

ノートン™ セキュリティ

製品マニュアル



ノートン™ セキュリティ製品マニュアル

このマニュアルで説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

マニュアルバージョン 8.5.4

Copyright © 2020 Symantec Corporation. All rights reserved.

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されています。本書のいかなる部分も、**Symantec Corporation** およびそのライセンサーからの事前に文書による許諾を得ることなく、いかなる方法によっても無断で複写、複製してはならないものとします。

本書は「現状有姿のまま」提供され、商品性、特定目的への適合性、不侵害の黙示的な保証を含む、すべての明示的または黙示的な条件、表明、保証は、この免責が法的に無効であるとみなされないかぎり、免責されるものとします。**SYMANTEC CORPORATION** およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書の内容は、事前の通知なく、変更される可能性があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Commercial Computer Software and Commercial Computer Software Documentation」(該当する場合)、さらに後継の法規則により制限権利の対象となります(シマンテックによってオンプレミスサービスとして提供されるか、ホステッドサービスとして提供されるかは関係ありません)。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示、開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043
<http://www.symantec.com>

目次

第 1 章	ノートンによるこそ	6
	Mac 版ノートンを開始する	6
	ノートン セキュリティのシステムの必要条件	7
第 2 章	ノートンのダウンロードとインストール	8
	ノートンのダウンロードとインストール	8
	追加デバイスへのノートンのインストール	10
	ノートンのライセンスの新しいデバイスへの移行	12
	Mac でノートンをアクティブ化または延長する	12
第 3 章	脅威の理解と対応	14
	Mac 上でノートンが検疫したファイルの修復、復元、または削除	14
	Mac でのノートンを最新に保つためのライブアップデートの実行	15
第 4 章	セキュリティの管理	17
	Mac でノートンが保護のために実行するタスクの表示またはカスタマイズ	17
	Mac でのノートンが監視するネットワーク活動の表示やカスタマイズ	19
第 5 章	Mac のスキャン	21
	Mac でノートンのスキャンを実行して脅威を確認する	21
	Mac 版でのノートン自動スキャンの設定変更	23
	Mac でのノートンのスキャンのスケジュール設定	23
	使用していないときに Mac をスキャンするようにノートンを設定する	24
第 6 章	インターネット上のセキュリティの確保	25
	脆弱性保護	26
	悪質な Web サイトに対して Mac の情報へのアクセスを遮断するようにノートン ファイアウォールを設定する	26
	脆弱性保護のオンとオフの切り替え	28
	Mac での攻撃シグネチャの除外または包含	28
	Mac での遮断した攻撃シグネチャに関する通知の有効化/無効化	29
	Mac 版でのファイアウォールの設定	30

	Mac での IP アドレスのファイアウォールルール	32
	Mac での IP アドレスのファイアウォールルールの設定	32
	Mac での IP アドレスのファイアウォールルールの修正	33
	Mac での IP アドレスのファイアウォールルールの削除	34
	Mac 版での拡張保護	34
	拡張保護機能の有効化/無効化	35
	Mac でのノートン ディープサイト コミュニティのダウンロード設定	36
	Mac での AutoBlock の設定	36
	Mac でのシグネチャの設定	37
	ノートンを最新版にアップグレードして Mac の保護を強化する	38
	Mac でのノートン コミュニティウォッチによる潜在的な新しい脅威の特 定	40
	Mac でノートンにエラーが発生した場合のシマンテック社へのレポートの送 信	40
第 7 章	Mac のチューンナップ	42
	ノートン クリーンを実行して Mac の速度を低下させる可能性があるファイ ルを削除する	42
	ノートンクリーンのスキャンをスケジュール設定またはカスタマイズして、Mac のパフォーマンスを改善する	43
第 8 章	重要なデータの保全	45
	Mac で詐欺またはフィッシング Web サイトを検出できるようにノートンを設 定する	45
	Mac で安全に閲覧、買い物を行うためのノートンのブラウザ拡張機能の追 加	46
第 9 章	設定のカスタマイズ	51
	Mac 版での接続遮断設定	52
	Mac での接続遮断の設定	52
	アプリケーションのアクセス設定	54
	アプリケーションのアクセスの設定	54
	サービスのアクセス設定	56
	サービスのアクセスの設定	56
	サービスの特定のアクセス設定のカスタマイズ	58
	サービスのアクセス設定の編集	60
	サービスのアクセス設定の削除	62
	Mac でのアプリケーションのファイアウォールの設定	63
	Mac でのアプリケーションのファイアウォールルールの設定	64
	Mac でのアプリケーションのファイアウォールルールの削除	65
	Mac 版でのネットワークの検出の設定	66

	Mac でのネットワークの検出の有効化/無効化	66
	ネットワーク上の場所に対する接続遮断の設定のエクスポート	66
	Mac でゲームをしたり映画を鑑賞するときのバックグラウンドタスクの停止	67
第 10 章	追加の解決策の検索	69
	ウイルスの名前と定義の確認	69
	Mac 版のプロダクトキーまたは PIN の入手	70
	Mac ユーザーアカウントの種類の確認	70
	Mac 上のノートンのアンインストール	71

ノートンによろこそ

この章では以下の項目について説明しています。

- [Mac 版ノートンを開始する](#)
- [ノートン セキュリティのシステムの必要条件](#)

Mac 版ノートンを開始する

ノートンは、次の方法で Mac を保護します。

- ウイルス、スパイウェア、マルウェア、フィッシング、トロイの木馬、その他のオンラインの脅威に対して防御します。
- オンライン時に個人情報や金融情報を保護します。
- 世界最大の民間脅威インテリジェンスネットワークを活用し、脅威を迅速に特定します。

Mac でノートンを起動したら、メインウィンドウのタイルをクリックして重要な機能にアクセスできます。

- セキュリティ
デバイスが保護されていることを確認し、コンピュータがリスクにさらされている、または確認が必要である場合に、問題を解決します。ほとんどのノートン製品のライセンスでは、アカウントにライセンスが残っている場合、ノートン アカウントにデバイスを追加することもできます。
- スキャン
クイックスキャン、完全スキャン、またはファイルスキャンを実行してデバイスに脅威がないか確認したり、スキャンのスケジュールを設定したりします。詳しくは、「[p.21 の「Mac でノートンのスキャンを実行して脅威を確認する」](#)を参照してください。」を参照してください。
- ライブアップデート
脅威に対する最新の保護、機能やパフォーマンスの強化が適用されていることを確認します。詳しくは、「[p.15 の「Mac でのノートンを最新に保つためのライブアップデートの実行」](#)を参照してください。」を参照してください。
- 詳細設定

デスクトップとオンラインの活動の設定を表示、変更します。ほとんどのユーザーは、デフォルトの設定で最適なレベルの保護が提供されますが、セキュリティとネットワークの設定をカスタマイズすることもできます。

- クリーン
スキャンを実行し、コンピュータの速度を低下させる可能性があるさまざまな種類のジャンクファイルを削除します。詳しくは、「p.42 の「ノートン クリーンを実行して Mac の速度を低下させる可能性があるファイルを削除する」を参照してください。」を参照してください。

ノートン セキュリティのシステムの必要条件

オペレーティングシステム

ノートン製品は、Mac OS X 10.7.5 (Lion) 以降でのみサポートされています。OS X 10.6 またはそれ以前のバージョンで Mac を実行している場合は、Mac オペレーティングシステムをサポート対象バージョンにアップグレードしてください。

ハードウェア

- Intel® Core 2 Duo、Core i3、Core i5、Core i7 または Xeon プロセッサを搭載した Mac コンピュータ)
- 2 GB の RAM
- 300 MB 以上のハードディスク容量
- LiveUpdate で利用できるインターネット接続

サポート対象のブラウザ

- Safari®^{1, 2}
- Mozilla Firefox®^{1, 2}
- Google Chrome™¹

¹ 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。

² 最新バージョンとその 1 つ前のバージョンの 32 ビットメジャーリリースをサポートします。

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
- 追加デバイスへのノートンのインストール
- ノートンのライセンスの新しいデバイスへの移行
- Mac でノートンをアクティブ化または延長する

ノートンのダウンロードとインストール

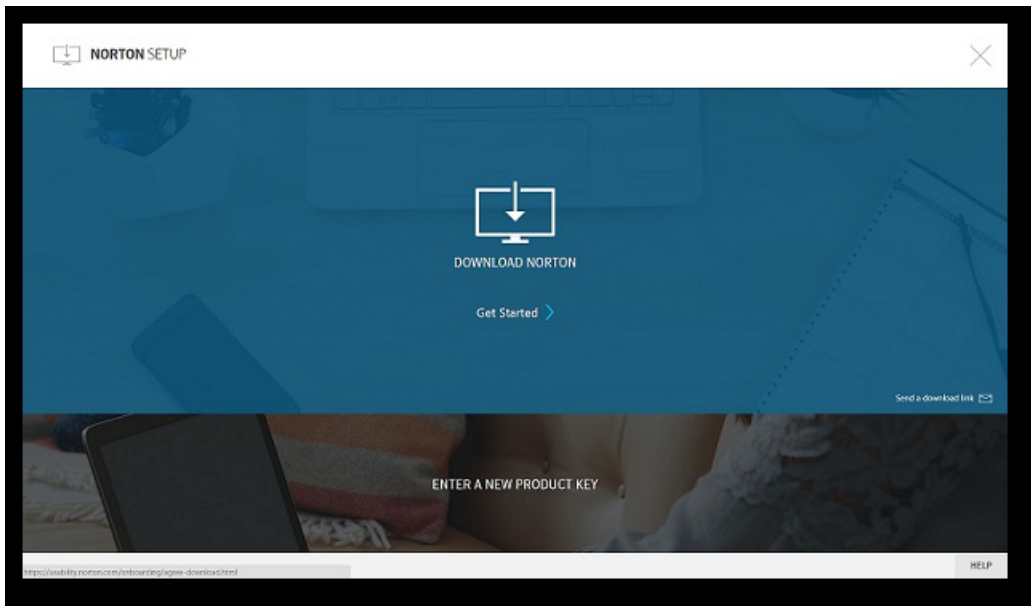
お使いのデバイスを保護してノートン製品を管理するのは、ノートンアカウントに新しいデバイスを追加するのと同じくらい簡単です。

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 norton.com/setup に移動します。
- 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とノートン アカウントのパスワードを入力して、[サインインする]をクリックします。

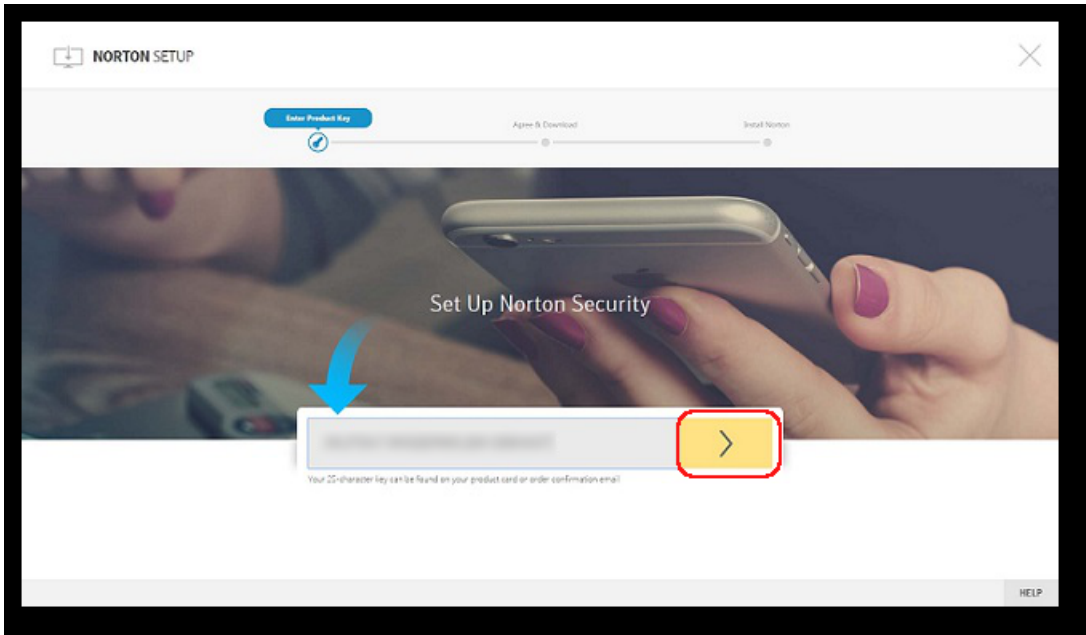
アカウントを持っていない場合は、[アカウントを作成する]をクリックして、サインアッププロセスを完了します。

- 3 [ノートンの設定]ウィンドウで[ノートンをダウンロード]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。



