、そのファイルをダブルクリックしてノートンをインストールします。デフォルトでは、ファイルは Mac と Windows パソコンの両方で Downloads フォルダに保存されます。

画面の指示に従って操作します。

ノートンのライセンスの新しいデバイスへの移行

ノートン製品がすでに使用していないデバイスにインストールされている場合、ノートン アカウントを使用してそのデバイスから別のデバイスへノートン製品を移行できます。

ノートン ライセンスの移行

1 ノートン アカウントにサインインします。

2 [デバイス]ページで、保護しない製品を特定します。

メモ: デバイスは緑のステータスで表示されます。使用しないデバイスが赤またはオレンジのステータスで表示される場合は、ノートン アカウントからそのデバイスを削除して、ライセンスを別のデバイスで利用できます。

---

3 デバイスの下の省略記号 (...) アイコンをクリックします。

4 表示されるメニューで[ライセンスの管理]をクリックします。

5 [デバイスの管理]ページで、以下の手順を実行します。

- デバイス名をクリックします。
- [実行したい管理作業の選択]で、[ノートンの削除]をクリックします。
- [次へ]をクリックします。

6 表示される[ノートンの削除]ウィンドウで、[はい]をクリックします。

7 表示されるページで[今すぐインストール]をクリックします。

8 [新しいデバイスにインストール]ページで次のいずれかを選択します。

- 現在のデバイスにノートンをインストールするには、[ダウンロード]をクリックします。
- 別のデバイスにノートンをインストールするには、[リンクを送信]をクリックします。

9 [次へ]をクリックします。

10 画面の指示に従ってインストールを完了します。

ノートン ブータブルリカバリツールでのトラブルシューティング

ノートン セキュリティをインストールできない場合、ノートン セキュリティを開けない場合、パソコンを起動できない場合は、ノートン ブータブルリカバリツールを使って問題を解決できます。

ノートン ブータブルリカバリツールはウイルス、スパイウェア、その他のセキュリティリスクをスキャンして削除します。ノートン ブータブルリカバリツールは、DVD または USB ドライブからのみ実行できます。

メモ: ノートン ブータブルリカバリツールは、ウイルスやセキュリティリスクからのリアルタイム保護機能の代わりとなるものではありません。

手順 1: 感染していないパソコンでノートン ブータブルリカバリツールの ISO ファイルをダウンロードする

ISO ファイルをダウンロードするには

1. ブラウザを開き、次の URL に移動します:

   http://norton.com/nbrt

2. [ダウンロード]をクリックします。
3. 画面の指示に従ってノートン ブータブルリカバリツールの ISO ファイルをダウンロードして保存します。

手順 2: ノートン ブータブルリカバリツールのブータブルメディアを作成する

ノートン ブータブルリカバリツールの ISO ファイルは、ブート可能メディアとして任意のツールを使って DVD または USB ドライブに書き込むことができます。その後に、任意の感染したパソコンでノートン ブータブルリカバリツールを実行できます。この DVD は、任意のパソコンでリカバリ DVD として使うこともできます。

警告: ノートン ブータブルリカバリツールを再書き込み可能な DVD または USB ドライブに作成する場合、その DVD または USB ドライブ上のすべてのデータは完全に削除されます。再書き込み可能な DVD または USB ドライブにノートン ブータブルリカバリツールを作成する前に、データをバックアップしてください。

メモ: USB ドライブでノートン ブータブルリカバリツールを作成する場合、USB ドライブには 1 GB 以上の容量があり、FAT32 ファイルシステムでフォーマットされている必要があります。

手順 3: ノートン ブータブルリカバリツールを起動する

DVD または USB ドライブでノートン ブータブルリカバリツールを作成したら、そのメディアを使ってノートン ブータブルリカバリツールを実行します。

ノートン ブータブルリカバリツールを起動するには

1. 作成したノートン ブータブルリカバリツールの DVD または USB ドライブを挿入します。
2. 感染したパソコンの電源を入れるか、または再起動してすぐに表示されるキーを押して BIOS モードに入ります。
3. ノートン ブータブルリカバリツールを作成した DVD または USB ドライブを選択して、Enter キーを押します。UEFI 対応のパソコンを使っている場合は、[UEFI ブート]オプションではなく、[レガシーブート]オプションの下にあるリカバリメディアを選択します。リカバリメディアはノートン ブータブルリカバリツールの DVD または USB ドライブです。
4. [NBRT へようこそ]ページで、[ブート]オプションを選択します。ブートに失敗した場合は、[ブート (基本ビデオ)]オプションを選択します。
5. [言語の選択]ドロップダウンリストで言語を選択し、[OK]をクリックします。
6. ノートン製品使用許諾契約を参照し、[同意]をクリックしてツールを起動します。

手順 4: 脅威をスキャンして解決する

ノートン ブータブルリカバリツールは、既知のすべてのセキュリティ脅威を識別してリストに表示します。潜在的なリスクとして識別された項目の処理方法を選択できます。

脅威をスキャンして解決するには

1. ノートン製品使用許諾契約を参照し、[同意]をクリックしてツールを起動します。
2. [パソコンのスキャン]セクションで[スキャンを開始]をクリックします。

   スキャンが完了すると、[スキャンが完了しました]ウィンドウに次の項目がリストに表示されます。

   - スキャンしたファイルの合計
   - 検出された脅威の合計
3. [スキャンが完了しました]ウィンドウでスキャン結果を確認し、次のいずれかの操作を実行します。
   - パソコンで見つかったすべての脅威を解決するには、[処理]列を選択します。
   - それぞれの脅威に適切に対処するには、[処理]列の関連する脅威の中から解決するものを選択します。

メモ: 削除されたファイルをパソコン上に復元することはできないため、脅威を解決する前にスキャン結果を慎重に確認してください。

4 [解決]をクリックします。

5 確認ダイアログボックスで[OK]をクリックします。

6 [修復]ウィンドウの[処理]列に各脅威の状態が表示されます。

7 [続行]をクリックします。

8 [パソコンの再ブート]ウィンドウで[再ブート]をクリックし、パソコンを再起動します。

スキャンを再実行する場合は、[再びスキャン]をクリックします。

インターネットに接続している状態でスキャンを開始すると、ノートン ブータブルリカバリツールはシマンテックサーバーから最新のウイルス定義を自動的にダウンロードして更新します。最新のウイルス定義を使うと、最新のウイルスとセキュリティの脅威からパソコンを保護できます。

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、オンラインの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。

3

脅威を理解して対応する

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うこともできます。

ノートン デバイスセキュリティを最新の状態に維持する

自動ライブアップデートをオフにしていたか、パソコンをオフラインで使用していた場合は、前回ノートン デバイスセキュリティの更新を受信した日時を確認し、必要に応じてライブアップデートを実行することで最新の

- ウイルス定義を取得できます。最新のウイルス定義によって、マルウェア、権限がないネットワークアクセス、スパム電子メールなどからデバイスを保護できます。
- プログラム更新を取得できます。プログラム更新によって、オペレーティングシステムまたはハードウェアの互換性の拡張やパフォーマンスの問題の調整、プログラムエラーの修正が行われます。

