中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（Microsoft Defender）

Ver1.0（2023.07）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに 3
2 チェックリスト項目に対応する設定作業一覧 4
3 管理者向け設定作業 5
3-1 チェックリスト 2-1 への対応 5
3-1-1 リアルタイム保護と定義ファイルの自動更新 5
4 利用者向け設定作業 8
4-1 チェックリスト 2-1 への対応 8
4-1-1 リアルタイム保護と定義ファイルの自動更新 8

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、Microsoft Defender を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

(イ) 前提条件

本製品は、Windows 10 に搭載されている標準ソフトウェアのため、インストール不要で無償で使用することができます。（2022 年 11 月 1 日現在）

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、第 4 章では利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であるとを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2022 年 11 月 1 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目管理者向け作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
2-1 マルウェア対策 **テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか、手動で更新するルールを作成する。**	・リアルタイム保護と定義ファイルの自動更新	P.5

表 3. チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
2-1 マルウェア対策 **テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか、手動で更新するルールを作成する。**	・リアルタイム保護と定義ファイルの自動更新	P.8

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1　チェックリスト 2-1 への対応

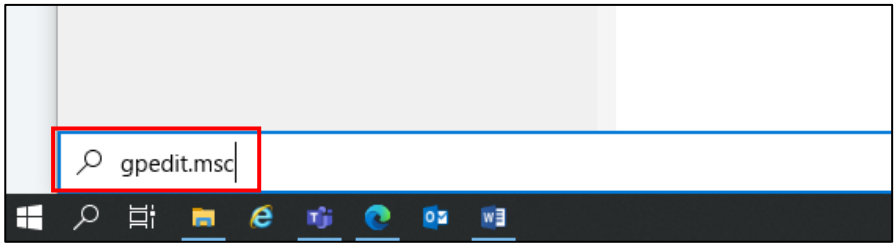
3-1-1　リアルタイム保護と定義ファイルの自動更新

リアルタイムでの保護を有効にすることで、テレワーク端末がマルウェアに感染した場合に即座に検知、防御することができます。Windows では、リアルタイム保護がデフォルトで有効になっていますので、設定は不要です。
また、Windows Update の機能の一部として、利用端末に最新の定義ファイルが、自動でダウンロードされるようになっています。定義ファイルの更新チェック間隔を任意の値に設定したい場合は、ポリシーの設定で更新チェック間隔を指定することもできます。

（参考）定義ファイルの更新チェック間隔の設定

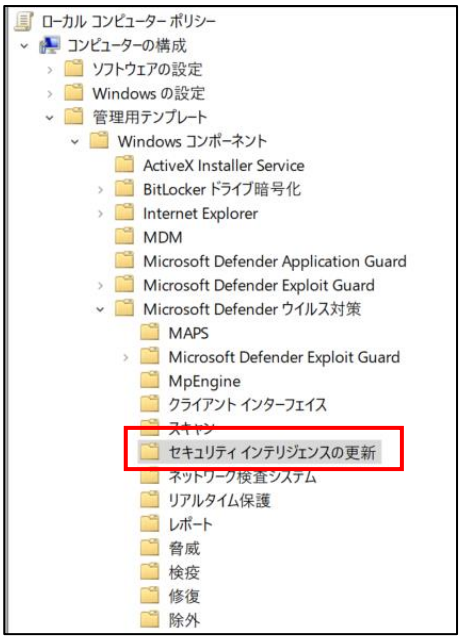
以下の手順は、AD（Active Directory）ドメイン環境ではない場合に、リモート接続先となる端末 1 台ずつに設定する場合の手順です。
AD ドメイン環境の場合は、AD サーバーで管理されている対象端末に対し、設定を一括で適用することができます。
そのため、AD ドメイン環境の場合は、AD サーバーで以下に記載するポリシーを有効にしたグループポリシーオブジェクト（GPO）を作成することを推奨します。AD ドメイン環境下でのグループポリシーの作成については、AD ドメイン環境構築した担当者にご確認ください。