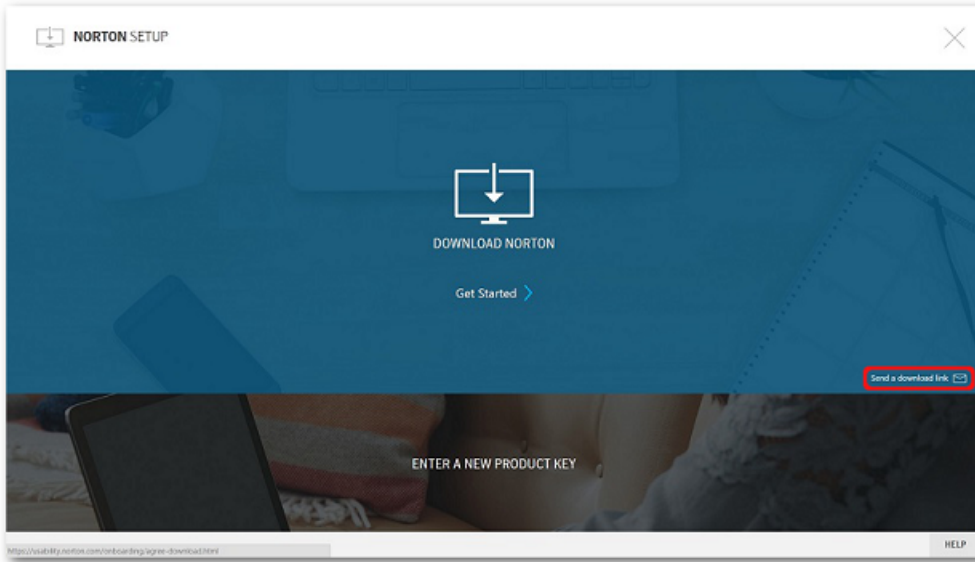
- 4 [同意してダウンロードする]をクリックします。
- 5 画面の青い矢印で示されている領域をクリックして、画面に表示される指示に従います。
 - Internet Explorer または Microsoft Edge ブラウザの場合は、[実行]をクリックします。
 - Firefox または Safari の場合は、ブラウザの右上隅にある[ダウンロード]オプションをクリックしてダウンロードされたファイルを表示し、ダウンロードしたファイルをダブルクリックします。
 - Chrome の場合は、左下隅に表示されるダウンロードしたファイルをダブルクリックします。
- 6 [ユーザーアカウント制御]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とノートン アカウントのパスワードを入力して、[サインインする]をクリックします。
- 3 [ノートンの設定]ウィンドウで、[ダウンロードリンクを送信する]をクリックします。



- 4 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。
- 5 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。
- 6 [今すぐダウンロード]をクリックします。
- 7 [同意してダウンロードする]をクリックします。
- 8 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。

メモ: ノートン アンチウイルス Mac 版は、ノートン アカウントを通して管理できません。

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。

Mac でノートンをアクティブ化または延長する

製品をアクティブ化していただくことで、シマンテック社のソフトウェアを適正に利用していることとなります。アクティブ化すると指定されたサブスクリプション期間ノートン製品が有効になります。

インストール後に製品をアクティブ化しなかった場合、製品をアクティブ化するまで、[サブスクリプション]の警告が定期的に表示されます。警告に明記されている期間内に製品をアクティブ化してください。そうしないと製品は動作を停止します。アクティブ化するには、この製品に含まれているプロダク

トキーを使う必要があります。また、サブスクリプションを更新して、ノートン製品の使用を継続できません。

インターネットに接続している場合は、ノートンアカウントの資格情報を入力するように求められます。既存のノートン アカウントを使用して新しいノートン アカウントを登録できます。ノートン アカウントにサインインしたら、プロダクトキーを入力してノートン製品をアクティブ化し、ノートン アカウントにプロダクトキーを登録します。ノートンアカウントでは、プロダクトキー、製品登録日、最近の製品のアップデートなど、詳細を表示できます。

警告からの製品のアクティブ化

- 1 警告で、[今すぐアクティブ化]を選択します。
- 2 画面の指示に従って操作して製品をアクティブ化します。

メインウィンドウからの製品のアクティブ化

- 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[今すぐアクティブ化]をクリックします。
- 3 表示されるウィンドウで次のいずれかのオプションをクリックします。
 - [今すぐアクティブ化]: 画面の指示に従って操作します。サービスプロバイダから発行された製品 PIN を入力するように要求されることがあります。
 - [スキップ]: ライセンスを後でアクティブ化するにはこのオプションを使用します。

脅威の理解と対応

この章では以下の項目について説明しています。

- **Mac** 上でノートンが検疫したファイルの修復、復元、または削除
- **Mac** でのノートンを最新に保つためのライブアップデートの実行

Mac 上でノートンが検疫したファイルの修復、復元、または削除

ノートンが、最新のウイルス定義では排除できない脅威を検出すると、**Mac** で拡散または感染しないように、影響を受けたファイルを検疫します。ファイルが検疫された場合、**Finder** でそのファイルを表示したり、使用することはできません。

使用している一部のアプリが、ノートンによって脅威として分類、検疫されたファイルにアクセスする必要がある場合があります。たとえば、多くのシェアウェアまたはフリーウェアのアプリは、脆弱性を引き起こすアドウェアをダウンロードします。これらのアプリは、アプリが操作する必要があるアドウェアファイルをノートンが検疫していれば、動作しません。

ノートンが表示する[検疫に入ったファイル]ウィンドウで、検疫された感染ファイルの詳細をさらに確認できます。新しいウイルス定義を受信した場合、検疫された項目の修復を試みることができます。一部の検疫項目は、ノートン製品による再スキャン後に正常に駆除が実行されます。このような項目は復元することもできます。

メモ:安全であるという確信がない場合は、検疫ファイルを復元しないでください。項目を元の場所以外のフォルダに復元すると正しく機能しないことがあります。したがって、プログラムを再インストールすることを推奨します。

場合によっては、[ファイルを削除しました]ウィンドウが表示され、ノートンが特定の感染ファイルを自動的に検出してゴミ箱に移動したか、修復できないファイルを **Mac** から削除したことが示されます。ファイルを修復できない場合、そのファイルは検疫に移動されるか、削除されます。

検疫に入ったファイルの修復、復元、または削除

一部の検疫項目は、ノートンによるウイルスのアップデートのダウンロードと項目の再スキャンの後に修復できます。

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[アクティビティ]をクリックします。
- 4 [セキュリティ履歴]行で、表示アイコンをクリックします。
- 5 [セキュリティ履歴]ウィンドウの[Macを保護する]で、[検疫]をクリックします。
- 6 検疫された項目のリストで、表示する項目を選択します。
- 7 左上隅の[処理]アイコンをクリックして、次のいずれかをクリックします。
 - [修復]。脅威を排除するためにファイルを再スキャンします。
 - [復元](非推奨)。脆弱性を引き起こす可能性があるファイルを検疫から取り出し、元の場所に戻します。
 - [削除]。検疫および Mac からファイルを完全に削除します。
- 8 [完了]をクリックします。

Macでのノートンを最新に保つためのライブアップデートの実行

デフォルトでは、ノートンはシマンテック社のサーバーから定期的に最新の定義とプログラムの更新をダウンロードしてインストールし、最新の脅威からコンピュータを保護します。オフラインの場合や自動ライブアップデートがオフの場合でも、いつでもライブアップデートを実行できます。

メモ: プログラム更新によってはインストールの後にコンピュータを再起動する必要があります。

ライブアップデートの実行

- 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[ライブアップデート]をクリックします。
- 3 [概略を表示する]をクリックして Mac にダウンロードおよびインストールされているアップデートのリストを表示します。

マイノートンウィンドウからのライブアップデートの実行

- 1 ノートンを起動します。
- 2 [マイノートン]ウィンドウの[デバイスセキュリティ]で、[ライブアップデート]をクリックします。
- 3 [概略を表示する]をクリックして **Mac** にダウンロードおよびインストールされているアップデートのリストを表示します。

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。

- **Mac** でノートンが保護のために実行するタスクの表示またはカスタマイズ
- **Mac** でのノートンが監視するネットワーク活動の表示やカスタマイズ

Macでノートンが保護のために実行するタスクの表示またはカスタマイズ

ノートンを使用すると、実行されたスキャン、送信された警告、検疫された項目、遮断されたアプリケーション、検出されたネットワークへのアクセス試行など、実行する一連のタスクを表示して保護に役立てることができます。

Macでノートンが保護のために実行するタスクの表示またはカスタマイズ

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[アクティビティ]をクリックします。
- 4 [セキュリティ履歴]行で、表示アイコンをクリックします。
- 5 [セキュリティ履歴]ウィンドウで、実行した活動を表示するカテゴリを選択します。
- 6 最近の活動を表示し、選択したイベントで実行可能な次の処理を行うことができます。
 - 次の

をクリックしてレポートをテキストファイルとして **Mac** ディスクにダウンロードします。
 - 次の



をクリックして記録イベントをすべて削除します。

- 次の



をクリックして要件に基づいて記録イベントをフィルタ処理します。

- 次の



をクリックしてレポートを印刷します。

- 次の



をクリックして選択したイベントに関する追加情報を表示します。

- 次の



をクリックして選択したイベントで実行可能な処理を行います。[処理]メニューのオプションは、リストから選択したイベントによって異なります。

- 次の



をクリックして各カテゴリに表示する必要があるオプションをカスタマイズします。[セキュリティ履歴表示オプション]ウィンドウで、必要に応じて次のオプションを設定します。

- IP アドレスの代わりにホスト名を表示する
- 重大度の高いイベントを異なる色で表示する
- [列]ドロップダウンメニューで、表示オプションを変更するログカテゴリを選択できます。カテゴリを選択すると、表示できる詳細の種類が示されます。[セキュリティ履歴]ウィンドウに表示する必要のある詳細を選択できます。

詳しい情報

- ◆ ■ p.21 の「[Mac でノートンのスキャンを実行して脅威を確認する](#)」を参照してください。
- p.14 の「[Mac 上でノートンが検疫したファイルの修復、復元、または削除](#)」を参照してください。

Mac でのノートンが監視するネットワーク活動の表示やカスタマイズ

ノートンを使用すると、着信と発信の接続、開いているネットワークポートで実行されるアプリケーションなど、監視するネットワーク活動を表示できます。

ネットワーク接続活動の表示やカスタマイズ

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[アクティビティ]をクリックします。
- 4 [ネットワーク活動]行で、表示アイコンをクリックします。
- 5 [ネットワーク活動]ウィンドウで、現在のネットワーク接続の詳細を表示するアプリケーション、サービス、ポートを選択します。
- 6 最近のネットワーク接続活動を表示し、選択したカテゴリで実行可能な次の活動を行うことができます。

- 次の



をクリックしてレポートをテキストファイルとして **Mac** ディスクにダウンロードします。

- 次の



をクリックしてレポートを印刷します。

- 次の



をクリックして選択したイベントに関する追加情報を表示します。

- 次の



をクリックして選択したイベントで実行可能な処理を行います。[処理]メニューのオプションは、リストから選択したイベントによって異なります。

- 次の



をクリックして各カテゴリに表示する必要があるオプションをカスタマイズします。[ネットワーク活動の表示オプション]ウィンドウで、必要に応じて次のオプションを設定します。

- IP アドレスの代わりにホスト名を表示する
- [列]セクションで、表示する接続オプションを設定します。

詳しい情報

- ◆ ■ p.6 の「[Mac 版ノートンを開始する](#)」を参照してください。

Mac 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。

- [Mac でノートンのスキャンを実行して脅威を確認する](#)
- [Mac 版でのノートン自動スキャンの設定変更](#)
- [Mac でのノートンのスキャンのスケジュール設定](#)
- [使用していないときに Mac をスキャンするようにノートンを設定する](#)

Mac でノートンのスキャンを実行して脅威を確認する

ノートン自動スキャンはウイルス定義を更新し、広範な脅威に対してコンピュータを定期的にスキャンします。自動スキャンが無効になっている、オフラインである、またはウイルスの存在が疑われる場合、手動で次の操作を実行できます。

- [クイックスキャン]は、脅威に対して最も脆弱なコンピュータの領域を分析します。
- [完全スキャン]は、クイックスキャンで確認されるファイルに加えて、脆弱性がそれほどないアプリケーション、ファイル、実行中のプロセスを含め、システム全体を分析します。
- [ファイルスキャン]は、リスクにさらされている疑いがある場合に、個別のファイルまたはフォルダを分析します。

クイックスキャン、完全スキャン、ファイルスキャンの実行

- 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[スキャン]をクリックします。
- 3 左ペインで、実行するスキャンをクリックします。
 - [クイックスキャン] > [クイックスキャンを開始する]
 - [完全スキャン] > [完全スキャンを開始する]

- [ファイルスキヤン] > [ファイルを選択する]
フォルダまたはファイルに移動し、[スキヤン]をクリックします。

コマンドラインを使ったスキヤンの実行

ノートン製品では、コマンドラインインターフェースから複数のスキヤンを実行できます。ノートン製品のノートン スキヤナ機能から、この上級ユーザー向け機能が提供されています。この機能は、詳しい知識のあるユーザーにのみ使用を推奨します。