ライセンスの有効期間内であれば、新種の脅威からの保護に役立つ更新が自動的に取得されます。

ノートンの前回の更新日を確認

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]をクリックします。

3 セキュリティの状態インジケータで、[保護情報の更新]の横の日付を確認します。

4 日付が昨日か一昨日より前である場合は、ライブアップデートを実行します。

ライブアップデートを実行してノートンの最新の更新版を取得する

メモ: インターネットに接続していることを確認します。

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

何らかの理由でライブアップデートに失敗した場合は、Intelligent Updater を実行して最新の更新を取得できます。

ライブアップデートに失敗した場合に Intelligent Updater を実行する

1 Intelligent Updater ダウンロードページに移動します。

2 Windows のバージョンに応じて、次のいずれかを実行します。

- Windows 8.1、8、7、Vista、XP の 32 ビット版の場合: ファイル名の下の最初のファイルをクリックします。ファイル名は、西暦で始まり v5i32.exe で終了します。たとえば、20130528-017-v5i32.exe などが挙げられます。
- Windows 8.1、8、7、Vista の 64 ビット版の場合: 64 ビットプラットフォームセクションに移動して、ファイル名の下の最初のファイルをクリックします。ファイル名は、西暦で始まり v5i64.exe で終了します。たとえば、20130528-017-v5i64.exe などが挙げられます。

3 ファイルを Windows のデスクトップに保存します。

4 デスクトップで、保存したファイルをダブルクリックします。

ノートン自動ライブアップデート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、[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、[更新]タブをクリックします。

5 [自動ライブアップデート]行で、スイッチを[オン]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。

デバイスを再起動しないで更新が適用されるようノートンを設定する

メモ: Windows 7 と 8.1 以降のデバイスでは、パソコンを再起動しないで更新を適用できます。

---

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、[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、[更新]タブをクリックします。

5 [再起動時にのみ更新を適用]行で次のいずれかの操作をします。

- 再起動せずに更新を適用するかどうかを確認するライブアップデート通知を受信するには、スイッチを[オフ]の位置に動かします。これはデフォルトの設定です。
- パソコンの再起動後にのみ更新を適用するには、スイッチを[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。

ノートンが検出したデバイスのセキュリティの脅威を表示し、修正する

ノートンが脅威を検出したときに、脅威の解決方法に関するユーザーからの指示が必要がない場合は、その脅威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、その脅威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

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。

未解決のリスクを解決できない場合にノートン パワーイレイサーを実行する

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。

メモ: ノートン パワーイレイサーは、強力なマルウェア駆除ツールです。ノートン パワーイレイサーによってマルウェアとともに正当なファイルも削除されることがあるため、ファイルを削除する前にスキャン結果を十分に確認する必要があります。

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

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。

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。

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。

シマンテック社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。シマンテック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[シマンテック社に提出]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。

4

セキュリティ管理

この章では以下の項目について説明しています。

システム活動を表示する

ノートン製品は、過去 3 カ月間に実行した重要なシステム活動に関する情報を提供します。

ノートン製品は、パソコンのパフォーマンスを監視します。プログラムまたはプロセスによるシステムリソースの使用率の増加が検出されると、パフォーマンス警告を表示します。

システム活動の詳細を表示する

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、[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]ウィンドウで、詳細を確認する月のタブをクリックします。
4. イベントグラフで、活動を示すアイコンまたはストライプをマウスで指します。
5. 表示されたポップアップで、活動の詳細を確認します。
6. ポップアップに[詳細を表示]オプションが表示された場合は、[詳細を表示]をクリックすると、[セキュリティ履歴]ウィンドウに追加の詳細が表示されます。

レポートカードの表示

[レポートカード]には、ノートンが実行したすべての活動が毎月自動的に表示されます。ノートンのメインウィンドウで、[レポートカード]をクリックしてレポートを手動で開くこともできます。

ノートンがファイルをスキャンする、ライブアップデートを実行する、ダウンロードを分析する、侵入を遮断する、感染したファイルを修復するたびに、活動に関する情報がレポートカードに記録されます。[レポートカード]ウィンドウで[詳細]オプションを選択すると、ノートンが実行した活動の詳細なリストが表示されます。

レポートカードを毎月自動的に表示しない場合は、このオプションをオフにできます。その場合にも手動でレポートを開くことができます。

レポートカードをオフにする

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、[管理の設定]をクリックします。

4 [レポートカード]行で、[オン/オフ]スイッチを[オフ]に移動します。

レポートカードを手動で表示する方法

ノートンのメインウィンドウで[レポートカード]オプションを使用してレポートを手動で表示することもできます。[レポートカード]オプションは、ノートンがパソコンで何らかの活動を行った場合にのみ利用できます。

5

パソコンのスキャン

この章では以下の項目について説明しています。

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利用してスキャンする

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[スキャン]をクリックします。

3 [スキャン]ウィンドウの[ノートン パワーイレイサー]で、[ノートン パワーイレイサー]をクリックします。

4 [実行]をクリックします。

5 [ノートン パワーイレイサー]ウィンドウで[OK]をクリックします。

6 ノートン パワーイレイサーのメインウィンドウで[高度な保護]をクリックします。

7 [システムスキャン]をクリックします。

8 スキャン結果を確認して、画面上の指示に従って検出されたセキュリティリスクを解決します。

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。

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スキャンはリムーバブルメディアを挿入するとウイルスを調べます。この処理は数秒で完了します。スキャンが完了すると、そのリムーバブルメディアは再挿入するかフォーマットするまで再スキャンされません。リムーバブルメディアの感染がまだ疑われる場合は、自動保護をオンにしてリムーバブルメディアを挿入し、メディアをエクスプローラーで開いて自動保護で再スキャンします。リムーバブルメディアを手動でスキャン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 (Symantec Online Network for Advanced Response の略) 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。

ノートン SONAR 保護が検出するリアルタイムの脅威を表示する

SONAR (Symantec Online Network for Advanced Response の略) 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。

SONAR 保護は常にオンのままにしておいてください。

メモ: 自動保護をオフにすると SONAR 保護も無効になり、パソコンは新しい脅威から保護されなくなります。

[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]スイッチを動かして、[オフ]または[オン]にあることを確認します。

わずかな期間でもスイッチをオフにすると、リアルタイム保護機能が無効になり、パソコンが脆弱になる可能性があります。

5 [適用]をクリックします。

6 スイッチをオフにした場合は、SONARを無効にする期間を選択して[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。

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。

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、スクリプトコントロール、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。

スキャン時に除外されるファイル ID を消去する

スキャンを実行するとき、ノートン製品は、スキャンの除外に追加されたファイルを除外します。ノートンでパソコン内のすべてのファイルをスキャンする場合、そのファイルの ID を消去する必要があります。

スキャン時に除外されたファイルの ID を消去する

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[スキャン時に除外されるファイル ID を消去]行で、[すべてクリア]をクリックします。

6 [警告]ウィンドウで、[はい]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、対策を取るように促します。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。ID に基づいて、悪質なプロセスがパソコンで処理を実行できないようにします。より積極的にファイルを保護するため、安全なプロセスでも、ランタイム中に悪質なファイルが挿入された場合は遮断されます。デフォルトでは、データプロテクタはオンになっており、事前設定されているフォルダと拡張機能を保護します。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、

  をクリックし、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

[スクリプトコントロール]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疑わし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。

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コンピュータ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、[スクリプトコントロール]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.38 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、[スクリプトコントロール]を選択します。

4 [スクリプトコントロール]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 [スクリプトコントロールの復元]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。

[スクリプトコントロール]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]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、[スクリプトコントロール]タブをクリックします。

5 [ドキュメントのダウンロード時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。

すべてのスクリプトコントロール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、[スクリプトコントロール]を選択します。

4 [スクリプトコントロール]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、[スクリプトコントロール]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、Adobe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 [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。

FAQ: ノートン スクリプト制御

スクリプトとは何ですか? また、なぜノートンはこれを削除するのですか?