【手順①】
スタートメニュー右側の検索ボックスに「gpedit.msc」と入力し、Enter キーを押下します。



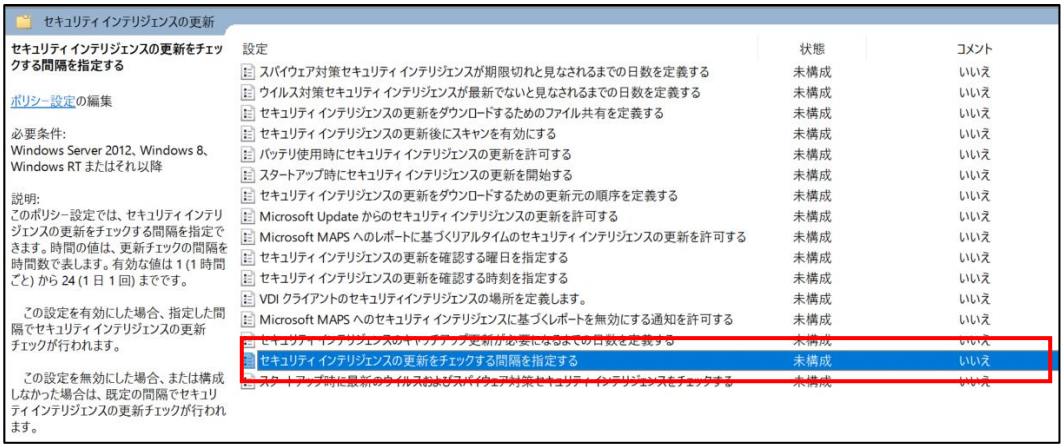
【手順②】

「ローカルグループポリシーエディター」が開いたら、左ペインで「ローカル コンピュータ ポリシー」-「コンピュータの構成」-「管理用テンプレート」-「Windows コンポーネント」-「Microsoft Defender ウイルス対策」-「セキュリティインテリジェンスの更新」を順に選択します。



【手順③】

「セキュリティインテリジェンスの更新をチェックする間隔を指定する」を開きます。



【手順④】

「有効」にチェックを入れ、更新をチェックする間隔を指定し、「OK」をクリックします。

「セキュリティインテリジェンスの更新をチェックする感覚を指定する」には、1 時間ごと（値： 1 ）から 1 日 1 回（値：24）の範囲の値を指定できます。以下は、3 時間ごとに指定した場合です。

参考情報：保護の更新をダウンロードして適用するスケジュールの管理 – グループ ポリシーを使用して保護の更新をスケジュールする

URL：https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/manage-protection-update-schedule-microsoft-defender-antivirus#use-group-policy-to-schedule-protection-updates

スケジュールスキャンを設定したい場合は、下記情報をご参照ください。

参照情報：スケジュールされたクイック スキャンまたは完全な Microsoft Defender ウイルス対策スキャンを構成する

URL：https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/scheduled-catch-up-scans-microsoft-defender-antivirus

４利用者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

４-１　チェックリスト 2-1 への対応

４-１-１　リアルタイム保護と定義ファイルの自動更新

リアルタイムでの保護を有効にすることで、**テレワーク端末がマルウェアに感染した場合に即座に検知、防御することができます。**Windows では、リアルタイム保護はデフォルトで有効になっており、定期的に自動でスキャンも実行されます。
また Windows Update の機能の一部として、利用端末に最新の定義ファイルが自動でダウンロードされるようになっています。そのため、基本的には手動スキャンや手動アップデートは不要ですが、手動で実施する場合は、下記を参考にして実施してください。

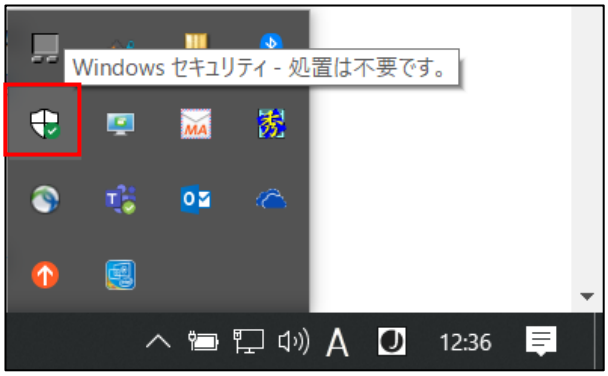
リアルタイム保護に関しては、「（参考）ウイルスと脅威の防止の設定」を参考に設定を確認することが出来ます。