コマンドラインインターフェースは、[Finder] > [アプリケーション] > [ユーティリティ] > [ターミナル]を選択して起動できます。

クイックスキヤンの実行

- ◆ コマンドラインで `/usr/bin/nortonscanner quickscan` と入力します。

システムの完全スキヤンの実行

- ◆ コマンドラインで `/usr/bin/nortonscanner systemscan` と入力します。

特定ファイルのスキヤン

- ◆ コマンドラインで `/usr/bin/nortonscanner -a <file path>` と入力します。

圧縮ファイルのスキヤン

- ◆ コマンドラインで `/usr/bin/nortonscanner -c <file path>` と入力します。

検疫のスキヤン

- ◆ コマンドラインで `/usr/bin/nortonscanner quarantine` と入力します。

[スキヤンの概略]ウィンドウを使用して、ノートン製品により最後に実行されたスキヤンの概略を表示できます。ノートン製品は、スキヤン中に検出された感染ファイルに対して適切な処理を自動的にを行います。[セキュリティ履歴]ウィンドウに、ウイルススキヤンの詳細を表示できます。

メモ: ノートン製品が感染ファイルを修復できない場合、そのファイルは検疫の対象となります。これによって、ノートン製品は、Macの他のファイルへの感染および拡散から感染するのを防ぎます。検疫項目は、[セキュリティ履歴]ウィンドウの[検疫]カテゴリで確認できます。

[完了]オプションを使用して、[スキヤン結果]ウィンドウを閉じることができます。不要である可能性のあるアプリケーションの場合は、[削除]ボタンが有効になります。[削除]ボタンを使用してアプリケーションを削除できます。

ノートン製品は、感染ファイルが修復され、ファイルを安全に使用できることを示す[ウイルススキヤンの完了]ウィンドウを表示します。[詳細設定]ウィンドウの[アクティビティ]セクションにある[セキュリティ履歴]オプションを使用して修復されたファイルの詳細を確認できます。検出されたウイルスとMacを保護するためにウイルスに対して適用された処理を確認することもできます。

Mac 版でのノートン自動スキャンの設定変更

ノートン自動スキャンは、ウイルス定義の定期更新、コンピュータのスキャン、着発信トラフィックの監視によって、セキュリティを最大限に高めます。デフォルトの設定はほとんどのユーザーにとって最適ですが、オプションをカスタマイズして、ファイルを自動スキャンの対象に含めたり対象から除外したり、一時的にこの機能をオフにしたりできます。

自動スキャンオプションの変更

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[Mac を保護する]をクリックします。
- 4 [自動スキャン]行で、設定アイコンをクリックし、次のいずれかを変更します。
 - [すべてをスキャンする]
 - [次のフォルダのみをスキャンする]または[次のフォルダをスキャンしない]
[+]をクリックして、自動スキャンの対象に含めるまたは対象から除外するフォルダを参照します。
 - [圧縮済みアーカイブ内のファイルをスキャンする] (.zip または .rar 形式を含む)
 - [アクセス時に外部ドライブに存在するファイルをスキャンする]

Mac でのノートンのスキャンのスケジュール設定

Mac にノートンをインストールすると、自動スキャンが有効になり、ウイルス定義が更新され、広範な脅威に対してコンピュータが定期的なスキャンされますが、特定のタイミングにスキャンをスケジュール設定したい場合もあります。

メモ: 別のユーザーが Mac を使用しているときでも[定期スキャン]設定は変更されず、スキャンの定期実行は継続されます。

ノートンのスキャンのスケジュール設定

- 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]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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[Mac を保護する]をクリックします。
- 4 [定期スキャン]行で、スイッチがオンになっていることを確認します。
スイッチがオフの場合、定期スキャンを実行または設定できなくなります。

- 5 設定アイコンをクリックします。
- 6 [定期スキャン]ウィンドウで、スキャンの対象とタイミングのオプションを設定します。
- 7 [保存]をクリックします。

使用していないときに Mac をスキャンするようにノートンを設定する

ノートンをインストールすると、Mac を使用中であることを検出して、ノートンがコンピュータのパフォーマンスに影響する可能性があるスキャンを実行しないように、[アイドルスキャン]機能が設定されます。デフォルトの設定はほとんどのユーザーにとって最適ですが、設定をカスタマイズして、コンピュータ全体または特定のファイルやフォルダのみをスキャンするようにカスタマイズできます。推奨ではありませんが、アイドルスキャンをオフにすることもできます。

[アイドルスキャンレポート]ウィンドウが表示され、ノートン製品がアイドルスキャンで 1 つ以上の感染ファイルを検出したことを示します。[ログの表示]オプションを使用して、感染ファイルの詳細を[セキュリティ履歴]ウィンドウで確認できます。

アイドルスキャン設定のカスタマイズ

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[Mac を保護する]をクリックします。
- 4 [アイドルスキャン]行で、スイッチがオンになっていることを確認します。
スイッチがオフの場合、作業中にコンピュータのパフォーマンスに影響が出る可能性があります。
- 5 [アイドルスキャン]ウィンドウで、スキャン設定をカスタマイズします。
 - [スキャン対象]では、スキャン対象としてシステム全体、起動ディスク、またはすべてのユーザーフォルダを指定します。
 - [圧縮済みアーカイブ内のファイルのスキャンする (推奨)]は、.zip ファイルなど、圧縮ファイルのスキャンします。
 - [アイドルスキャン結果を表示する]は、スキャン結果のレコードを保存します。
 - [デフォルトに戻す]は、すべての変更を推奨されるデフォルトに戻します。

詳しい情報

- ◆ ■ p.23 の「[Mac 版でのノートン自動スキャンの設定変更](#)」を参照してください。

インターネット上のセキュリティの確保

この章では以下の項目について説明しています。

- 脆弱性保護
- 悪質な Web サイトに対して Mac の情報へのアクセスを遮断するようにノートン ファイアウォールを設定する
- 脆弱性保護のオンとオフの切り替え
- Mac での攻撃シグネチャの除外または包含
- Mac での遮断した攻撃シグネチャに関する通知の有効化/無効化
- Mac 版でのファイアウォールの設定
- Mac での IP アドレスのファイアウォールルール
- Mac での IP アドレスのファイアウォールルールの設定
- Mac での IP アドレスのファイアウォールルールの修正
- Mac での IP アドレスのファイアウォールルールの削除
- Mac 版での拡張保護
- 拡張保護機能の有効化/無効化
- Mac でのノートン ディープサイト コミュニティのダウンロード設定
- Mac での AutoBlock の設定
- Mac でのシグネチャの設定
- ノートンを最新版にアップグレードして Mac の保護を強化する

- **Mac** でのノートン コミュニティウォッチによる潜在的な新しい脅威の特定
- **Mac** でノートンにエラーが発生した場合のシマンテック社へのレポートの送信

脆弱性保護

脆弱性保護機能は、インターネットを介した侵入を検出して防止するのに役立ちます。脆弱性保護は悪質な攻撃に対する **Mac** 上のプログラムの脆弱性に関する情報を提供します。また、既知の攻撃についての情報も提供します。

脆弱性とは、**Mac** 全体のセキュリティで弱点となる可能性のあるプログラムまたはオペレーティングシステムの欠陥です。**Mac** の設定やセキュリティの設定が不適切な場合にも脆弱性が生じます。外部からの攻撃は、このような脆弱性を悪用して、**Mac** 上で悪質な処理を実行します。このような悪質な攻撃の例には、アクティブデスクトップの監視、キーロガー、ハッキングがあります。このような攻撃は **Mac** のパフォーマンスを低下させ、プログラム障害を引き起こしたり、個人データや機密情報をネット犯罪者にさらす原因となる可能性があります。

ノートン製品はシグネチャベースのソリューションを提供して、一般的なインターネット攻撃のほとんどから **Mac** を保護します。攻撃シグネチャには攻撃者がオペレーティングシステムまたは **Mac** プログラムの既知の脆弱性を悪用する試みを識別する情報が含まれます。ノートン製品の侵入防止機能は攻撃シグネチャの広範にわたるリストを使って疑わしいネットワーク活動を検出し、遮断します。

悪質な Web サイトに対して Mac の情報へのアクセスを遮断するようにノートン ファイアウォールを設定する

フリーウェアやシェアウェアのアプリケーションをインストールして開くと、いくつかの悪質な Web サイトがデバイスの情報に不正にアクセスしようとする場合があります。悪質な Web サイトは脆弱性を検出して攻略し、暗号通貨マイニングのマルウェアなど、デバイスの情報をサイバー犯罪者に公開できるマルウェアをダウンロードします。

[URL 監視]をオンにすると、コンピュータにインストールされたすべてのアプリケーションをノートンが監視し、悪質な Web サイトによるデバイス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。また、[セキュリティ履歴]ウィンドウを使用して、攻撃に関する情報を表示できます。

メモ: URL 監視は、ブラウザアプリケーションを監視しません。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。詳しくは、「[p.46 の「Mac で安全に閲覧、買い物を行うためのノートンのブラウザ拡張機能の追加」](#)を参照してください。」を参照してください。

URL 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、URL 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、[URL 監視]をオンにした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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックし、[脆弱性保護]スイッチがオンになっていることを確認します。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[URL 監視]タブをクリックします。
- 6 オフになっている場合は、[オン]オプションをクリックします。

URL またはドメインの監視からの除外

脆弱性保護は攻撃シグネチャの広範にわたるリストを使用して疑わしい Web サイトを検出し、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 Web サイトまたはドメインを監視から除外できます。

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックし、[脆弱性保護]スイッチがオンになっていることを確認します。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[URL 監視]タブをクリックします。
- 6 [追加]ボタンをクリックし、監視から除外する URL またはドメイン名を入力します。
- 7 [保存]をクリックします。
- 8 URL またはドメインを編集または削除する場合、次の操作を実行します。
 - リストから URL またはドメインを選択して[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、[保存]をクリックします。
 - 削除する URL またはドメインを選択して[削除]ボタンをクリックします。

遮断された Web サイトに関する情報を表示

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[アクティビティ]をクリックします。
- 4 [セキュリティ履歴]行で、表示アイコンをクリックします。
- 5 [セキュリティ履歴]ウィンドウの[ファイアウォール]カテゴリで、[脆弱性保護]をクリックします。
- 6 遮断された Web サイトの詳細を確認するには、右ペインで攻撃シグネチャをダブルクリックします。
- 7 [脆弱性を遮断しました]ウィンドウで[詳細情報]をクリックして、攻撃シグネチャの詳細を確認します。

脆弱性保護のオンとオフの切り替え

Mac の脆弱性に影響する可能性がある脅威から Mac を保護するかどうかを選択できます。

デフォルトでは、[脆弱性保護]オプションはオンになっています。悪質な攻撃から Mac を保護するために[脆弱性保護]オプションはオンのままにすることをお勧めします。

脆弱性保護のオンとオフの切り替え

- 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[詳細設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、スイッチを[オフ]または[オン]の位置に動かします。

Mac での攻撃シグネチャの除外または包含

ノートン製品は、既知の攻撃シグネチャとファイルのシグネチャを比較して、Mac 上の脅威を識別します。攻撃シグネチャは、攻撃者が既知のオペレーティングシステムまたはアプリケーションの脆弱性を悪用する試みを識別するために使われます。

Mac をすべての攻撃シグネチャから保護するか、選択したシグネチャのみから保護するかを選択できます。場合によっては攻撃シグネチャに似た悪質でないネットワーク活動が表示される可能性があります。攻撃があるかもしれないと通知が繰り返し表示される場合があります。その通知を引き起こしている攻撃が安全であることがわかっている場合には悪質でない活動に一致するシグネチャの除外リストを作成できます。

脆弱性に対する保護は必要であっても遮断した攻撃についての通知を受信したくない場合には、脆弱性保護による通知の表示を停止できます。シグネチャを無効にする妥当な理由がないかぎり、シグネチャはオンのままにしてください。シグネチャを無効にした場合、コンピュータは攻撃に対して脆弱になることがあります。

攻撃シグネチャの有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[シグネチャ]タブをクリックします。
- 6 [シグネチャ]リストでシグネチャを選択して、次のいずれかを実行します。
 - 攻撃シグネチャの検出を無効にするには、[このシグネチャを有効にする]のチェックマークをはずします。
 - 攻撃シグネチャの検出を有効にするには、[このシグネチャを有効にする]のチェックマークを付けます。
- 7 [完了]をクリックします。

Mac での遮断した攻撃シグネチャに関する通知の有効化/無効化

攻撃の疑いのある通信を脆弱性保護が遮断した場合に通知を表示したいかどうかを選択できます。通知メッセージでは次のようなことができます。

- 遮断した攻撃の詳細の表示。
- 誤って検出された攻撃の報告。

脆弱性保護の活動はすべて、[セキュリティ履歴]ウィンドウに記録されます。活動ログのエントリには、権限のないアクセスの試みとその他の詳細に関する情報が含まれます。

通知は遮断したすべての攻撃についてまたは個々の攻撃シグネチャについて有効または無効にできます。

遮断したすべての攻撃の通知の有効化/無効化

- 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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[詳細設定]タブをクリックします。
- 6 [詳細設定]タブで次のいずれかの操作をします。
 - 遮断された攻撃すべての通知を無効にするには、[脆弱性保護による攻撃の自動遮断時に通知する]の選択を解除します。
 - 遮断された攻撃すべての通知を有効にするには、[脆弱性保護による攻撃の自動遮断時に通知する]を選択します。
- 7 [完了]をクリックします。