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。

スクリプトには次のものがあります。

- 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 オブジェクト
- カラーテーマファイル

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フィッシングの試行で攻略して、ユーザーのコンピュータ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。

スクリプトを削除すると問題が発生しますか?

それは場合によって異なります。そのドキュメントに含まれているスクリプトによって対話性や追加コンテンツのダウンロードなどの機能が実現されている場合、スクリプトを削除するとそれらの機能は動作しなくなります。

[スクリプト制御]をオフにしても保護されていることになりますか?

ノートンはドキュメント内でマルウェア (スクリプトによって埋め込まれたマルウェアを含む) が実行されようとするとそれを検出するため、保護は引き続き有効です。[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。

元のファイルに戻すことはできますか?

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。

潜在的な脅威が検出された場合、ノートンはどのアプリケーションを遮断しますか?

潜在的に危険な活動を検出すると、ノートンは次のアプリケーションの起動を遮断します。

- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Word

これらのアプリケーションに加えて、ノートンは Adobe のドキュメント、一般的なデベロッパーユーティリティ、WMI (Windows Management Instrumentation) ツール、コマンドラインインターフェース、スクリプティングインターフェースを検出して遮断します。

スクリプトを遮断するタイミングがドキュメントをダウンロードするときかドキュメントを開くときかで、どう違いますか?

スクリプトが埋め込まれたドキュメントをダウンロードすると、スクリプト制御は自動保護 を使用して疑わしいスクリプトを検出します。自動保護は、ノートンがウイルス定義の更新中に受信する脅威シグネチャやその他のセキュリティ更新によって、ダウンロードしたファイルの安全性を判別します。

スクリプトが埋め込まれたドキュメントを開くと、スクリプト制御は SONAR 保護を使用して、潜在的に危険な活動を検出します。ファイルの動作に基づいて潜在的な脅威を識別し、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。

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 [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] オプションを使用できます。

スクリプト制御の両方のオプションを常にオンにすることを推奨します。

6

インターネット上でのセキュリティを確保

この章では以下の項目について説明しています。

- データ通信ポリシーのオンとオフを切り替える
- Wi-Fi セキュリティ
- ノートン セーフウェブを使用した銀行情報の保護

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性に影響し、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を許可する

時に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。プログラムのインターネットアクセスの設定を手動で決定したい場合にはプログラムの自動制御をオフにします。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、アクセスの設定を要求する警告が表示されます。

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。

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。

[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。

侵入防止除外リスト

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]を使うと、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には

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。

エクスプロイト、サイバー犯罪者、ゼロデイ攻撃などの脅威から保護するためノートンを設定する

ゼロデイ攻撃とは、サイバー犯罪者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サイバー犯罪者にさらされることがあります。

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

リモートのサイバー犯罪者が Java プロセスから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
  リモートのサイバー犯罪者が、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。

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不正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。

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。

自動遮断で遮断しているパソコンの遮断を解除する

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。

Wi-Fi セキュリティ

Wi-Fi セキュリティの機能により、MITM 攻撃、SSLStrip 攻撃、コンテンツ改ざん攻撃、ARP 詐称攻撃、DNS 詐称攻撃から保護します。

フリー Wi-Fi 接続は中間者 (MITM) 攻撃に対して脆弱です。MITM 攻撃は、攻撃者がユーザーと Wi-Fi プロバイダとの間に入り込むことにより行われます。信頼できる Wi-Fi プロバイダに接続していると思っていても、実際には悪質なツールに接続し、キー入力やパスワードがすべて記録されます。

あなたが信頼するネットワークをノートンが MITM 攻撃として識別した場合はどうしたらよいでしょうか。

ノートンが既知の信頼できるネットワークを MITM 攻撃として識別した場合は、そのネットワークを信頼できるネットワークのリストに追加します。ノートンは、MITM 攻撃のような動作を識別したときに通知します。警告に対して[信頼]をクリックした場合は、次回そのネットワークにアクセスしても通知を受け取ることはなくなります。誤って[切断]をクリックした場合は、[セキュリティ履歴]を使用して信頼できるネットワークに追加し直すことで、ノートンが以前に遮断したネットワークを信頼できます。

ノートンが以前に遮断したネットワークを信頼するには

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]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、[Wi-Fi セキュリティ]を選択します。

4 特定のアクティビティを選択し、[その他のオプション]をクリックします。

5 [セキュリティ履歴 - 詳細]ウィンドウで、[このネットワークを信頼]をクリックします。

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。

7

機密データを保護

この章では以下の項目について説明しています。

ノートンのブラウザ拡張機能を追加する

ノートンをインストールした後に、Web ブラウザにノートンのブラウザ拡張機能を追加するように求められます。ノートンは、Google Chrome、Microsoft Internet Explorer、Mozilla Firefox、Microsoft Edge の各ブラウザに拡張機能を追加します。

ノートン パスワード マネージャーのブラウザ固有のすべての機能に簡単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。 p.73 の「ノートン セーフウェブのオンとオフを切り替える」を参照してください。
ノートン セーフサーチ	検索結果、サイトの安全性の状態とノートン評価に基づきランク付けする安全な検索エンジン。
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 検索機能を強化する Web ページ。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、口座情報などの重要な情報のすべてを保存できる安全なオンラインロケーションです。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。

メモ: Internet Explorer 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が必要です。

Google Chrome

Google Chrome にノートンのブラウザ拡張機能を追加する

ノートンは 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

Google 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. ノートン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。

メモ: Internet Explorer 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が必要です。

Mozilla Firefox

Mozilla Firefox にノートンのブラウザ機能を追加する

ノートンは Mozilla 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

Mozilla 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 ノートン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]をクリックすると拡張機能のページが表示されます。

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。

メモ: Internet Explorer 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が必要です。

ノートン セーフウェブのオンとオフを切り替える

ノートン セーフウェブは、Internet Explorer、Firefox、Google Chrome、または Microsoft Edge を使って閲覧、検索、またはオンラインショッピングを行うユーザーを保護します。表示する Web サイトのセキュリティレベルを分析し、Web サイトが脅威を受けていないかどうかを示します。検索結果の横にサイト評価アイコンが表示されるため、Web サイトにアクセスする前に、そのサイトが悪質かどうかを確認することができます。

Google Chrome の[拡張機能]ページからノートン セーフウェブのオンとオフを切り替える

1. Google Chrome を起動します。
2. 右上の[設定]をクリックします。
3. [設定]ウィンドウで、[その他のツール]をクリックしてから[拡張機能]をクリックします。
4. [拡張機能]ページでノートン セーフウェブが有効になっている場合、[有効]のチェックマークをはずします。