（参考）スキャンの手動実行

【手順①】

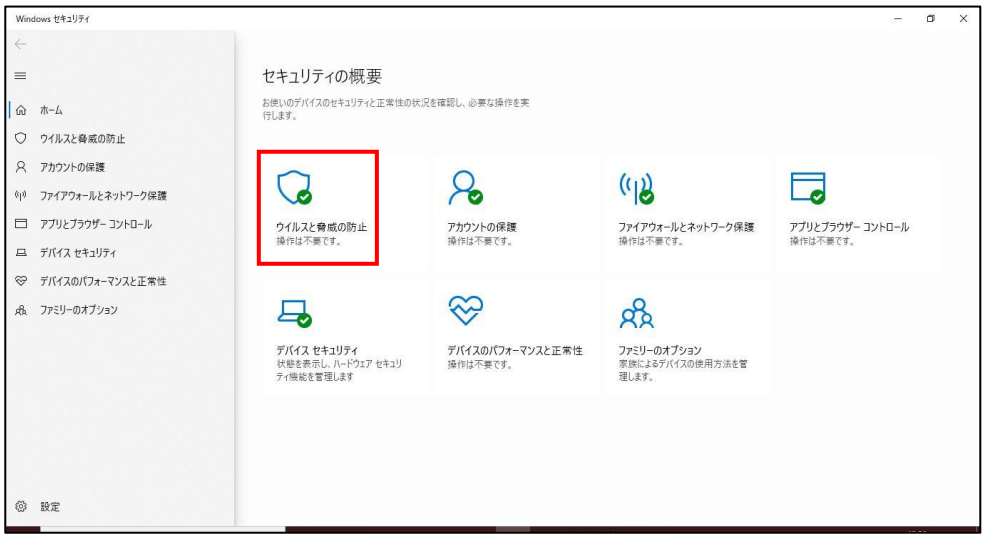
- 「スタート」-メニューから「Windows セキュリティ」をクリックします。

※　もしくはタスクバーの通知領域の「Windows セキュリティ」アイコンをクリックします。



【手順②】

「Windows セキュリティ」画面が開くので、「ウイルスと脅威の防止」をクリックします。



【手順③】

「現在の脅威」欄の「クイックスキャン」をクリックします。

クリック後、クイックスキャンが実行されます。

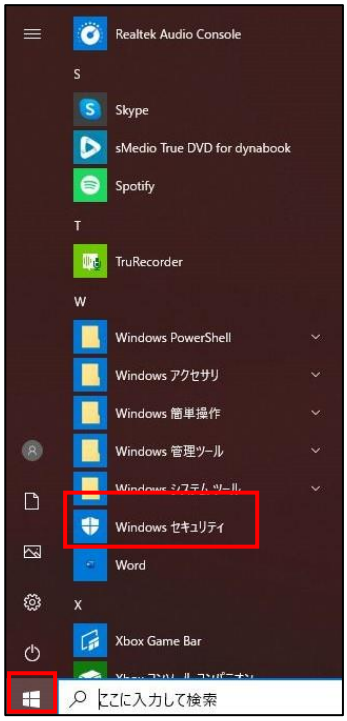
「現在の脅威」欄の「スキャンのオプション」からクイックスキャン以外に下記方法でスキャンすることもできます。
各スキャンの内容は以下の通りです。

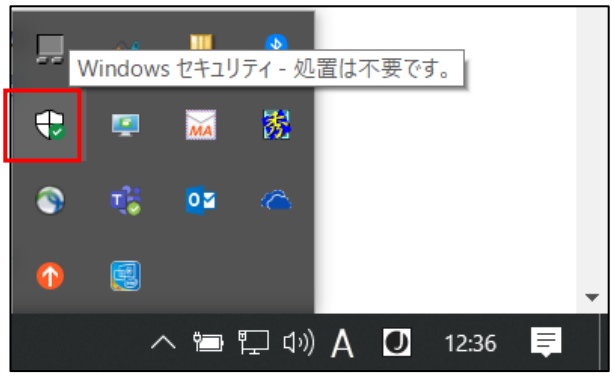
- 「フルスキャン」：ハードディスク上の全ファイルおよび実行中の全プログラムをスキャンします。
- 「カスタムスキャン」：チェックするファイルと場所を選択してスキャンします。
- 「Windows Defender オフラインスキャン」：通常のスキャンでは見つからない悪意のあるソフトウェアを検出して削除できる可能性があります。