個々の攻撃シグネチャの通知に関する有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[シグネチャ]タブをクリックします。
- 6 [シグネチャ]リストで次のいずれかの操作をします。
 - 通知を無効にするには、[このシグネチャの通知を表示する]の選択を解除します。
 - 通知を有効にするには、[このシグネチャの通知を表示する]を選択します。
- 7 [完了]をクリックします。

Mac 版でのファイアウォールの設定

ファイアウォールの設定を使用して、インバウンドとアウトバウンドのネットワーク通信に対しファイアウォールがどのように監視と応答をするかをカスタマイズできます。ファイアウォールの設定には、Mac のアプリケーション、サービス、ポートのアクセス設定が含まれます。また、Mac が接続されているネットワーク内の他のコンピュータへの発信接続または着信接続のアクセス設定も含まれます。

[ファイアウォール]ウィンドウを使って、次のファイアウォールの設定をカスタマイズできます。

アプリケーションの遮断	<p>Mac で動作し、インターネットに接続するアプリケーションのファイアウォールルールを設定できます。</p> <p>アプリケーションの遮断の設定によって、アプリケーション (Web ブラウザや iTunes など) によるインターネットへの接続を許可するか拒否するかが決定されます。</p> <p>アプリケーションの遮断の設定は、ネットワーク上の特定の場所に固有ではありません。アプリケーションの遮断の設定は、ネットワーク上の別の場所に移動しても変更されません。</p> <p>[アプリケーションの遮断]の[設定]オプションを使って、Mac 上のアプリケーションのインターネットアクセスを設定できます。</p> <p>メモ: 接続遮断の設定とアプリケーションの遮断の設定の間に重複がある場合は、常に接続遮断の設定がアプリケーション遮断の設定よりも優先されます。</p>
接続の遮断	<p>次のことを行うアプリケーション、ポート、サービス、IP アドレスを許可または遮断できます。</p> <ul style="list-style-type: none">■ Mac に接続する。■ ネットワークに接続する。 <p>接続遮断の設定によって、特定のサービス、アプリケーション、ポートを使う発信接続または着信接続を許可するか拒否するかが決定されます。ファイアウォールでネットワーク上の特定の IP アドレスを許可または遮断するように設定することもできます。</p> <p>接続遮断の設定は、特定の場所にも適用されます。</p> <p>[接続の遮断]行の設定アイコンを使って、Mac 上のアプリケーションとサービスの接続を設定できます。</p>
脆弱性保護	<p>インターネットを介した侵入を検出して防止するのに役立ちます。脆弱性保護は Mac 上のすべての着発信トラフィックを監視し、権限のないアクセスを遮断します。</p> <p>さらに、悪質な攻撃に対する Mac 上のプログラムの脆弱性に関する情報を提供します。また、既知の攻撃についての情報も提供します。脆弱性保護のシグネチャのリストを管理できます。</p>
ネットワークの検出	<p>Mac が接続されているネットワーク上の場所に基づくファイアウォール設定を設定できます。</p> <p>設定されるファイアウォール設定には、Mac で動作するアプリケーションとサービスの接続遮断設定が含まれます。ポータブル Mac を新しいネットワーク上の場所に接続すると、ノートン製品はそのネットワーク上の場所に対する新しいファイアウォール設定の選択を要求します。</p>
ディープサイト	<p>[ノートンディープサイトコミュニティのダウンロード]を利用し、設定できます。シマンテック社が攻撃者として識別した IP アドレスの更新リストを取得できます。ノートンディープサイトコミュニティのダウンロード機能を有効にして、シマンテック社のサーバーから IP アドレスの更新リストを取得できます。</p>

Mac での IP アドレスのファイアウォールルール

[接続の遮断]ウィンドウを使って、Mac が接続されているネットワーク内のゾーンのファイアウォールを設定できます。ゾーンのアクセス設定を設定して、接続を許可または遮断する IP アドレスを指定できます。

[表示]ペインの[信頼ゾーン]には、ネットワーク上の場所にある、着発信アクセス試行を許可した IP アドレスが表示されます。[表示]ペインの[遮断ゾーン]には、ネットワーク上の場所にある、着発信アクセス試行を遮断した IP アドレスが表示されます。

[接続の遮断]ウィンドウで、ゾーンに対して次のことを実行できます。

- IP アドレスのアクセス設定の設定
- IP アドレスのアクセス設定の編集
- IP アドレスのアクセス設定の削除

Mac での IP アドレスのファイアウォールルールの設定

ネットワーク上の場所の設定に固有の IP アドレスのファイアウォールルールを指定できます。

[表示]ペインの[信頼ゾーン]には、ネットワーク上の場所にある、着発信アクセス試行を許可した IP アドレスが表示されます。[表示]ペインの[遮断ゾーン]には、ネットワーク上の場所にある、着発信アクセス試行を遮断した IP アドレスが表示されます。

IP アドレスのファイアウォールルールの設定

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]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[詳細設定]または[設定]をクリックします。

3 左ペインで[ファイアウォール]をクリックします。

4 [接続の遮断]行で、設定アイコンをクリックします。

5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、ネットワーク上の場所を選択します。

6 [表示]メニューで、[ゾーン]を選択します。

7 [IP アドレスを追加]をクリックします。

[遮断ゾーン]行または[信頼ゾーン]行の横にある[+]記号を使って IP アドレスのアクセス設定を指定することもできます。

- 8 [アドレスを編集]ウィンドウで、デフォルトのアクセス設定オプションを選択します。次のオプションがあります。
- | | |
|--------|------------------------------------------|
| [許可する] | ネットワーク上に存在するすべてのコンピュータの発信接続や着信接続を許可できます。 |
| [遮断する] | 指定した IP アドレスのコンピュータの発信接続や着信接続を遮断できます。 |
- 9 アドレスメニューでオプションを選択して、アクセス設定を適用するコンピュータの IP アドレスを指定します。次のオプションがあります。
- | | |
|------------------------|-----------------------------------------------|
| [ネットワーク上のすべてのコンピュータ] | ネットワーク上のすべてのコンピュータの発信接続や着信接続を許可または遮断できます。 |
| [単一のコンピュータ] | 指定した IP アドレスのコンピュータの発信接続や着信接続を許可または遮断できます。 |
| [次の番号で始まるすべての IP アドレス] | 指定した基準アドレスを持つコンピュータに対して発信接続や着信接続を許可または遮断できます。 |
| [ネットワーク上のすべての IP アドレス] | ローカルネットワーク上のコンピュータの発信接続や着信接続を許可または遮断できます。 |
- 10 [ログと通知の設定]をクリックして、ノートン製品がアクセス試行について記録を保持したり、通知するように設定します。
- 11 [保存]をクリックします。

Mac での IP アドレスのファイアウォールルールの修正

ネットワーク上の場所の設定に固有の IP アドレスのファイアウォールルールを編集できます。

IP アドレスのファイアウォールルールの修正

- 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。
- ノートン製品のメインウィンドウで[詳細設定]または[設定]をクリックします。
- 左ペインで[ファイアウォール]をクリックします。
- [接続の遮断]行で、設定アイコンをクリックします。
- [設定の編集]メニューにある[接続の遮断]ウィンドウで、IP アドレスの設定を変更する[接続の遮断]設定を選択します。

- 6 [表示]メニューで[ゾーン]をクリックし、修正する IP アドレスのアクセス設定を含む行を選択します。
- 7 [編集]をクリックします。
- 8 [アドレスを編集]ウィンドウで、必要な変更を行います。
- 9 [保存]をクリックします。

Mac でのIP アドレスのファイアウォールルールの削除

ネットワーク上の場所に固有の IP アドレスのファイアウォールルールを削除できます。

IP アドレスのファイアウォールルールの削除

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [設定の編集]メニューにある[接続の遮断]ウィンドウで、[接続の遮断]設定を選択します。
- 6 [表示]メニューで、[ゾーン]を選択します。
- 7 [表示]ペインで、IP アドレスのアクセス設定を含む行を選択して、次のいずれかの操作をします。
 - [削除]をクリックし、確認ウィンドウで再度[削除]をクリックします。
 - 削除する IP アドレスの横にある[-]オプションをクリックし、確認ウィンドウで再度[削除]をクリックします。

Mac 版での拡張保護

[詳細設定]ウィンドウでは、ノートン製品の拡張保護機能を設定できます。

次に、さまざまな拡張保護機能を示します。

- [ノートン ディープサイト コミュニティのダウンロード] シマンテック社が攻撃者として識別したコンピュータの IP アドレスの更新版リストを自動的に取得するよう、ノートン製品を設定できます。

[脆弱性保護]

Mac 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るように、ノートン製品を設定できます。

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や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。

拡張保護機能の有効化/無効化

[詳細設定]ウィンドウでは、ノートン製品の次の拡張保護機能を有効または無効にできます。

- [ノートン ディープサイト コミュニティのダウンロード]
- [脆弱性保護]

デフォルトでは、拡張保護機能が有効になっています。ファイアウォールのすべての拡張機能を有効にしておくことを推奨します。

ノートン ディープサイト コミュニティのダウンロードの有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [ディープサイト]行で、設定アイコンをクリックします。
- 5 [ノートン ディープサイトの設定]ウィンドウの[ダウンロード]タブで、次のいずれかの操作をします。
 - [ノートン ディープサイト コミュニティのダウンロード]を無効にするには、[オフ]を選択します。
 - [ノートン ディープサイト コミュニティのダウンロード]を有効にするには、[オン]を選択します。
- 6 [完了]をクリックします。

脆弱性保護の有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、スイッチを[オフ]または[オン]の位置に動かします。

Mac でのノートン ディープサイト コミュニティのダウンロード設定

ノートン ディープサイト コミュニティのダウンロード機能では、シマンテック社が攻撃者として識別した IP アドレスの更新リストを取得できます。

ノートン ディープサイト コミュニティのダウンロード機能をオンにして、シマンテック社のサーバーから IP アドレスの更新リストを取得できます。

[詳細設定]ウィンドウで [ノートン ディープサイト コミュニティのダウンロード]機能をオンまたはオフにして、シマンテック社のサーバーからの情報のダウンロードを許可または拒否できます。

ノートン ディープサイト コミュニティのダウンロードの設定

- 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]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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[ファイアウォール]をクリックします。

- 4 [ディープサイト]行で、設定アイコンをクリックします。

[ノートン ディープサイトの設定]ウィンドウには、シマンテック社が攻撃者として識別した IP アドレスのリストが表示されます。

- 5 [ダウンロード]タブで必要なオプションを選択してリスト内のすべての IP アドレスの接続を設定します。

次のオプションがあります。

[すべての接続を遮断する]

リスト内のすべての IP アドレスについて、着信接続と発信接続を遮断できます。

[着信接続のみを遮断する]

リスト内の IP アドレスからの着信接続のみを遮断できます。

- 6 [完了]をクリックします。

Mac での AutoBlock の設定

[脆弱性保護]ウィンドウの[自動遮断]ページを使って、シマンテック社が攻撃者として識別したコンピュータの IP アドレスを自動的に遮断できます。[自動遮断]オプションをオンにすると、ノートン製品は攻撃者の IP アドレスを[現在自動遮断が遮断するアドレス]リストに追加します。[アドレスをリストに残す期間]メニューを使って、攻撃者の IP アドレスからの任意の接続をノートン製品が遮断する期間を指定できます。

[削除]オプションを使って、[現在自動遮断が遮断するアドレス]リストから **IP** アドレスを削除できます。

また、[除外するアドレス]オプションを使って、信頼する **IP** アドレスの例外を作成できます。ノートン製品は、除外したアドレスからの接続を許可し、そのアドレスを[現在自動遮断が遮断するアドレス]リストに含めません。

自動遮断の設定

- 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]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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[ファイアウォール]をクリックします。

- 4 [脆弱性保護]行で、設定アイコンをクリックします。

- 5 [脆弱性保護]ウィンドウで、[自動遮断]ページを選択します。

- 6 [オン]オプションをクリックして、自動遮断をオンにします。

- 7 [現在自動遮断が遮断するアドレス]リストで、脆弱性保護機能によって遮断される **IP** アドレスのリストを確認します。

- 8 [アドレスをリストに残す期間]リストで、ノートン製品が接続を遮断する期間を設定します。

デフォルト値は **30** 分です。

- 9 [完了]をクリックします。

Macでのシグネチャの設定

脆弱性保護は頻繁に更新されるシグネチャのリストを使って既知の攻撃を検出します。シグネチャのリストは、[シグネチャ]リストで確認できます。

[シグネチャ]リストのシグネチャの横にある[有効]オプションと[通知]オプションを使って、シグネチャに一致するアクセス試行があったときに警告が表示されるようにできます。デフォルトでは、すべてのシグネチャが有効で、通知が選択されています。