   ノートン セーフウェブが無効になっている場合、[有効]ボックスにチェックマークを付けます。
5. Google Chrome を再起動します。

Mozilla Firefox の[アドオン]ページからノートン セーフウェブのオンとオフを切り替える

1. Mozilla Firefox を起動します。
2. Firefox メニューで[アドオン]をクリックします。
3. [拡張機能]タブで[有効化]をクリックします。

   ノートン セーフウェブがグレー表示されていない場合、[無効化]をクリックします。
4. Mozilla Firefox を再起動します。

Safari の[拡張機能]ページからノートン セーフウェブのオンとオフを切り替える

1. Safari を起動します。
2. Safari のメニューで、[Safari]、[環境設定]の順に選択します。
3. [拡張機能]をクリックします。
4. 左のペインでノートン セーフサーチが有効になっている場合、[有効]のチェックマークをはずします。

   ノートン セーフサーチが無効になっている場合、[有効]ボックスにチェックマークを付けます。

Microsoft Edge の[拡張機能]ページからノートン セーフウェブのオンとオフを切り替える

1 Microsoft Edge を起動します。

2 右上に表示される[設定など]をクリックします。

[拡張機能]を選択します。

3 [拡張機能]ウィンドウで[その他の拡張機能を探す]をクリックします。

4 [ストア]ウィンドウの検索フィールドに「ノートン」と入力します。

5 検索結果で、[ノートン セーフウェブ]をクリックし、[インストール]をクリックします。

6 拡張機能をインストールしたら[起動]をクリックします。

7 [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。

ポップアップウィンドウが表示されなかった場合は、Microsoft Edge の右上に表示される[設定など]をクリックし、

[拡張機能]を選択します。

8 [ノートン セーフウェブ]ウィンドウの[ノートン セーフウェブ]で、スライダーを[オン]に切り替えます。

ノートン セーフウェブ拡張機能をオフにするには、スライダーを[オフ]に切り替えます。

ノートン セーフサーチを使って Web を検索する

ノートン セーフサーチは Web 検索操作を拡張します。ノートン セーフサーチを使用してインターネットを検索すると、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、生成された検索結果ごと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 セーフサーチは、検索語句のいくつかの文字を入力したときに検索のヒントを表示する高度なインクリメンタル機能を提供します。

メモ: ノートン セーフサーチ機能は、オーストラリア、ベルギー、ブラジル、カナダ、デンマーク、フィンランド、フランス、ドイツ、イタリア、日本、オランダ、ノルウェー、スペイン、スウェーデン、スイス、米国、英国など、一部の地域でのみ利用可能です。プライバシー保護機能は、米国、英国、カナダでのみ利用可能です。

パスワード マネージャー機能をオフにしている場合でも、ノートン セーフサーチを使用できます。

メモ: ノートン セーフサーチをサポートするブラウザは、Internet Explorer、Firefox、Chrome のみです。

ノートン セーフサーチを使って Web を検索する

1. ブラウザを開きます。
2. ノートン セキュリティツールバーの[ノートン セーフサーチ]フィールドに、検索したい検索文字列を入力します。
3. 次のいずれかの操作をします。
   - [セーフサーチ]をクリックします。
   - 表示されるポップアップウィンドウで、検索文字列に一致する検索のヒントを選択します。

ツールバーの[ノートン セーフサーチ]フィールドを有効にする

メモ: この機能は Internet Explorer でのみ利用できます。

ノートンをインストールすると、ノートン セキュリティツールバーが Internet Explorer に追加されます。Internet Explorer を開くと、ツールバーの[ノートン セーフサーチ]フィールドを有効にすることを求めるメッセージが表示されます。

ノートン セーフサーチを手動で無効にした後、もう一度有効にする場合は、以下の手順に従います。

1. ブラウザを開きます。
2. ノートン セキュリティツールバーで、(...) アイコンをクリックします。
3. 表示されるメニューで、[ノートン セーフサーチ]の横のスイッチを[オフ]の位置に動かします。

[ノートン セーフサーチ]フィールドを有効にするには、次の操作を実行します。

1. ブラウザを開きます。
2. ノートン セキュリティツールバーで、(...) アイコンをクリックします。
3. 表示されたメニューで、[ノートン セーフサーチ]の横のスイッチを[オフ]の位置に動かします。

Web インサイト

Web インサイトを使うと、住基ネット個人 ID またはクレジットカードなどの重要な情報が詐欺サイトに漏えいするのを防止できます。評価ベースの脅威の検出を使って疑わしい Web サイトや脆弱な Web サイトを検出する場合に役立ちます。個人情報の入力が必要な Web サイトを主な対象としています。

[ノートン セーフウェブ]ポップアップウィンドウは、アクセスする Web サイトが安全か安全でないかを把握するのに役立ちます。

フィッシング対策

フィッシング対策によって、安全でない Web サイトを表示しないように保護されます。フィッシング対策機能は、ユーザーがアクセスするすべての Web サイトのセキュリティレベルを分析し、その結果を[ノートン セーフウェブ]ポップアップウィンドウに表示します。フィッシング対策は、詐欺サイトであると確認されている Web サイトへの移動も遮断します。

[ノートン セーフウェブ]ポップアップウィンドウは、アクセスする Web サイトが安全か安全でないかを把握するのに役立ちます。

ノートン パスワード マネージャーへのアクセス

次の領域からパスワード マネージャーにアクセスできます。

- Windows で、製品のメインウィンドウの[インターネットセキュリティ]セクションから
- ノートン パスワード マネージャー拡張機能から
- Android と iOS 上のノートン パスワード マネージャーアプリから

[Web 保護]ウィンドウの[ログイン情報]と[カード]オプションを使用して、[ログイン情報の管理]ウィンドウと[カードの管理]ウィンドウにそれぞれアクセスできます。

製品のライセンスが終了した後も、すべてのパスワード マネージャーデータにアクセスできます。次に、製品のライセンスが終了した後に表示またはアクセスできる機能を示します。

ログイン情報	オンライン銀行口座のログイン資格情報、電子メールのユーザー ID、パスワードなどの保存されたログイン情報を確認できます。
アドレス	名前、生年月日、住所、電子メールアドレス、電話番号などの保存された個人情報を確認できます。
ウォレット	クレジットカード情報、銀行口座情報、クレジット支払いの詳細などの保存された経済的情報を確認できます。
メモ	後で参照できるよう入力したテキストを確認できます。

メモ: パスワード マネージャー機能にアクセスするには、パスワード マネージャーにサインインする必要があります。パスワード マネージャー機能は、Internet Explorer、Firefox、Safari、Chrome ブラウザでサポートされます。

ノートン パスワード マネージャーアプリを Android または iOS にダウンロードしてインストール

1 次のいずれかの操作をします。

- Android では Play ストアに移動します。初めて Play ストアを開く場合は、利用規約画面が表示されます。[同意する]をタップして続行します。
- iOS では、ホーム画面の[App Store]アイコンをタップします。

2 ノートン パスワード マネージャーアプリを検索し、選択します。

3 次のいずれかの操作をします。

- Android では、アプリケーション詳細画面で[インストール]をタップして、[同意してダウンロード]をタップします。
- iOS では、[無料]をタップして、[App をインストール]をタップします。[Apple ID のパスワード]画面で、Apple アカウントのパスワードを入力します。

ノートン パスワード マネージャーのオンとオフを切り替える

パスワード マネージャーはパスワードの管理に役立ち、オンライントランザクションの実行中のセキュリティを強化することができます。パスワード マネージャーのさまざまな機能を使用して、住所、生年月日、クレジットカード情報などの個人データを管理できます。

パスワード マネージャーは、Google Chrome の[拡張機能]ページまたは Mozilla Firefox の[アドオン]ページからオンまたはオフに切り替えることができます。