（参考）定義ファイルの手動更新

【手順①】

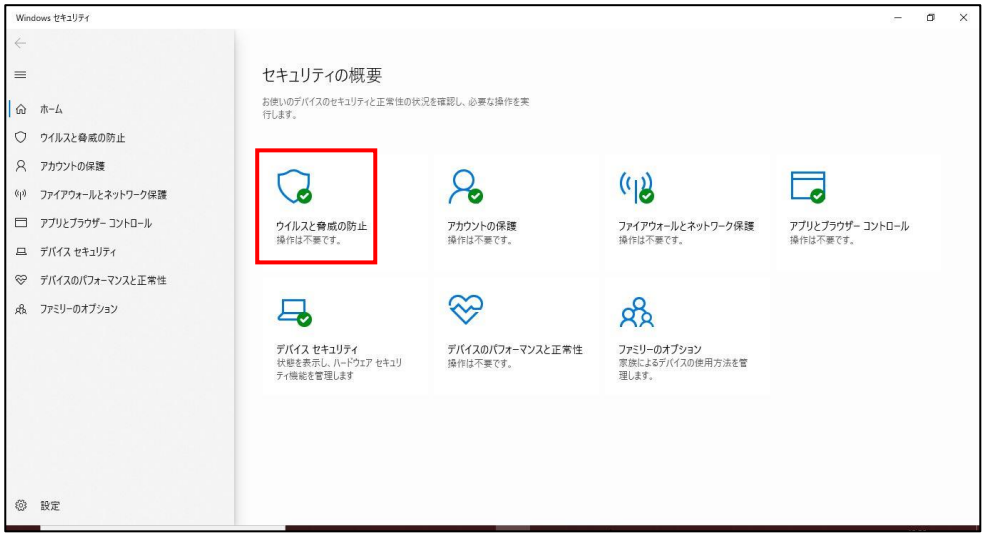
「スタート」-メニューから「Windows セキュリティ」をクリックします。もしくはタスクバーの通知領域の「Windows セキュリティ」アイコンをクリックします。





【手順②】

「Windows セキュリティ」画面が開くので、「ウイルスと脅異の防止」をクリックします。



【手順③】

「ウイルスと脅威の防止の更新」欄の「更新プログラムのチェック」をクリックします。

【手順④】

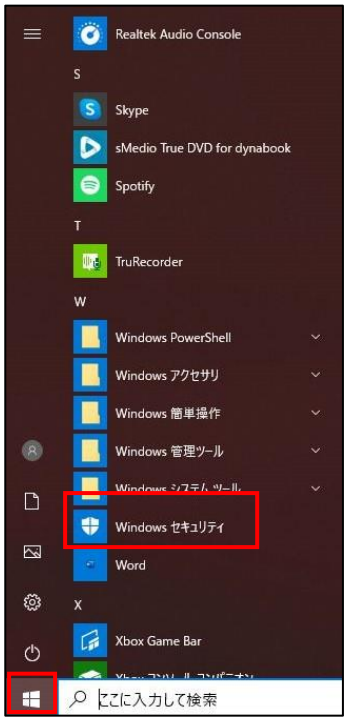
「更新プログラムのチェック」をクリックすると、定義ファイルの更新が確認され、更新がある場合は自動で適用されます。

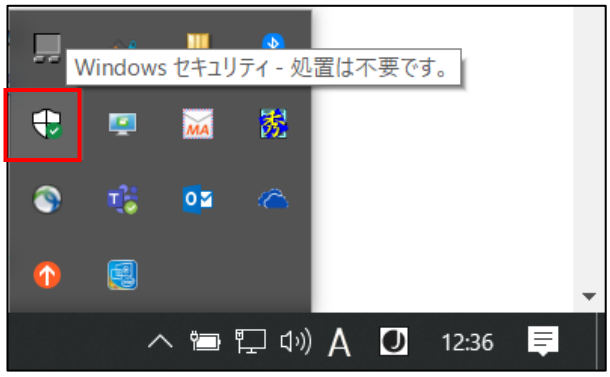
（参考）現在の脅威の確認手順

以下の手順を実施することで、マルウェア感染の有無などを確認することができます。

【手順①】

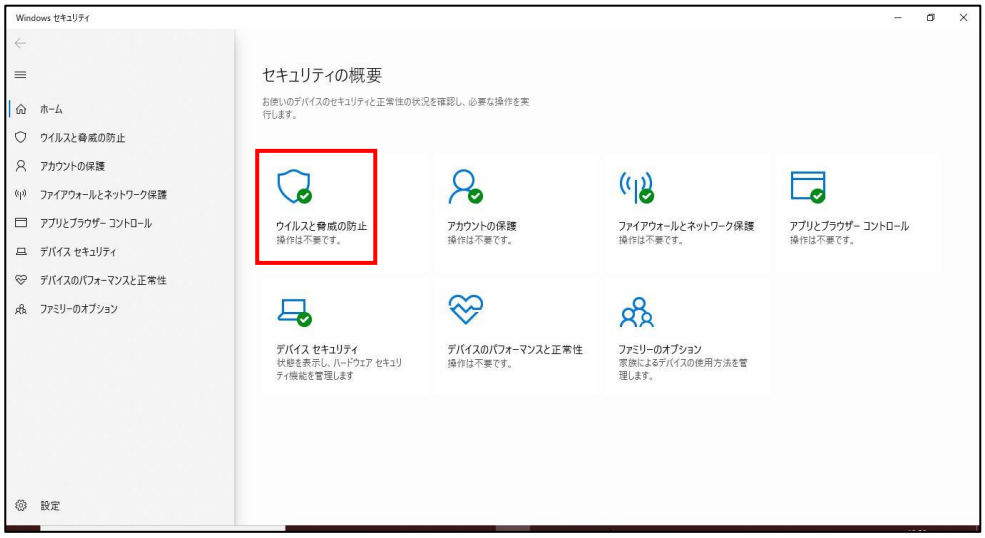
「スタート」-メニューから「Windows セキュリティ」をクリックします。もしくはタスクバーの通知領域の「Windows セキュリティ」アイコンをクリックします。