[シグネチャ]リストのどのシグネチャも、無効にしないでください。シグネチャを無効にすると、[脆弱性保護]機能はシグネチャに関連する脅威からコンピュータを保護できません。

[脆弱性保護による攻撃の自動遮断時に通知する]警告を有効にして、脆弱性保護によって攻撃が遮断されたときに常に警告が表示されるようにすることもできます。

シグネチャの設定

- 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]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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [脆弱性保護]行で、設定アイコンをクリックします。
- 5 [脆弱性保護]ウィンドウで、[シグネチャ]ページを選択します。
- 6 [シグネチャ]リストで、シグネチャに必要なオプションを有効または無効にします。
- 7 [完了]をクリックします。

ノートンを最新版にアップグレードして Mac の保護を強化する

アップグレードすると、最新版のノートン デバイス向けセキュリティをダウンロードしてインストールできます。これにより、Mac で最新のセキュリティ機能を使用できます。アップグレードするにはオンラインにする必要があります。

メモ:最新版のノートンへのアップグレードは、ライブアップデートによる脅威定義の更新とは異なります。最新版のノートン デバイス向けセキュリティが利用可能な場合にのみアップグレードできます。ただし、いつでもライブアップデートを実行して最新の脅威定義や多少更新されたアプリケーション拡張機能を入手できます。

通知や警告が表示された場合のアップグレード

アップグレード警告または通知を表示するには、[自動アップグレード]オプションを有効にする必要があります。デフォルトでは、[自動アップグレード]オプションは有効になっています。

- 1 アップグレード警告で[アップグレード]をクリックします。
- 2 ライセンスが最新の場合は、以下の操作を行います。
 - [無料の製品アップグレード]ウィンドウで[今すぐアップグレード]をクリックします。
 - プロンプトが表示されたら、管理者アカウントパスワードを入力して、[インストールヘルパー]をクリックします。
 - [再起動する]をクリックしてアップグレードプロセスを完了します。
- 3 ライセンスの期限が切れている場合は、以下の操作を行います。
 - 期限が切れたライセンスをアンインストールするには、[同意してインストールする]をクリックして、[続行する]をクリックします。
 - [再起動する]をクリックしてアンインストールします。
 - コンピュータが再起動されたら、最新版のノートンにアップグレードしたり体験版を使用できます。ノートン製品使用許諾契約を読んでから、[同意してインストールする]をクリックします。
 - [再起動する]をクリックしてアップグレードプロセスを完了します。

Mac メニューバーに[アップグレードできます]と表示された場合のアップグレード

- 1 Mac メニューバーで、シマンテックアイコンをクリックします。
- 2 [アップグレードできます]をクリックします。
- 3 ライセンスが最新の場合は、以下の操作を行います。
 - [無料の製品アップグレード]ウィンドウで[今すぐアップグレード]をクリックします。
 - プロンプトが表示されたら、管理者アカウントパスワードを入力して、[インストールヘルパー]をクリックします。
 - [再起動する]をクリックしてアップグレードプロセスを完了します。
- 4 ライセンスの期限が切れている場合は、以下の操作を行います。
 - 期限が切れたライセンスをアンインストールするには、[同意してインストールする]をクリックして、[続行する]をクリックします。
 - [再起動する]をクリックしてアンインストールします。
 - コンピュータが再起動されたら、最新版のノートンにアップグレードしたり体験版を使用できます。ノートン製品使用許諾契約を読んでから、[同意してインストールする]をクリックします。
 - [再起動する]をクリックしてアップグレードプロセスを完了します。

ノートンのメインウィンドウの[ヘルプ]ドロップダウンに[アップグレードできます]と表示された場合のアップグレード

- 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[ヘルプ]をクリックします。
- 3 [ヘルプ]ドロップダウンメニューで[アップグレードできます]をクリックします。
- 4 ライセンスが最新の場合は、以下の操作を行います。
 - [無料の製品アップグレード]ウィンドウで[今すぐアップグレード]をクリックします。
 - プロンプトが表示されたら、管理者アカウントパスワードを入力して、[インストールヘルパー]をクリックします。
 - [再起動する]をクリックしてアップグレードプロセスを完了します。
- 5 ライセンスの期限が切れている場合は、以下の操作を行います。
 - 期限が切れたライセンスをアンインストールするには、[同意してインストールする]をクリックして、[続行する]をクリックします。
 - [再起動する]をクリックしてアンインストールプロセスを完了します。

- コンピュータが再起動されたら、最新版のノートンにアップグレードしたり体験版を使用できます。ノートン製品使用許諾契約を読んでから、[同意してインストールする]をクリックします。
- [再起動する]をクリックしてアップグレードプロセスを完了します。

自動アップグレードの有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[製品の設定]をクリックします。
- 4 [自動アップグレード]行で、スイッチを[オフ]または[オン]の位置に動かします。

Mac でのノートン コミュニティウォッチによる潜在的な新しい脅威の特定

ノートン製品を使用している場合、ノートンコミュニティウォッチにより脅威の特定が向上し、新しいセキュリティの脅威から保護する時間を短縮できます。このプログラムは、選択したセキュリティデータとアプリケーションデータを収集し、そのデータをシマンテック社に送信して分析し、新しい脅威とその発生源を特定します。このプログラムは、ユーザーから送信されたデータを分析することで、セキュリティ製品を向上させ、より強力にします。

ノートンが特定の製品のデータにアクセスし、収集、処理する方法について詳しくは、[ノートン プライバシーポリシー](#) お読みください。

ノートン コミュニティウォッチ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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[製品の設定]をクリックします。
- 4 [ノートン コミュニティウォッチ]行で、スイッチを[オフ]または[オン]の位置に動かします。

Mac でノートンにエラーが発生した場合のシマンテック社へのレポートの送信

ノートンエラー管理により、ノートン製品で発生した問題が文書にされます。このような場合、ユーザーはシマンテック社にエラーを報告できます。

[エラー管理]のオンとオフの切り替え

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[製品の設定]をクリックします。
- 4 [エラー管理]行で、スイッチを[オフ]または[オン]の位置に動かします。
- 5 [エラー管理]ウィンドウで設定アイコンをクリックし、ノートンを有効にしてエラーに関する詳しいデータを送信します。
- 6 シマンテック社が収集するデータについて詳しくは、[エラー管理]ウィンドウで[収集対象]をクリックしてください。
ノートンが特定の製品のデータにアクセスし、収集、処理する方法について詳しくは、[ノートンプライバシー](#) ポリシーを参照してください。

Mac 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 クリーンを実行して Mac の速度を低下させる可能性があるファイルを削除する
- ノートンクリーンのスキャンをスケジュール設定またはカスタマイズして、Mac のパフォーマンスを改善する

ノートン クリーンを実行して Mac の速度を低下させる可能性があるファイルを削除する

一時ファイル、インストールファイル、電子メールや写真アルバムの重複ファイルなどのジャンクファイルは、コンピュータのパフォーマンスに影響を及ぼす可能性があります。ノートンクリーンは、Mac の速度を低下させる可能性があるさまざまな種類のジャンクファイルを削除します。

ノートン クリーンは、接続されたデバイスはスキャンしません。また、Mac OS X 10.10.5 以降でのみ実行できます。デフォルトでは、ノートンクリーンはジャンクファイルをゴミ箱に移動するだけで削除しません。ジャンクファイルを自動的に削除するようにノートン クリーンを設定するには、p.43 の「ノートン クリーンのスキャンをスケジュール設定またはカスタマイズして、Mac のパフォーマンスを改善する」を参照してください。を参照してください。

ノートン クリーンを実行してジャンクファイルを削除する

- 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[クリーン]をクリックします。
- 3 [今すぐ実行]または[開始する]をクリックします。
ノートンクリーンによって写真や iTunes アプリを開くかどうか確認されたら、[開く]をクリックします。

- 4 [概要]ウィンドウの[類似]行と[重複]行で、[レビュー]をクリックし、削除するファイルを選択して、[完了]をクリックします。

類似とは、2つのファイルが同一に見えるが、ファイル名が異なるなど、若干の違いがあることを意味します。重複とは、ファイルが同一であることを意味します。

- 5 [クリーン]をクリックすると、選択したファイルがゴミ箱に移動されます。

[クリーンアップが完了しました]ウィンドウで、スキャンの結果を確認できます。

ノートンクリーンのスキャンをスケジュール設定またはカスタマイズして、Mac のパフォーマンスを改善する

ノートン クリーンのスケジュール設定またはカスタマイズ

- 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[クリーン]をクリックします。
- 3 [クリーン]ウィンドウで、[今すぐ実行]または[開始する]ボタンの横にある設定アイコンをクリックします。
- 4 ポップアップで、次のタブをクリックして、スキャンのスケジュール設定または設定の構成を行います。
 - 一般
 - [検索対象]の横で、ノートン クリーンで削除するファイルの種類を選択します。最善の結果を得るには、すべてのデフォルトのチェックマークを付けたままにします。
 - [ノートンクリーンのスケジュールを設定]の横で、定期スキャンを実行する頻度を設定します。
 - [ディスク容量が少なくなったらノートンクリーンを実行]を選択すると、ハードディスクドライブ容量がいっぱいになり近付いたときに自動的にファイルを削除できます。
 - ノートン クリーンを実行したときにジャンクファイルをゴミ箱に移動するか、すぐに完全に削除するかのをいずれかにチェックマークを付けます。ゴミ箱にファイルを移動する場合、ファイルを完全に削除するにはゴミ箱を空にする必要があります。
 - 類似と重複

ほとんどのユーザーは、デフォルトの設定を使用すると最善の結果が得られます。

 - 左ペインで[一般]を選択し、次の操作を行います。
ノートン クリーンを実行するたびに[写真]と iTunes アプリを開くかどうか尋ねないようにする場合は、これらを自動的に開くオプションを選択します。
重複や類似ファイルが最も見つけやすい場所以外もノートンクリーンでスキャンする場合は、[拡張検索を実行]を選択します。

ノートン クリーンのスキャンをスケジュール設定またはカスタマイズして、Mac のパフォーマンスを改善する

- 左ペインの[除外]で、次の操作を行います。
スキャンから除外するファイルの種類を追加または削除する場合は、[ファイルの種類]を選択します。
スキャンから除外する特定のファイルまたはフォルダにナビゲートする場合は、[パス]を選択し、[+]をクリックします。
- 左ペインの[種類]で、次の操作を行います。
デフォルトの設定を変更するには、各ファイルの種類をクリックして、オプションを選択します。
- 自動選択
 - [+]アイコンをクリックします。
 - [自動選択ルールを追加]ウィンドウで、ドロップダウンを使用して、ノートン クリーンを実行するときにスキャンの対象または対象外にするファイルのルールを追加します。

重要なデータの保全

この章では以下の項目について説明しています。

- **Mac** で詐欺またはフィッシング Web サイトを検出できるようにノートンを設定する
- **Mac** で安全に閲覧、買い物を行うためのノートンのブラウザ拡張機能の追加

Mac で詐欺またはフィッシング Web サイトを検出できるようにノートンを設定する

ノートンのデバイスセキュリティには、Firefox、Safari、または Chrome を使用して閲覧しているときにサイトを分析するセーフウェブが含まれています。サイトのセキュリティについてランク付けして、詐欺またはフィッシングサイトを検出すると警告を表示します。セーフウェブを使用すると、金融情報や個人情報を入力させるために不正なショッピングサイトなどの偽のサイトを構築するサイバー犯罪者から保護できます。

セーフウェブのオプションの有効化と設定

メモ: Mac OS X 10.9 以前のバージョンでのみ、セーフウェブのオプションを有効にして設定できます。

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[セーフウェブ]をクリックし、[セーフウェブ]スイッチがオンになっていることを確認します。
- 4 [セーフウェブ]行で、設定アイコンをクリックし、必要に応じて次のオプションを設定します。
 - 検索エンジンの結果を拡張し、検索結果にサイトの評価を表示する
 - 有害な Web サイトの参照時に警告を表示する

- 有害な Web サイトを遮断する
- フィッシング対策をオンにして、表示する Web サイトのセキュリティレベルを分析する
- 疑わしい Web サイトが検出されたときに分析のためシマンテック社にサイトの URL を送信できるように、完全 URL を提出する

ノートン セーフサーチをデフォルトの検索エンジンとして有効にする

さらに、ノートン ホームページをデフォルトのホームページとして設定できます。

- 1 ブラウザを開いて、セーフウェブの拡張子アイコンをクリックします。
- 2 表示されるセーフウェブのポップアップで、設定アイコンをクリックします。
- 3 [ブラウザの設定] ページで、[ノートン セーフサーチをデフォルトの検索エンジンとして有効にします] にチェックマークを付けます。