Google Chrome の[拡張機能]ページからパスワード マネージャーをオンにする

1 Google Chrome を起動します。

2 右上の[設定]をクリックします。

3 [設定]ウィンドウで、[その他のツール]をクリックしてから[拡張機能]をクリックします。

4 [拡張機能]ページでノートン パスワード マネージャーが無効になっている場合、[有効]にチェックマークを付けます。

5 Google Chrome を再起動します。

Mozilla Firefox の[アドオン]ページからノートン パスワード マネージャーをオンにする

1 Mozilla Firefox を起動します。

2 Firefox メニューで[アドオン]をクリックします。

3 [拡張機能]タブで[ノートン パスワード マネージャー]をクリックします。

4 [ノートン パスワード マネージャー]がグレー表示されていない場合、[有効化]をクリックします。

5 Mozilla Firefox を再起動します。

Safari の[拡張機能]ページからノートン パスワード マネージャーをオンにする

1. Safari を起動します。
2. Safari のメニューで、[Safari]、[環境設定]の順に選択します。
3. [拡張機能]をクリックします。
4. 左のペインでノートン パスワード マネージャーが無効になっている場合、[有効]にチェックマークを付けます。

Google Chrome の[拡張機能]ページからパスワード マネージャーをオフにする

1. Google Chrome を起動します。
2. 右上の[設定]をクリックします。
3. [設定]ウィンドウで、[その他のツール]をクリックしてから[拡張機能]をクリックします。
4. [拡張機能]ページでノートン パスワード マネージャーが有効になっている場合、[有効]のチェックマークをはずします。
5. Google Chrome を再起動します。

Mozilla Firefox の[アドオン]ページからパスワード マネージャーをオフにする

1. Mozilla Firefox を起動します。
2. Firefox メニューで[アドオン]をクリックします。
3. [拡張機能]タブで[ノートン パスワード マネージャー]をクリックします。
4. [ノートン パスワード マネージャー]がグレー表示されている場合、[有効化]をクリックします。
5. Mozilla Firefox を再起動します。

Safari の[拡張機能]ページからノートン パスワード マネージャーをオフにする

1. Safari を起動します。
2. Safari のメニューで、[Safari]、[環境設定]の順に選択します。
3. [拡張機能]をクリックします。
4. 左のペインでノートン パスワード マネージャーが有効になっている場合、[有効]のチェックマークをはずします。

ノートン パスワード マネージャーのクラウドデータ保管庫を作成する

ノートン パスワード マネージャーを使用してクラウドデータ保管庫を作成し、ノートン パスワード マネージャーのデータを保存できます。ノートン アカウントごとにクラウドデータ保管庫を 1 つ作成できます。新しいローカルデータ保管庫を作成できません。ただし、ノートン製品をアップグレードするときに既存のローカルデータ保管庫のデータをクラウド型のデータ保管庫に移動できます。ノートン パ

スワード マネージャーのデータをローカルデータ保管庫からクラウドデータ保管庫に移動すると、ローカルデータ保管庫のデータにアクセスできなくなります。クラウドデータ保管庫により、移動中でもノートン パスワード マネージャーのデータを簡単に使用できます。

ノートン パスワード マネージャーのクラウドデータ保管庫には、インターネットに接続されているパソコンからアクセスできます。

ブラウザからクラウドデータ保管庫を作成する

1. ブラウザを開きます。
2. ブラウザの右上にある[ノートン パスワード マネージャー]をクリックします。
3. ノートン パスワード マネージャーのサインイン画面で、[サインイン]をクリックします。
4. [ノートンにようこそ]ウィンドウが表示されたら、[アカウントの作成]をクリックします。
5. [アカウントの作成]タブで詳細を入力し、[アカウントの作成]をクリックします。
6. [データ保管庫は検出されませんでした]ウィンドウで、[データ保管庫を作成する]をクリックします。
7. [データ保管庫を作成する]ウィンドウで、パスワードを入力し、[次へ]をクリックします。

   使用するパスワードは、所定の基準をすべて満たす必要があります。
8. 再度パスワードを入力し、[次へ]をクリックします。
9. パスワードを思い出すためのヒントを入力し、[データ保管庫を作成する]ボタンをクリックします。
10. [セットアップ完了]ウィンドウで、[データ保管庫に移動する]ボタンをクリックします。

ノートンでクラウドデータ保管庫を作成する

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、[インターネットセキュリティ]をダブルクリックしてから[パスワード マネージャー]をクリックします。
3. [始めましょう]ウィンドウで[サインイン]をクリックします。

   ノートン アカウントを持っていない場合は、[今すぐサインアップ]リンクを使って新しいノートン アカウントを作成します。
4. [新しいデータ保管庫の作成: パスワード マネージャーパスワード]ウィンドウの[パスワード マネージャーパスワード]ボックスに、パスワードを入力し、[次へ]をクリックします。
5. [データ保管庫の作成: パスワードの確認]ウィンドウに、確認のためにパスワードを再び入力し、[次へ]をクリックします。

6 [データ保管庫の作成: パスワードのヒント]フィールドにパスワードのヒントを入力し、[次へ]をクリックします。

パスワード マネージャーデータのバックアップがすでにある場合は、[インポート]をクリックし、新しいアカウントに結合するバックアップファイルを選択します。

7 [完了]をクリックします。

Android または iOS でクラウドデータ保管庫を作成する

1 ノートン パスワード マネージャーアプリにログオンします。

2 [サインイン]ウィンドウで、ノートン 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ます。

3 [サインイン]をタップして、画面上のインストラクションに従います。

ノートン パスワード マネージャーのクラウドデータ保管庫を削除する

クラウド型のデータ保管庫は暗号化されて、ノートン アカウントのパスワードとデータ保管庫用のパスワードを使用する方法でのみアクセスできます。クラウド型のデータ保管庫の削除は手動で実行する必要があります。デバイスからノートンをアンインストールした場合でも、他のデバイスから引き続きデータ保管庫を使えます。

警告: データ保管庫を削除すると、データ保管庫に保管したすべてのパスワード マネージャーデータが完全に削除されます。後でデータ保管庫のデータを使う可能性があると思われる場合は、データ保管庫を削除しないでください。

ブラウザからクラウドデータ保管庫を削除する

1 ブラウザを開きます。

2 ブラウザの右上にある[ノートン パスワード マネージャー]をクリックします。

3 表示されるポップアップで[データ保管庫を開く]をクリックします。

4 [データ保管庫のロックを解除する]ウィンドウにデータ保管庫のパスワードを入力し、[データ保管庫を開く]をクリックします。

5 ノートン パスワード マネージャー拡張機能のアイコンをクリックして、[データ保管庫]をクリックします。

6 [ノートン パスワード マネージャー]ウィンドウで、

記号をクリックし、[設定]ページを起動します。

7 [データ保管庫の削除]をクリックします。

8 ノートン サインインページでログイン資格情報を入力し、[サインイン]をクリックします。

9 [データ保管庫の削除]ページで、[はい、データ保管庫を削除します]をクリックします。

ノートンからクラウドデータ保管庫を削除する

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、[インターネットセキュリティ]をダブルクリックしてから[パスワード マネージャー]をクリックします。