【手順②】

「Windows セキュリティ」画面が開くので、「ウイルスと驚異の防止」をクリックします。



【手順③】

「ウイルスと脅威の防止」画面の「現在の脅威」欄を確認します。

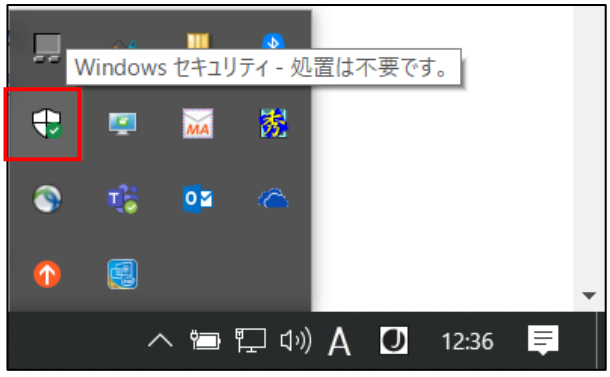
「現在の脅威はありません。」と表示されていれば、マルウェアは検出されなかったか、既に対処が行われています。

「現在の脅威」欄から「保護の履歴」をクリックすると、脅威や推奨事項がある場合は、その内容が表示されます。脅威や推奨事項がない場合は、「最近の操作はありません」と表示されます。

（参考）ウイルスと脅威の防止の設定

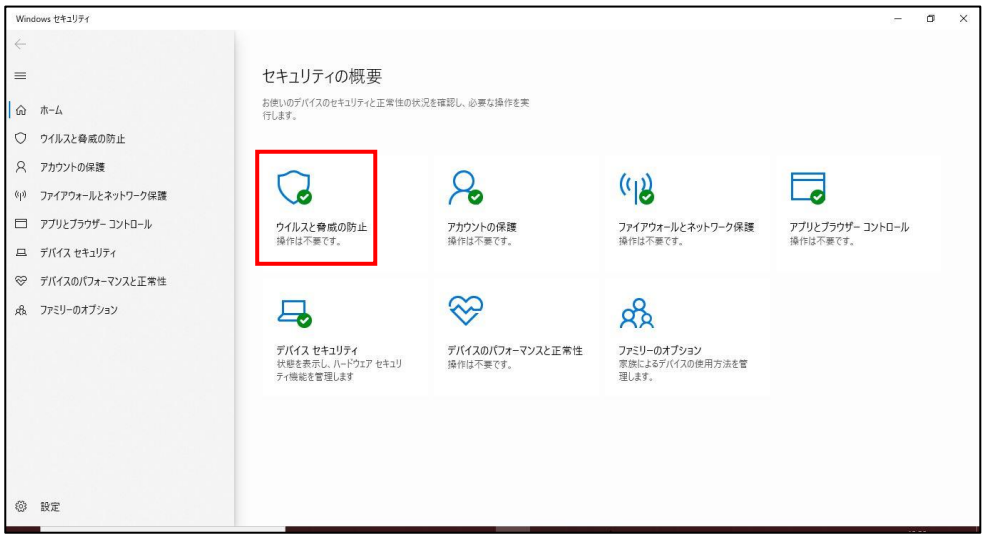
【手順①】

「スタート」-メニューから「Windows セキュリティ」をクリックします。もしくはタスクバーの通知領域の「Windows セキュリティ」アイコンをクリックします。



【手順②】

「Windows セキュリティ」画面が開くので、「ウイルスと驚異の防止」をクリックします。



【手順③】

「ウイルスと脅威の防止の設定」欄の「設定の管理」をクリックします。

【手順④】

下記の 4 項目が「オン」になっていることを確認します。「オフ」になっている項目があれば、「オン」に設定します。

- リアルタイム保護
- クラウド提供の保護
- サンプルの自動送信
- 改ざん防止