Mac で安全に閲覧、買い物を行うためのノートンのブラウザ拡張機能の追加

Mac にノートンをインストールした後、初めて Safari、Firefox、または Chrome を開くと、ブラウザ拡張機能を追加するように求められます。ノートンでは、ブラウザにフォーカスを置いたときのみブラウザ拡張機能警告が表示されるブラウザフォーカス機能が提供されています。オンラインでのセキュリティを最大限に高めるには、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 マネージャー拡張機能を有効にします。

Mac OS X 10.10.x 以降を利用している場合、ノートンのスタンドアロンのブラウザ拡張機能は、ノートン製品をアンインストールした後でも使用できます。Mac OS X 10.9 以前からノートン製品をアンインストールする場合、Chrome ブラウザにインストールされた拡張機能を除いて、Safari と Firefox に関連するすべてのブラウザ拡張機能が削除されます。

メモ: ノートン セーフウェブ、ノートン ホームページ、ノートン セーフサーチ、ノートン ID セーフのスタンドアロンの拡張機能は、Mac OS X 10.9 以前と旧バージョンの Web ブラウザではサポートされません。最新のノートンのブラウザ拡張機能をインストールするには、使用している Mac オペレーティングシステムと Web ブラウザを最新バージョンにアップグレードします。

Mac OS X 10.10 以降へのノートンのブラウザ拡張機能の追加

Safari

macOS 10.14.4 (Mojave) 以上での Safari 12 以上のバージョン

- 1 ノートンのインストール後に初めて Safari を起動すると、ノートン セーフウェブやノートン セーフウェブプラスの警告が表示されます。
- 2 警告で次のいずれかの操作を実行します。

- ノートン セーフウェブの拡張機能をインストール場合は、[ダウンロード]をクリックします。
- ノートン セーフウェブの拡張機能を後でインストール場合は、[後で通知する]をクリックします。
- [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを 3 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から 2 週間この警告が無視されます。

メモ: デフォルト Web ブラウザが Safari の場合、2 週間後に[今すぐ解決]という警告が表示されます。ノートン セーフウェブの拡張機能をインストールするには、[今すぐ解決]をクリックします。[今すぐ解決]の警告を無視すると、6 カ月後、Safari ブラウザを開いたときに改めて警告が表示されます。

詳しくは、「[Safari 版ノートン セーフウェブプラスアプリ拡張機能のダウンロードとインストール](#)」を参照してください。

Firefox

- 1 ノートンをインストールした後、初めて Firefox ブラウザにフォーカスを置くと、新しいタブで Firefox の[ブラウザ保護]ページが自動的に開き、ノートン セーフサーチ、ノートン ホームページ、ノートン セーフウェブ、ノートン ID セーフを含む拡張機能をインストールできます。

メモ: ノートン セーフサーチのスタンドアロンの拡張機能は、Firefox の最新バージョンでのみサポートされます。

- 2 [有効にする]オプションを使用すると、画面上の指示に従ってブラウザ拡張機能を有効にできます。代わりに、[ノートンのすべての拡張機能を有効にする]オプションを使用してすべてのブラウザ拡張機能をインストールすることもできます。
- 3 ノートン ID セーフ以外の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 Firefox を起動すると Firefox のブラウザ拡張機能の警告が表示されます。警告で次のいずれかの操作を実行します。
 - [追加する]をクリックすると、新しいタブで Firefox の[ブラウザ保護]ページが自動的に開きます。[有効にする]オプションを使用すると、画面上の指示に従って拡張機能を有効にできます。
 - [後で通知する]をクリックすると、後でノートンのブラウザ拡張機能をインストールできます。
 - [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを 3 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から 2 週間この警告が無視されます。

メモ: 2 週間後、デフォルト Web ブラウザが **Firefox** で、ノートン セーフウェブの拡張機能をインストールしていない場合、[今すぐ解決]という警告が表示されます。[今すぐ解決]をクリックすると、ブラウザ拡張機能がインストールされます。[今すぐ解決]の警告を無視すると、6 カ月後、**Firefox** ブラウザを開いたときに改めて **Firefox** ブラウザ拡張機能の警告が表示されます。

Chrome

- 1 ノートンをインストールした後、初めて **Chrome** ブラウザを開くと、**Chrome** の[ブラウザ保護]ページが自動的に起動され、ノートン セーフサーチ、ノートン ホームページ、ノートン セーフウェブ、ノートン ID セーフを含む拡張機能をインストールできます。
- 2 [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ブラウザの拡張機能を有効にできます。代わりに、[ノートンのすべての拡張機能の追加]オプションを使用してすべてのブラウザ拡張機能をインストールすることもできます。
- 3 ノートン ID セーフ以外の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 **Chrome** を起動すると **Chrome** のブラウザ拡張機能の警告が表示されます。警告で次のいずれかの操作を実行します。
 - [追加する]をクリックすると、**Chrome** の[ブラウザ保護]ページが自動的に開きます。[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拡張機能を有効にできます。
 - [後で通知する]をクリックすると、後でノートンのブラウザ拡張機能をインストールできます。
 - [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを 3 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から 2 週間この警告が無視されます。

メモ: 2 週間後、デフォルト Web ブラウザが **Chrome** で、ノートン セーフウェブの拡張機能をインストールしていない場合、[今すぐ解決]という警告が表示されます。[今すぐ解決]をクリックすると、ブラウザ拡張機能がインストールされます。[今すぐ解決]の警告を無視すると、6 カ月後、**Chrome** ブラウザを開いたときに改めて **Chrome** ブラウザ拡張機能の警告が表示されます。

Mac OS X 10.9 以前へのノートンのブラウザ拡張機能の追加

Safari

- 1 ノートンをインストールした後、初めて **Safari** ブラウザを開くと、ノートン製品によって **Safari** のブラウザ拡張機能の警告が表示され、ノートン セーフサーチ、ノートン ホームページ、ノートン セーフウェブなどのブラウザ固有の機能を含む拡張機能をインストールできます。
- 2 次のいずれかの操作をします。

- [追加する]をクリックすると、ノートンのブラウザ拡張機能をインストールできます。新しいタブで **Safari** の[ブラウザ保護]ページが自動的に開きます。[今すぐ有効化]オプションを使用すると、画面上の指示に従って拡張機能を有効にできます。
- [後で通知する]をクリックすると、後でノートンのブラウザ拡張機能をインストールできます。
- [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを **3** 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から **2** 週間この警告が無視されます。

メモ: 2 週間後、デフォルト Web ブラウザが **Safari** で、ノートン セーフウェブの拡張機能をインストールしていない場合、[今すぐ解決]という警告が表示されます。[今すぐ解決]をクリックすると、ブラウザ拡張機能がインストールされます。[今すぐ解決]の警告を無視すると、**6** カ月後、**Safari** ブラウザを開いたときに改めて **Safari** ブラウザ拡張機能の警告が表示されます。

Firefox

- 1 ノートンをインストールした後、初めて **Firefox** ブラウザを開くと、ノートン製品によって **Firefox** のブラウザ拡張機能の警告が表示され、ノートン セーフサーチ、ノートン ホームページ、ノートン セーフウェブなどのブラウザ固有の機能を含む拡張機能をインストールできます。
- 2 次のいずれかの操作をします。
 - [追加する]をクリックすると、**Firefox** ブラウザによって、拡張機能のポップアップが新しいタブで開きます。[追加する]をクリックすると、新しいタブで **Firefox** の[ブラウザ保護]ページが自動的に開きます。[今すぐ有効化]オプションを使用すると、画面上の指示に従って拡張機能を有効にできます。
 - [後で通知する]をクリックすると、後でノートンのブラウザ拡張機能をインストールできます。
 - [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを **3** 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から **2** 週間この警告が無視されます。

メモ: 2 週間後、デフォルト Web ブラウザが **Safari** で、ノートン セーフウェブの拡張機能をインストールしていない場合、[今すぐ解決]という警告が表示されます。[今すぐ解決]をクリックすると、ブラウザ拡張機能がインストールされます。[今すぐ解決]の警告を無視すると、**6** カ月後、**Safari** ブラウザを開いたときに改めて **Safari** ブラウザ拡張機能の警告が表示されます。

Chrome

- 1 ノートンをインストールした後、初めて **Chrome** ブラウザを開くと、**Chrome** の[ブラウザ保護] ページが自動的に起動され、ノートンセーフサーチ、ノートンホームページ、ノートンセーフウェブを含む拡張機能をインストールできます。
- 2 [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ブラウザ拡張機能を有効にできます。代わりに、[ノートンのすべての拡張機能の追加]オプションを使用してすべてのブラウザ拡張機能をインストールすることもできます。
- 3 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 **Chrome** を起動すると **Chrome** のブラウザ拡張機能の警告が表示されます。警告で次のいずれかの操作を実行します。
 - [追加する]をクリックすると、**Chrome** の[ブラウザ保護]ページが自動的に開きます。[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拡張機能を有効にできます。
 - [後で通知する]をクリックすると、後でノートンのブラウザ拡張機能をインストールできます。
 - [いいえ、必要ありません]: このオプションは、[後で通知する]オプションを 3 回使用すると表示されます。[後で通知する]の代わりに[いいえ、必要ありません]オプションを含むブラウザ拡張機能の警告が表示されます。[いいえ、必要ありません]オプションをクリックすると、その時点から 2 週間この警告が無視されます。

メモ: 2 週間後、デフォルト Web ブラウザが **Chrome** で、ノートン セーフウェブの拡張機能をインストールしていない場合、[今すぐ解決]という警告が表示されます。[今すぐ解決]をクリックすると、ブラウザ拡張機能がインストールされます。[今すぐ解決]の警告を無視すると、6 カ月後、**Chrome** ブラウザを開いたときに改めて **Chrome** ブラウザ拡張機能の警告が表示されます。

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。

- **Mac** 版での接続遮断設定
- **Mac** での接続遮断の設定
- アプリケーションのアクセス設定
- アプリケーションのアクセスの設定
- サービスのアクセス設定
- サービスのアクセスの設定
- サービスの特定のアクセス設定のカスタマイズ
- サービスのアクセス設定の編集
- サービスのアクセス設定の削除
- **Mac** でのアプリケーションのファイアウォールの設定
- **Mac** でのアプリケーションのファイアウォールルールの設定
- **Mac** でのアプリケーションのファイアウォールルールの削除
- **Mac** 版でのネットワークの検出の設定
- **Mac** でのネットワークの検出の有効化/無効化
- ネットワーク上の場所に対する接続遮断の設定のエクスポート
- **Mac** でゲームをしたり映画を鑑賞するときのバックグラウンドタスクの停止

Mac 版での接続遮断設定

アプリケーション、サービス、IP アドレスに対して接続遮断を設定できます。接続遮断の設定に基づいて、ファイアウォールは着信と発信のネットワーク接続を許可または遮断します。

設定する接続遮断の設定は、選択したネットワーク上の場所に固有です。この設定は、指定したネットワーク上の場所に **Mac** が接続するときのみ適用されます。

次に対して接続遮断を設定できます。

アプリケーション	Mac で動作するアプリケーションのアクセス設定を指定できます。
サービス/ポート	Mac で動作するサービスとポートのアクセス設定を指定できます。
ゾーン	発信接続や着信接続を許可または遮断する IP アドレスを指定できます。
すべてを優先度の順に	選択したファイアウォール設定のすべてのアクセス設定を表示できます。 設定が重複するときは、リストの上位の設定がリストの下位の設定より常に優先されます。

Mac での接続遮断の設定

接続遮断の設定は、特定のアプリケーション、サービス、ポート、IP アドレスを使う着信接続と発信接続に適用されます。

[接続の遮断]ウィンドウを使って、アプリケーションまたはサービスのインターネットやローカルネットワークへの接続を許可するかどうかを設定できます。[編集中の設定]メニューから目的のネットワーク上の場所を選択して、接続遮断を設定できます。

メモ: [詳細設定]ウィンドウで[接続の遮断]オプションが有効な場合にのみ、[接続の遮断]設定を設定できます。

メモ: このタスクを実行するには、管理者権限を持つユーザーアカウントが必要です。

接続遮断の設定

- 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]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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断を設定するネットワーク上の場所を選択します。
- 6 [表示]メニューのオプションを選択します。

[表示]メニューに表示されるオプションは、[編集中の設定]メニューで選択したネットワーク上の場所によって異なります。

次のオプションがあります。

アプリケーション

Macで動作するアプリケーションの接続遮断の設定を指定できます。

サービス/ポート

Macで動作するサービスとポートに接続遮断の設定を指定できます。

ゾーン

ファイアウォールで発信または着信接続を許可または遮断するIPアドレスを指定できます。

すべてを優先度の順に

アプリケーション、サービス、ポート、ゾーンに対する現在の接続遮断の設定を優先度の順に指定できます。

- 7 次のいずれかのページを選択します。

[着信]

Macで動作するアプリケーションまたはサービスを使う着信接続のアクセス設定を指定できます。

[発信]

Macで動作するアプリケーションまたはサービスを使う発信接続のアクセス設定を指定できます。

[着発信]