3 [データ保管庫は閉じています]ウィンドウで、不正なパスワードを 3 回入力します。

4 [データ保管庫を削除する必要がありますか。]の横にある[ここをクリック]リンクをクリックします。オプションの横に表示されるので、これをクリックします。

5 [データ保管庫の削除]ウィンドウで、[はい、データ保管庫を削除します]をクリックします。

6 [警告]ダイアログボックスで、[はい]をクリックします。

7 検証のためにノートン アカウントのパスワードを入力して[サインイン]をクリックします。

8 確認ウィンドウで[OK]をクリックします。

ノートンをアンインストールした後にクラウド型のデータ保管庫アカウントにアクセスする方法

1 ノートン アカウントの資格情報を使用してノートン パスワード マネージャー Web サイトにサインインします。

2 [データ保管庫を開く]ウィンドウにデータ保管庫のパスワードを入力し、[データ保管庫を開く]をクリックします。

ノートン パスワード マネージャーのデータをエクスポートする

セキュリティ目的やデータ回復のため、またはパスワード マネージャーデータを新しいパソコンに移す場合に、パスワード マネージャーデータをエクスポートできます。データ保管庫パスワードはリセットできません。そのため、データ保管庫のバックアップを定期的に作成することを推奨します。自動バックアップ機能を有効にすると、データ保管庫のバックアップが自動的に作成され、ローカルデバイスに保存されます。

製品のライセンスが終了したときは、パスワード マネージャーデータを取り込むことができます。

メモ: ノートン パスワード マネージャーは、ノートン パスワード マネージャー (.NPM) ファイルのエクスポートを許可しません。

ブラウザからノートン パスワード マネージャーのデータをエクスポートする

1. ブラウザを開きます。
2. ブラウザの右上にある[ノートン パスワード マネージャー]をクリックします。
3. 表示されるポップアップで[データ保管庫を開く]をクリックします。
4. [データ保管庫のロックを解除する]ウィンドウにデータ保管庫のパスワードを入力し、[データ保管庫を開く]をクリックします。
5. ノートン パスワード マネージャー拡張機能のアイコンをクリックして、[データ保管庫]をクリックします。
6. [ノートン パスワード マネージャー]ウィンドウで、

   をクリックして[データ保管庫をエクスポート]をクリックします。
7. [保護対象のデータ保管庫の処理]ウィンドウで、ノートン パスワード マネージャーのデータのエクスポートに使用するデータ保管庫のパスワードを入力します。

ノートンからノートン パスワード マネージャーのデータをエクスポートする

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、[インターネットセキュリティ]をダブルクリックしてから[パスワード マネージャー]をクリックします。
3. [ノートン パスワード マネージャー]ウィンドウの下部に表示される[設定]アイコンをクリックします。
4. [インポート/エクスポート]タブをクリックします。
5. [エクスポート]ウィンドウで、ファイル形式を選択します。

   次のいずれかを選択できます。

   - パスワード マネージャーのバックアップ形式 – DAT ファイル
     セキュリティの向上のためにパスワードを設定してデータのバックアップを作成したい場合、パスワードを入力して確認します。
   - [テキスト形式 - CSV ファイル (ログイン情報とメモのみ)]

   データ保管庫のバックアップは My Documents¥Norton Password Manager Backups¥<ノートン アカウント名> にあります。
6. [エクスポート]をクリックします。

7 [パスワード マネージャーパスワードを確認]ウィンドウで、パスワード マネージャーデータのエクスポートに使用するパスワード マネージャーパスワードを入力します。

8 確認ダイアログボックスで[OK]をクリックします。

ノートン パスワード マネージャーのデータをインポートする

以前にバックアップしたファイルからパスワード マネージャーデータをインポートできます。データ保管庫の自動バックアップは、自動バックアップ機能が有効な場合にのみ実行されます。自動バックアップフォルダのデフォルトの場所は C:¥Documents¥Norton Password Manager です。

[既存のデータにインポートしたデータを結合する]と[インポートしたデータで既存のデータを置換する]オプションは、バックアップファイルからノートン パスワード マネージャーのデータをインポートする場合に表示されます。インポートしたデータを現在サインインしているデータ保管庫と結合することも、データ保管庫に保存している既存のデータを置き換えることもできます。

メモ: インポート時のファイルサイズは、.CSV ファイルの場合は 15 MB 以下である必要があります。また、ノートン パスワード マネージャーではノートン パスワード マネージャー (.NPM) ファイルのインポートを許可しません。

ノートンからノートン パスワード マネージャーのデータをインポートする

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、[インターネットセキュリティ]をダブルクリックしてから[パスワード マネージャー]をクリックします。

3 [ノートン パスワード マネージャー]ウィンドウの下部に表示される[設定]アイコンをクリックします。

4 [インポート/エクスポート]タブをクリックします。

5 [インポート]行で、[インポート]をクリックします。

6 [データ保管庫のインポート]ウィンドウで、次のいずれかのオプションを選択します。

- [既存のデータにインポートしたデータを統合する]
- [インポートしたデータで既存のデータを置換する]

7 [インポート]をクリックします。

8 インポートするファイルの場所を参照します。

データ保管庫のバックアップは My Documents¥Norton Password Manager Backups¥<ノートン アカウント名> にあります。

9 そのファイルを選択してから[開く]をクリックします。

10 現在使っているデータ保管庫とインポートするデータ保管庫に格納したログイン情報のパスワードが異なる場合は、確認メッセージが表示されます。次のいずれかを選択します。

- クラウド型のデータ保管庫に格納されているパスワードを保持するには、[既存のパスワードを保存する]をクリックします。
- クラウド型のデータ保管庫に格納されているパスワードをインポートするデータ保管庫に格納されているパスワードで上書きするには、[インポートしたパスワードを保存する]をクリックします。

11 確認ダイアログボックスで[OK]をクリックします。

ノートン セキュリティツールバーを有効または無効にする

ノートン セキュリティツールバーが有効になっている場合、[ノートン セーフウェブ]ポップアップウィンドウと、アクセスする Web サイトのセキュリティランキングがノートン パスワード マネージャーに表示されます。ツールバーが無効になっている場合、ノートン パスワード マネージャーに[ノートン セーフウェブ]ポップアップウィンドウは表示されませんが、疑わしいサイトや詐欺サイトについては通知されます。

ノートン セキュリティツールバーを有効または無効にする

◆ 希望のブラウザを開きます。

- Internet Explorer で、メニューバーを右クリックし、[ノートン セキュリティツールバー]のチェックマークを付けるかはずして有効または無効にして、画面上の指示に従います。
- Safari で、[表示] > [ツールバーのカスタマイズ]の順にクリックして、有効または無効にするノートン セキュリティツールバー拡張機能をドラッグアンドドロップします。

8

パソコンのチューンナップ

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。

パソコンを最適化する

パソコンのハードディスクを最適化するとパフォーマンスと信頼性が向上する可能性があります。ノートンはハードディスクの断片化を自動的に調べ、10% を超えて断片化している場合にはディスクを最適化します。最適化が必要かどうかを確認するために最新レポートを常に調べることができます。

ディスクの最適化は、ディスクに 15% を超える空き領域がある場合にのみ実行できます。ディスクの最適化処理中にソリッドステートドライブ (SSD) が断片化解消されるのは Windows 8 以降のオペレーティングシステムのみです。

ハードディスクを最適化する

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[ディスクの最適化]をクリックします。

3 活動が完了したら、[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。

使用しているファイルのノートン信頼レベルを表示または変更する

ノートン インサイトは評価に基づいてファイルまたはアプリをホワイトリストに登録し、ファイルの信頼レベルとパソコン上の信頼できるファイルの割合を表示します。信頼できるファイルはスキャンから除外されるので、信頼できるファイルの割合が高くなるほどスキャンの実行が速くなります。

ノートン インサイトでは、ノートン コミュニティで使用率の高いファイルに加え、ノートン ネットワークで信頼されているファイルと信頼できないとされているファイルが表示されます。ファイルインサイトでは、ファイルのシグネチャ、インストール日、リソース使用率、ソースなど、より詳細な情報が得られます。安全と考えられるファイルに対してノートンが低度の信頼評価を与えた場合も、ノートンがそのファイルを信頼するように設定できます。ただし、そのような設定は推奨されません。

使用しているファイルのノートン信頼レベル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、[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]ウィンドウで、[ノートン インサイト]を選択し、[実行]をクリックします。

4 [ノートン インサイト]ウィンドウの[信頼レベル]タブで、[表示]ドロップダウンリストのオプションを選択して、ファイルのカテゴリを表示します。

詳細領域に表示されているすべてのファイルを表示するために下へのスクロールが必要な場合があります。

5 リスト内の任意のファイルをクリックして、ファイルのシグネチャやインストール日などの詳細情報を表示したり、信頼レベルを変更したりします。

[特定ファイルを調べる]をクリックして、1 つのファイルを参照することもできます。

6 [ファイルインサイト]ウィンドウで、次の作業を行います。

- [詳細]タブで、[検索する]をクリックして、ファイルがパソコンのどこにあるかを探します。ノートンがファイルに信頼できる評価を与えていない場合は、ファイルを信頼するためのオプションが表示されることがあります。
- [提供元]タブで、ファイルのソースについての情報を表示します。

- [活動]タブで、[表示]ドロップダウンから項目を選択することで、平均リソース、CPU、メモリ使用率などのパフォーマンスの問題を表示できます。

7 [閉じる]をクリックします。

パフォーマンスの問題について警告するようにノートン製品を設定する

ノートン製品は、システムのパフォーマンスを監視します。プログラムまたはプロセスによるシステムリソースの使用率の増加が検出されると、パフォーマンス警告を表示します。

[パフォーマンス警告]オプションを使うと、プログラムまたはプロセスによってシステムリソースの使用率が増加した場合にパフォーマンス警告を受信できます。

パフォーマンスの問題について警告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。

[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 [パフォーマンス監視]の[パフォーマンス警告]行で、スイッチを次のいずれかの位置に動かします。

[オフ]	パフォーマンス警告を通知しない場合は、このオプションを選択します。
[オン]	プログラムまたはプロセスがシステムのリソース使用率のしきい値制限を超えたときに、パフォーマンス警告の通知を受信する場合は、このオプションを選択します。
[ログのみ]	パソコンで実行中のすべてのプログラムまたはプロセスによるシステムリソース使用率の監視のみを行う場合は、このオプションを選択します。 デフォルトでは、[パフォーマンス警告]オプションは[ログのみ]になっています。 プログラムまたはプロセスがシステムのリソース使用率のしきい値制限を超えると、その詳細が[セキュリティ履歴]ウィンドウに記録されます。[セキュリティ履歴]ウィンドウの[パフォーマンス警告]カテゴリで、パフォーマンス警告に関連する詳細を確認することができます。

5 [高い使用率の警告]で、次のいずれかの操作をします。

- ノートン製品で CPU 使用率を監視するには、[CPU]スイッチを[オン]の位置に動かします。
- ノートン製品でメモリ使用率を監視するには、[メモリ]スイッチを[オン]の位置に動かします。
- ノートン製品でディスクの使用率を監視するには、[ディスク]スイッチを[オン]の位置に動かします。
- ノートン製品でハンドル件数を監視するには、[ハンドル]スイッチを[オン]の位置に動かします。
  デフォルトでは、このオプションはオフになっています。

6 [適用]をクリックしてから[閉じる]をクリックします。

しきい値になるリソースプロファイルを設定する

システムリソースのしきい値制限によって、*パフォーマンス警告*を通知する時点が決まります。特定のプログラムが使うシステムリソースがしきい値制限を超えると、パフォーマンス警告が通知されます。

しきい値になるリソースプロファイルを設定する

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、[管理の設定]をクリックします。

4 [パフォーマンス監視]の[警告のしきい値になるリソースプロファイル]行で、オプションのいずれかを選択します。

5 [適用]をクリックしてから[閉じる]をクリックします。

ノートン診断レポートを実行する

診断レポートでは、オペレーティングシステム、プログラム、ハードウェアを含む、パソコンについての情報が収集されます。このレポートを使用して、問題を見つけて解決できます。診断レポートは、タイムスタンプ付きのリアルタイムのレポートです。ノートンはこのレポートを自動的に生成しません。

ノートンがパソコンで問題を検出した場合は、[今すぐ解決]オプションを使用して問題を解決できます。確認のために必要な場合、レポートは保存、電子メールによる送信、印刷が可能です。

診断レポートを実行する

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]ウィンドウで、[診断レポート]を選択し、[実行]をクリックします。

パソコン起動時のノートンの効果を最大限に設定する

パソコンを起動したとき、起動項目と呼ばれるいくつかのプログラムが自動的に起動されるため、パソコンの起動時間が長くかかる場合があります。ノートン起動マネージャにより、起動時間を管理できます。パソコンの電源を入れたときにプログラムが自動的に起動されないようにする場合は、起動マネージャでそのプログラムを無効にできます。

パソコンの起動時間を短縮してパフォーマンスを向上させるために、パソコンの電源を入れたときの一部のプログラムの起動を延期できます。ノートンは、延期したプログラムの起動を 5 分間延期します。延期された、以降のすべてのプログラムは、さらに 10 秒間延期して起動されます。

起動項目を延期する

起動項目を延期する

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]ウィンドウの[起動の延期]列で、延期したいプログラムを選択します。

4 [適用]をクリックします。

5 [閉じる]をクリックします。

延期した起動項目を手動で実行する

延期した起動項目を手動で実行する

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、[延期した項目を今すぐ実行]をクリックします。

4 プログラムが起動するまで待ってから[起動マネージャ]ウィンドウで[閉じる]をクリックします。

起動項目を無効にする

起動項目を無効にする

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、[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 [オン/オフ]列で、パソコンの電源を入れたときに自動的に起動させないプログラムのチェックマークをはずします。

4 変更を保存するには[適用]をクリックします。

5 [閉じる]をクリックします。

起動項目を有効にする

起動項目を有効にする

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、[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 [オン/オフ]列で、パソコンの電源を入れたときに自動的に起動させるプログラムにチェックマークを付けます。

4 変更を保存するには[適用]をクリックします。

5 [閉じる]をクリックします。

9

設定のカスタマイズ

この章では以下の項目について説明しています。

ネットワークプロキシを設定する

プロキシサーバーを使ってインターネットに接続する場合は、プロキシサーバーの詳細を指定する必要があります。[ネットワークプロキシの設定]ウィンドウでは、自動設定、プロキシ設定、プロキシサーバー認証設定を入力できます。ネットワークプロキシ設定により、サービスのアクティブ化やサポートオプションへのアクセスなどのタスクの実行中にインターネットに接続できます。