指定したIPアドレスへの発信接続と着信接続のアクセスを設定できます。

このページは、[表示]メニューで[ゾーン]を選択した場合にのみ表示されます。

- 8 [接続の遮断]ウィンドウの下部にある[処理]ポップアップメニューを使って、接続遮断のその他の設定を指定します。次のオプションがあります。

ログと通知の設定

ノートン製品で記録を保持するアクセス試行の種類を指定できます。

ノートン製品で通知するアクセス試行の種類も指定できます。

拡張設定

ファイアウォールの拡張オプションを指定できます。

デフォルトに戻す

設定をデフォルトのレベルにリセットできます。

- 9 [完了]をクリックします。

アプリケーションのアクセス設定

[接続の遮断]ウィンドウを使って、ネットワークに接続するアプリケーションのアクセス設定を指定できます。ファイアウォールをカスタマイズして、iTunes などのアプリケーションに対する着信または発信のネットワーク接続を許可または遮断できます。

アプリケーションのデフォルトのアクセス設定と特定のアクセス設定を設定することもできます。デフォルトのアクセス設定は、ネットワーク内のすべての着信接続と発信接続に適用されます。特定のアクセス設定を使うと、特定のコンピュータへの接続を許可または遮断できます。

[接続の遮断]ウィンドウを使って、アプリケーションに対して次のことを実行できます。

- アクセスを設定する
- 特定のアクセス設定をカスタマイズする
- アクセス設定を編集する
- アクセス設定を削除する

アプリケーションのアクセスの設定

ノートン製品では、Mac で動作するアプリケーションのアクセス設定を構成できます。ファイアウォールは、指定された設定と、Mac のネットワーク上の場所に基づいて、着信接続と発信接続を許可または遮断します。

アプリケーションのアクセスを設定すると、アプリケーションの名前が[接続の遮断]ウィンドウの[表示]ペインに表示されます。また、選択したアプリケーションのデフォルトのアクセス設定がアプリケーション名の下に表示されます。

ノートン製品によって、[<他のすべてのアプリケーション>]アクセス設定がデフォルトで作成されます。このアクセス設定には、Mac で動作するすべてのアプリケーションが含まれます。

アプリケーションのアクセスの設定

- 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]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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、アクセスを設定するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[アプリケーション]を選択します。
- 7 次のいずれかのページを選択します。

[着信]	アプリケーションの着信接続のアクセス設定を指定できます。
------	------------------------------

[発信]	アプリケーションの発信接続のアクセス設定を指定できます。
------	------------------------------

- 8 [アプリケーションの追加]をクリックします。
- 9 [アプリケーションの選択]ダイアログボックスで目的のアプリケーションを選択します。
 目的のアプリケーションがリストに表示されない場合は、[その他]をクリックしてアプリケーションを検索します。
- 10 ダイアログボックスの上部にあるメニューで、次のいずれかのデフォルトのアクセス設定を選択します。

許可する	このアプリケーションのネットワーク接続を許可します。
------	----------------------------

遮断する	このアプリケーションのネットワーク接続を遮断します。
------	----------------------------

確認	プログラムがインターネットにアクセスを試みるときにファイアウォールが通知するように設定します。
----	-------------------------------------------------

- 11 [選択]をクリックします。
 [接続の遮断]ウィンドウの[表示]ペインに、追加したアプリケーションの名前が表示されます。

- 12 [接続の遮断]ウィンドウ下部の[処理]ドロップダウンメニューを使用して、ファイアウォールの拡張設定を指定します。次のオプションがあります。

ログと通知の設定	ノートン製品で記録を保持するアクセス試行の種類を指定できます。
[拡張設定]	ファイアウォールの拡張オプションを指定できます。
デフォルトに戻す	設定をデフォルトのレベルにリセットできます。

- 13 [完了]をクリックします。

サービスのアクセス設定

[接続の遮断]ウィンドウを使って、Mac で動作しているサービスのアクセス設定を指定できます。たとえば、Mac 上の共有フォルダへのポート 21 を使ったアクセスを許可するファイル転送プロトコル (FTP) サービスのアクセス設定をカスタマイズできます。FTP のファイアウォールをカスタマイズして着信接続と発信接続を許可または遮断できます。

既存のサービスを追加すると、ノートン製品はそのサービスが着信接続と発信接続の通信に使うポートを表示します。

サービスのデフォルトのアクセス設定と特定のアクセス設定を指定することもできます。デフォルトのアクセス設定は、そのサービスを使うコンピュータのすべての着信接続と発信接続に適用されます。特定のアクセス設定を使うと、特定のコンピュータへの接続を許可または遮断できます。

[接続の遮断]ウィンドウを使って、サービスに対して次のことを実行できます。

- アクセスを設定する
- 特定のアクセス設定をカスタマイズする
- アクセス設定を編集する
- アクセス設定を削除する

サービスのアクセスの設定

ノートン製品では、Mac で動作するサービスのアクセス設定を指定できます。ファイアウォールは、指定されたアクセス設定と、Mac の現在のネットワーク上の場所に基づいて、サービスを使うネットワーク接続を許可または遮断します。

設定するアクセス設定は、選択したネットワーク上の場所に固有です。接続遮断を設定したネットワーク上の場所に Mac が接続するときのみ Mac に適用されます。

サービスを追加すると、[接続の遮断]ウィンドウの[表示]ペインに、サービスの名前が表示されます。また、サービスのデフォルトのアクセス設定がサービス名の下に表示されます。

デフォルトでは、ノートン製品によって[<他のすべてのサービス>]アクセス設定が作成されます。このアクセス設定には、Macで動作するすべてのサービスが含まれます。

サービスのアクセス設定の指定

- 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 ノートン製品のメインウィンドウで[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、アクセスを設定するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 次のいずれかのページを選択します。

[着信] サービスを使う着信接続のアクセス設定を指定できます。

[発信] サービスを使う発信接続のアクセス設定を指定できます。

- 8 [サービスを追加]をクリックします。
- 9 表示される[新しいサービス]ダイアログボックスで、サービスに対して適用するデフォルトのアクセス設定オプションを選択します。次のオプションがあります。

[許可する] このサービスのネットワーク接続を許可します。

[遮断する] このサービスのネットワーク接続を遮断します。

- 10 [サービス名]メニューで目的のサービスを選択します。
サービスが[サービス名]メニューに表示されていない場合は、[サービス名]メニューに新しいサービスの名前を入力します。また、[説明]フィールドにサービスの説明を入力することもできます。

11 必要に応じて次のページを設定します。

[ポート]	<p>サービスが開くことのできるファイアウォールのポートを指定します。</p> <p>新しいサービスを追加するときのみ、[追加]オプション、[編集]オプション、[削除]オプションを使うことができます。</p> <p>これらのオプションを使って、ポート番号を追加したり、追加するポート番号を修正することができます。</p>
[ログ記録]	<p>ノートン製品がログを記録する必要がある接続の種類を示します。</p>
[通知]	<p>接続が試行されたときにノートン製品で通知する接続の種類を指定します。</p> <p>このサービスを使う接続試行をファイアウォールで許可するか遮断するかを選択できます。</p>

12 [保存]をクリックします。

13 [接続の遮断]ウィンドウ下部の[処理]ドロップダウンメニューで、ファイアウォールの拡張設定を指定します。次のオプションがあります。

ログと通知の設定	<p>ノートン製品で記録を保持するアクセス試行の種類を指定できます。</p> <p>ノートン製品で通知するアクセス試行の種類も指定できます。</p>
拡張設定	<p>ファイアウォールの拡張オプションを指定できます。</p>
デフォルトに戻す	<p>設定をデフォルトのレベルにリセットできます。</p>

14 [完了]をクリックします。

サービスの特定のアクセス設定のカスタマイズ

ノートン製品では、Mac上のサービスごとに着信と発信のネットワーク接続設定をカスタマイズできます。接続の試みを許可または遮断するIPアドレスを指定できます。指定した特定のアクセス設定は、アプリケーション名の下に行に、マイナス (-) とプラス (+) 記号とともに表示されます。

メモ: サービスに対して任意の数の特定のアクセス設定を追加できます。たとえば、あるサービスに対して、ネットワーク上のすべてのコンピュータからの接続を許可する特定のアクセス設定を追加できます。同じサービスに対して、単一のコンピュータからの接続を遮断する別の特定のアクセス設定も追加できます。

サービスの特定のアクセス設定のカスタマイズ

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集集中の設定]メニューで、特定のアクセス設定を指定するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 次のいずれかのページを選択します。

[着信]	サービスを使う着信接続のアクセス設定を指定できます。
------	----------------------------

[発信]	サービスを使う発信接続のアクセス設定を指定できます。
------	----------------------------

- 8 [表示]ペインで、サービス名の横にある[+]記号をクリックします。
- 9 [アドレスを編集]ダイアログボックスで、接続のアクセスの種類を選択します。次のオプションがあります。

許可する	特定の IP アドレスの発信または着信接続を許可できます。
------	-------------------------------

遮断する	特定の IP アドレスの発信または着信接続を遮断できます。
------	-------------------------------

10 次のいずれかのオプションを選択して特定のアクセス設定をカスタマイズします。

ネットワーク上のすべてのコンピュータ	ネットワーク上のすべてのコンピュータの発信接続や着信接続を許可または遮断できます。
[単一のコンピュータ]	指定した IP アドレスのコンピュータの発信接続や着信接続を許可または遮断できます。
[次の番号で始まるすべての IP アドレス]	指定した基準アドレスを持つコンピュータに対して発信接続や着信接続を許可または遮断できます。
[ネットワーク上のすべての IP アドレス]	ローカルネットワーク上のコンピュータの発信接続や着信接続を許可または遮断できます。

11 [保存]をクリックします。

サービスのアクセス設定の編集

サービスの次のアクセス設定を編集できます。

- アクセス設定
- 特定のアクセス設定
- デフォルトのアクセス設定

サービスのアクセス設定の編集

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断の設定を編集するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 次のいずれかのページを選択します。

[着信]	サービスを使う着信接続のアクセス設定を指定できます。
------	----------------------------

[発信]	サービスを使う発信接続のアクセス設定を指定できます。
------	----------------------------

- 8 [表示]ペインで、サービス名を含む行を選択して、[編集]をクリックします。
- 9 [サービスを編集]ダイアログで、必要に応じて変更します。
- 10 [保存]をクリックします。

サービスの特定のアクセス設定の編集

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断の設定を編集するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 [着信]ページまたは[発信]ページで、特定のアクセス設定を編集するサービスを選択します。
- 8 [表示]ペインで、アプリケーションの特定のアクセス設定を含む行を選択して、[編集]をクリックします。
- 9 [サービスを編集]ウィンドウで、必要に応じて変更します。
- 10 [保存]をクリックします。

サービスのデフォルトのアクセス設定の編集

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断の設定を編集するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 [着信]タブまたは[発信]タブの[表示]ペインでサービスのデフォルトのアクセス設定を含む行を選択し、[編集]をクリックします。

- 8 表示される[<サービス名>のデフォルト処理]ウィンドウで、次のオプションのいずれかを選択します。

許可する	このサービスのネットワーク接続を許可します。
[遮断する]	このサービスのネットワーク接続を遮断します。

- 9 [保存]をクリックします。

サービスのアクセス設定の削除

[接続の遮断]ウィンドウを使って、サービスに対して設定したアクセス設定と特定のアクセス設定を削除できます。

ただし、リストに表示されるデフォルトの接続遮断の設定は削除できません。

サービスのすべてのアクセス設定の削除

- 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。
- ノートン製品のメインウィンドウで[詳細設定]または[設定]をクリックします。
- 左ペインで[ファイアウォール]をクリックします。
- [接続の遮断]行で、設定アイコンをクリックします。
- [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断の設定を削除するネットワーク上の場所を選択します。
- [表示]メニューで、[サービス/ポート]を選択します。
- 次のいずれかのページを選択します。

[着信]	サービスを使う着信接続のアクセス設定を指定できます。
[発信]	サービスを使う発信接続のアクセス設定を指定できます。
- [表示]ペインで目的のサービスを選択し、次のいずれかの操作をします。
 - [削除]をクリックします。
 - サービス名の横にある[-]記号をクリックします。
- 確認ウィンドウで[削除]をクリックします。

サービスの個々のアクセス設定の削除

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [接続の遮断]行で、設定アイコンをクリックします。
- 5 [接続の遮断]ウィンドウの[編集中の設定]メニューで、接続遮断の設定を削除するネットワーク上の場所を選択します。
- 6 [表示]メニューで、[サービス/ポート]を選択します。
- 7 次のいずれかのページを選択します。

[着信] サービスを使う着信接続のアクセス設定を指定できます。

[発信] サービスを使う発信接続のアクセス設定を指定できます。

- 8 [表示]ペインで、サービスの特定のアクセス設定を含む行を選択して、次のいずれかの操作をします。
 - [削除]をクリックします。
 - サービス名の横にある[-]記号をクリックします。
- 9 確認ウィンドウで[削除]をクリックします。