ネットワークプロキシを設定する

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、[管理の設定]をクリックします。
4. [ネットワークプロキシの設定]行で[設定]をクリックします。
5. [ネットワークプロキシの設定]ウィンドウで、次の操作を行います。
   - ブラウザにネットワーク接続設定を自動的に検出させる場合は、[自動設定]の[自動的に設定を検出]にチェックマークを付けます。

- プロキシサーバーに自動設定 URL が必要な場合は、[自動設定]の[自動設定スクリプトを使う]にチェックマークを付けます。[URL]フィールドに PAC ファイルの URL を入力します。
- ネットワークでプロキシサーバーを使う場合は、[プロキシの設定]の[HTTP 接続の場合にプロキシサーバーを使う]にチェックマークを付けます。[アドレス]フィールドにプロキシサーバーの URL または IP アドレスを入力し、[ポート]フィールドにプロキシサーバーのポート番号を入力します。1 から 65535 の値を指定できます。
- プロキシサーバーにユーザー名とパスワードが必要な場合は、[認証]の[ファイアウォールまたはプロキシサーバーを通して接続するための認証を必要とする]にチェックマークを付けます。[ユーザー名]フィールドにユーザー名を入力し、[パスワード]フィールドにパスワードを入力します。

6 [ネットワークプロキシの設定]ウィンドウで、[適用]をクリックします。

バッテリ使用を最適化するようにノートン製品を設定する

パソコンがバッテリ電源で動作しているとき、アクティブなソフトウェアプログラムが使用するリソースを最小限にすることが重要です。そうすることでパソコンのバッテリの寿命を最大限にし、エネルギー効率を向上させることができます。バッテリの使用時のための低いしきい値のプロファイルを設定できます。プログラムまたはプロセスが[低]しきい値制限を超えると、パフォーマンス警告が通知されます。プログラムまたはプロセスを手動で停止してリソースを解放することもできます。[管理の設定]ウィンドウの[バッテリ使用時に低リソースプロファイルを使用]オプションがオンの場合は、パソコンがバッテリ電源で動作している場合に、しきい値プロファイルが自動的に[低]に変更されます。デフォルトでは、このオプションはオンになっています。

[バッテリ使用時に低リソースプロファイルを使用]オプションをオンのままにしておくことを推奨します。

[バッテリ使用時に低リソースプロファイルを使用]オプション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、[管理の設定]をクリックします。

4 [パフォーマンス監視]の[バッテリ使用時に低リソースプロファイルを使用]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 [適用]をクリックしてから[閉じる]をクリックします。

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不正な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

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 を使用すると、よりすばやく検索を起動したり、ショートカットを設定したりすることができます。

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。

10

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。

製品のバージョン番号を確認する

ノートン製品をアップグレードする場合や、カスタマーサポートに問い合わせる場合は、パソコンにインストールされているノートン製品の完全なバージョン番号を確認しておく必要があります。バージョン番号は、問題の正確な解決策を特定するのに役立ちます。

製品のバージョン番号を確認する

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[ヘルプ]をクリックします。
3. [ヘルプセンター]ウィンドウの[一般情報]で、[バージョン情報]をクリックします。

ノートン製品をアップグレードする

ライセンスが残っている場合は、現在のノートン製品を無料で最新版にアップグレードできます。

新しいバージョンを入手できるか確認するには、ノートン製品のメインウィンドウで[ヘルプ] > [新しいバージョンの確認]をクリックします。新しいバージョンがある場合は、画面の指示に従って新しい製品をダウンロードします。セキュリティの脅威に対する保護を強化する新機能や拡張機能が含まれるため、製品の最新バージョンを入手することを推奨します。

ダウンロードに成功すると、シームレスにインストールするよう求めるメッセージがノートン製品に表示されます。製品の新しいバージョンをインストールする前に、画像や会計記録などの重要なすべてのデータを保存する必要があります。

アップグレードが完了しても、ライセンスの状態は以前のバージョンの製品と同じままです。たとえば、製品の現在のバージョンのライセンスが 200 日残っていて、最新バージョンにアップグレードしたとします。その場合は、アップグレードした製品のライセンスは 200 日のみ残っている状態になります。

メモ: シマンテック社のサーバーと通信するための互換性がブラウザにない場合には、このアップグレードプロセスが機能しないことがあります。サポート対象のブラウザは、Internet Explorer 11 以降、Chrome 30 以降、Firefox 27 以降、Safari 7 以降、Opera 17 以降です。

製品のアップグレードは、ライブアップデートによって処理される保護の更新とは異なります。主に次の点が異なっています。

- 製品のアップグレードでは、製品全体の新しいバージョンをダウンロードしてインストールできます。
- 保護の更新は最新の脅威対策技術を備えてノートン製品を最新の状態に保つためのファイルです。

最新バージョンがインストールされている場合も、最新の保護の更新がすべてインストールされていることを必ず確認してください。ライブアップデートを使うと、保護の更新の取得とインストールの処理が自動化されます。[ライブアップデート]を実行するか、[自動ライブアップデート]をオンにして最新の更新を取得することができます。

ノートン製品をアンインストールする

次の方法でパソコンからノートン製品を削除できます。

- Windows のコントロールパネルを使う。
- スタートメニューを使う。
- Windows の[スタート]画面を使う (Windows 8/8.1)。

メモ: アンインストールを続行する前にこのヘルプトピックを印刷してください。アンインストール中にヘルプにアクセスすることはできません。

Windows の[コントロールパネル]でノートン製品をアンインストールする

1 次のいずれかの操作をします。

- Windows のスタートメニューで[コントロールパネル]を選択します。
- Windows 8 では、[アプリ]に移動して、[Windows システム]の[コントロールパネル]をクリックします。

- Windows 10 では、[スタート]、[すべてのアプリ]の順にクリックし、[Windows システム]の[コントロールパネル]をクリックします。

2 Windows のコントロールパネルで次のいずれかの操作をします。

- Windows XP では[プログラムの追加と削除]をダブルクリックします。
- Windows Vista では[プログラムのアンインストール]をダブルクリックします。
- Windows 7 と Windows 8 では、[プログラム]、[プログラムと機能]の順にクリックします。[プログラム]オプションは、[表示方法]ドロップダウンリストで[カテゴリ]オプションを選択すると利用できます。
- Windows 10 では、[プログラムのアンインストール]をクリックします。

3 現在インストールされているプログラムのリストで、次のいずれかの操作をします。

- Windows XP では、ノートン製品を選択してから[変更と削除]をクリックします。
- Windows Vista、Windows 7、Windows 8、または Windows 10 では、ノートン製品を選択してから[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ノートン製品は完全にはアンインストールされません。

スタートメニューからノートン製品をアンインストールする

1 Windows タスクバーで、[スタート] > [すべてのプログラム/すべてのアプリ] > [ノートン セキュリティ] > [ノートン セキュリティのアンインストールする]をクリックします。

2 ノートン ホームページをデフォルトホームページとして、ノートン セーフサーチをデフォルトの検索プロバイダとして維持しない場合は、下部に表示されるチェックボックスを選択します。

3 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ノートン製品は完全にはアンインストールされません。

Windows 8/8.1 のスタート画面からノートン製品をアンインストールする

1 スタート画面でノートン製品を右クリックし、[アンインストール]をクリックします。

2 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から[アンインストールと変更]をクリックします。

3 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ノートン製品は完全にはアンインストールされません。