Macでのアプリケーションのファイアウォールの設定

アプリケーションの遮断の設定では、Macで動作するさまざまなアプリケーションのファイアウォールルールを設定できます。これらの設定に基づいて、ファイアウォールはアプリケーションからのインターネットへの接続を許可または遮断できます。

メモ: Macが接続されているネットワークに基づくアプリケーションのファイアウォール設定は指定できません。アプリケーションの遮断の設定は、ネットワーク上の場所に関係なく同じです。アプリケーションの遮断では、特定のIPアドレスへの接続を許可または遮断することはできません。

インターネットアクセスを指定していないアプリケーションがインターネットに接続しようとしたときは、ノートン製品の通知ダイアログが表示されます。そのアプリケーションのインターネットアクセスをファイアウォールで許可するか遮断するかを選択できます。

[アプリケーションの遮断]ウィンドウでは、アプリケーションのインターネットアクセスの設定に加えて、アプリケーションの次のオプションも選択できます。

[検索アイコン]	[設定]リスト内でアプリケーションを検索できます。
[アプリケーションの追加]	アプリケーションを追加してインターネットアクセスを手動で設定できます。
[削除]	選択したアプリケーションを[設定]リストから削除できます。
[Apple の署名付きアプリケーションを許可する]	Apple 社によって署名されたアプリケーションによるインターネットへのアクセスを自動的に許可できます。
[遮断したアプリケーションがインターネットを使おうとするとときに通知する]	遮断したアプリケーションがインターネットにアクセスを試みるたびに通知するようにノートン製品を設定できます。
[インターネットを使うすべてのアプリケーションをログに記録する]	インターネットにアクセスするアプリケーションを記録できます。 この情報は、[セキュリティ履歴]ウィンドウで表示可能です。
デフォルトに戻す	設定をデフォルトのレベルにリセットできます。

Mac でのアプリケーションのファイアウォールルールの設定

Mac 上で動作するアプリケーションは、インターネットに接続して更新版をダウンロードしたり、プログラムに関する情報を送信します。たとえば、Apple iTunes を開くと、インターネットに接続して最新の iTunes Store 情報が取得されます。アプリケーションを信頼する場合は、アプリケーションのインターネットへの接続を許可できます。

場合によっては、一部のアプリケーションのインターネットアクセスを拒否する必要があります。たとえば、ノートン製品はインターネットに接続しようとするアプリケーションに関する情報を通知します。そのアプリケーションのインターネット接続を遮断して、悪質な情報の送受信を禁止できます。

[アプリケーションの遮断]ウィンドウを使って、アプリケーションのインターネットアクセスを設定できます。[アプリケーションの遮断]ウィンドウの[設定]リストに、選択したアプリケーションが表示されます。選択したアプリケーション名とファイアウォールの設定は、[アプリケーションの遮断]ウィンドウの[設定]リストに表示されます。

アプリケーションのファイアウォールルールの設定

- 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]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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [アプリケーションの遮断]行で、設定アイコンをクリックします。
- 5 [アプリケーションの遮断]ウィンドウで[アプリケーションの追加]を選択します。
選択するアプリケーションがリストに表示されない場合は、[その他]をクリックしてアプリケーションを検索します。
- 6 [アプリケーションの選択]ダイアログボックスで目的のアプリケーションを選択します。
- 7 [選択]をクリックします。
[アプリケーションの遮断]ウィンドウの[設定]リストに、追加したアプリケーションの名前が表示されます。
- 8 [完了]をクリックします。

Mac でのアプリケーションのファイアウォールルールの削除

必要に応じて、[アプリケーションの遮断]ウィンドウを使って、一部のファイアウォールルールを削除できます。

メモ: 詳しい知識のあるユーザー以外はファイアウォールルールを削除しないでください。ファイアウォールルールを削除するとファイアウォールの機能に影響し、Macのセキュリティが低下することがあります。

アプリケーションのファイアウォールルールの削除

- 1 [アプリケーションの遮断]ウィンドウで、アプリケーション名の行を選択します。
- 2 [削除]をクリックします。
- 3 確認ウィンドウで[削除]をクリックします。
- 4 [完了]をクリックします。

Mac 版でのネットワークの検出の設定

ネットワークの検出の設定によって、Mac が接続されているネットワーク上の場所に基づくファイアウォール設定を設定できます。設定されるファイアウォール設定には、Mac で動作するアプリケーションとサービスの接続遮断設定が含まれます。ポータブル Mac を新しいネットワーク上の場所に接続すると、ノートン製品はそのネットワーク上の場所に対する新しいファイアウォール設定の選択を要求します。

[ネットワークの検出] ウィンドウを使って次のことができます。

- ネットワークの検出機能のオンとオフを切り替える。
- Mac が現在接続しているネットワーク上の場所を表示する。

Mac でのネットワークの検出の有効化/無効化

ネットワークの検出機能によって、Mac が接続するネットワークごとに[接続の遮断]設定を設定できます。ノートン製品のインストール時、Mac が接続されているネットワークはデフォルトで[信頼できる]と分類されます。Mac をより弱いか脆弱性のあるネットワークに接続すると、これらのネットワークはノートン製品によって[信頼できない]と分類されます。ただし、ネットワークが安全で信頼できると考えられる場合は、ネットワークカテゴリを[信頼できる]に変更できます。

ネットワークの検出機能は[拡張]ウィンドウから無効または有効にすることができます。

ネットワークの検出の有効化/無効化

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[ファイアウォール]をクリックします。
- 4 [ネットワークの検出]行で、スイッチを[オフ]または[オン]の位置に動かします。

ネットワーク上の場所に対する接続遮断の設定のエクスポート

[エクスポート]ウィンドウを使って、ネットワーク上の場所の設定をエクスポートできます。ノートン製品のメニューバーのファイルメニューにある[エクスポート]オプションを使用できます。ノートン製品はネットワークの場所の設定を .npfx ファイル形式でエクスポートします。

次のオプションを使ってネットワーク上の場所の設定をエクスポートできます。

[すべての設定をエクスポート]

選択したネットワーク上の場所のすべての設定をエクスポートできます。

[これらの設定のみをエクスポートする]

選択したネットワーク上の場所の設定のうち、必要なもののみをエクスポートできます。次のオプションがあります。

- [アプリケーションの遮断]
- [接続の遮断]
- [アプリケーション]
- [サービスとポート]
- [ゾーン]
- 脆弱性保護
- ノートン ディープサイト™コミュニティのダウンロード

[エクスポート設定をパスワード保護する]

パスワードを追加することで、エクスポートしたファイルを保護できます。

メモ: [エクスポート設定をパスワード保護する]チェックボックスを使って、エクスポートされるネットワーク上の場所の設定を保護できます。

保存した設定を後でインポートし、確認したり、ノートン製品がインストールされている別のコンピュータに適用したりできます。

ネットワーク上の場所に対する接続遮断の設定のエクスポート

- 1 ノートン クイックメニューで、[ノートン セキュリティを開く]をクリックします。
- 2 ノートン製品のメニューバーのファイルメニューで[エクスポート]を選択します。
- 3 [エクスポート]ウィンドウで、エクスポートオプションを選択します。
- 4 [エクスポート]をクリックします。

Mac でゲームをしたり映画を鑑賞するときのバックグラウンドタスクの停止

全画面モードで重要なタスクを実行したり映画を見たりゲームをしたりする場合に、警告メッセージの送信を停止したり、パフォーマンスを低下させるバックグラウンドタスクを中断するようにノートンを設定できます。サイレントモードをオンにするだけでこのように設定されます。

[サイレントモード]のオンとオフの切り替え

- 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[詳細設定]または[設定]をクリックします。

- 3 左ペインで[製品の設定]をクリックします。
- 4 [サイレントモード]行で、スイッチを[オフ]または[オン]の位置に動かします。

追加の解決策の検索

この章では以下の項目について説明しています。

- [ウイルスの名前と定義の確認](#)
- [Mac 版のプロダクトキーまたは PIN の入手](#)
- [Mac ユーザーアカウントの種類の確認](#)
- [Mac 上のノートンのアンインストール](#)

ウイルスの名前と定義の確認

[ウイルス定義]ウィンドウには、ウイルスの名前とその定義が表示されます。**Mac**が特定のウイルスから保護されているかを確認するには、ウイルスの名前を検索します。デフォルトでは、ノートンは定期的にウイルス定義を自動更新します。

各ウイルスを選択して[影響] (i) アイコンをクリックすると、**Mac**が感染したときにどの程度深刻な影響を受けるか表示できます。[詳細情報]をクリックすると、概略を読むことができます。各ウイルスの概略は別々の **Web** ページに表示されます。

ウイルスの名前と定義の確認

- 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[詳細設定]または[設定]をクリックします。
- 3 左ペインで[**Mac**を保護する]をクリックします。
- 4 [ウイルス定義]行で、設定アイコンをクリックします。
- 5 [ウイルス定義]ウィンドウの検索フィールドにウイルスの名前または名前の一部を入力します。ノートン製品に、関連するすべてのウイルスが表示されます。詳しい情報を表示したいウイルスをクリックします。
- 6 [完了]をクリックします。

詳しい情報

- ◆ ■ p.23 の「[Mac 版でのノートン自動スキャンの設定変更](#)」を参照してください。

Mac 版のプロダクトキーまたは PIN の入手

ここでは、ノートン製品のアクティブ化や延長に必要なプロダクトキーまたは PIN の確認方法について説明します。

- プロダクトキー: 英数字を組み合わせた 25 文字の文字列で、5 文字ずつハイフンで 5 つに区切られています。ノートン製品のライセンスをアクティブ化または延長する場合に必要です。

登録した電子メールアドレスにサービスプロバイダから PIN が届いている可能性があります。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。それでも PIN が見つからない場合は、サービスプロバイダにお問い合わせください。

- 製品がプリインストールされていた場合、プロダクトキーは製品にすでに格納されている可能性があります。必要なのは、ノートン アカウントに製品を登録することのみです。登録したら、アカウントにサインインしてプロダクトキーを入手できます。製造元によっては、同梱のアクティブ化カードにプロダクトキーが記載されている場合もあります。問題がある場合は、デバイスの製造元にお問い合わせください。
- ノートン製品をサードパーティ Web サイトで購入した場合には、プロダクトキーは注文確認メールに記載されています。その電子メールが受信ボックスで見つからない場合は、迷惑メールフォルダを調べます。
- プロダクトキーカードを受け取っている場合には、プロダクトキーとその使い方がカードに印刷されています。
- 販売店でノートンのカードを購入した場合、プロダクトキーはノートンのカードの裏側に印刷されています。

Mac ユーザーアカウントの種類の確認

ユーザーアカウントはユーザーが Mac で実行できる処理を定義します。Mac では次の種類のユーザーアカウントを作成できます。

- 管理者アカウント
- 標準アカウント
- 制限付きアカウント

各アカウントの権限は異なります。管理者アカウントでは、Mac のすべての領域へのアクセス、ソフトウェアのインストールと更新、別のユーザーアカウントの作成と保守が可能です。

自分のユーザーアカウントの種類がわからない場合には[システム環境設定]で確認できます。

Mac ユーザーアカウントの種類の確認

- 1 [Apple]メニューで[システム環境設定]をクリックします。
- 2 [ユーザーとグループ]をクリックします。
- 3 [ユーザーとグループ]ウィンドウの左側にアカウント名とアカウントの種類が表示されます。

Mac 上のノートンのアンインストール

ノートンをアンインストールするには、管理者アカウントのユーザー名とパスワードが必要です。

ノートンのアンインストール後に、Mac を再起動する必要があります。

メモ: 継続的な保護を確実に行うため、ノートンを Mac にインストールしたままにすることを推奨します。

macOS 10.14.x (Mojave) 以前でのノートンのアンインストール

- 1 Mac メニューバーで[ノートン]アイコンをクリックし、[ノートンを開く]をクリックします。
- 2 ノートンのメニューで、[ノートン] > [ノートンのアンインストール]を選択します。
- 3 表示されるウィンドウで[アンインストール]をクリックします。
- 4 プロンプトが表示されたら、管理者アカウントパスワードを入力します。
- 5 [今すぐ再起動]をクリックします。

ノートン アプリケーションを[アプリケーション]フォルダから[ゴミ箱]にドラッグアンドドロップしても、ノートンをアンインストールできます。

macOS 10.15.x (Catalina) 以降でのノートンのアンインストール

メモ: ノートン アプリケーションを開いている場合は、以下の手順を実行する前に閉じてください。

- 1 Mac で[アプリケーション]フォルダを開き、ノートン アプリケーションのアイコンを[ゴミ箱]にドラッグアンドドロップします。
- 2 [続行]をクリックします。
- 3 プロンプトが表示されたら、管理者アカウントパスワードを入力して、[OK]をクリックします。
- 4 表示されるウィンドウで[アンインストール]をクリックします。
- 5 プロンプトが表示されたら、管理者アカウントパスワードを入力して、[インストールヘルパー]をクリックします。
- 6 [今すぐ再起動]をクリックします。