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
（Windows）

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

(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、Windows OS 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

利用するエディションやバージョンにより使用可能な機能が異なります。本資料では **Window 10 Pro（バージョン 1909）の利用を前提**としております。

(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と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
1-1　資産・構成管理 **テレワークには許可した端末のみを利用するよう周知し、テレワーク端末とその利用者を把握する。**	・端末と利用者の把握	P.6
7-2　インシデント対応・ログ管理 **テレワーク端末と接続先の各システムの時刻を同期させる。**	・時刻同期設定	P.7
9-1　アカウント・認証管理 **テレワーク端末のログインアカウントや、テレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また、可能な限りパスワード強度の設定を強制する。**	・ログインパスワードポリシー設定	P.11
9-3　アカウント・認証管理 **テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合、それ以上のパスワード入力を受け付けないよう設定する。**	・アカウントロックアウト設定	P.14

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
2-2 マルウェア対策 **不審なメールを開封し、メールに記載されている URL をクリックしたり、添付ファイルを開いたりしないよう周知する。**	・Microsoft Defender SmartScreen の設定 ・ファイル拡張子の表示設定	P.16 P.18
4-1 物理セキュリティ **テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。**	・第三者からの盗聴・のぞき見の対策	P.19
5-1 脆弱性管理 **テレワーク端末にはメーカーサポートが終了した OS やアプリケーションを利用しないよう周知する。**	・メーカーサポートの確認	P.21
5-2 脆弱性管理 **テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。**	・OS 及びアプリケーションの最新化	P.25
6-1 通信暗号化 **Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特に ID・パスワード等の入力を求められる場合）は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。**	・サービスへの接続確認	P.30
6-2 通信暗号化 **無線 LAN ルーターを利用する場合は、セキュリティ方式として「WPA2」又は「WPA3」を利用し、無線の暗号化パスワードは第三者に推測されにくいものにする。**	・無線 LAN のセキュリティ方式の確認	P.31
8-1 データ保護 **スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。**	・端末位置の把握	P.32
8-3 データ保護 **テレワーク端末の盗難・紛失時に情報が漏えいしないよう、端末に内蔵されたハードディスクやフラッシュメモリ等の記録媒体の暗号化を実施する。ただし、端末に会社のデータを保管しない場合を除く。**	・BitLocker による暗号化設定	P.38
9-2 アカウント・認証管理 **テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。**	・初期パスワード設定変更	P.43

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 1-1 への対応

3-1-1　端末と利用者の把握

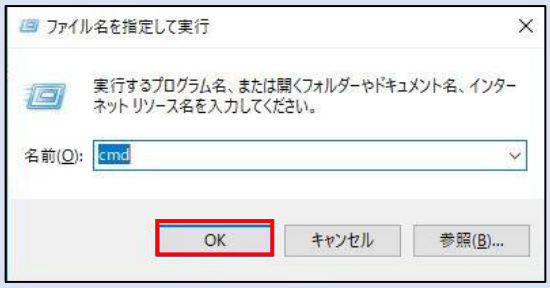
テレワーク用に従業員へ貸与する端末のシリアル番号を確認します。管理者は、利用者が使用している端末とその設置場所をあらかじめ把握し、**定期的な棚卸によって紛失を検知できるようにすることが重要です。**ここでは端末を識別するシリアル番号の確認手順を記載します。

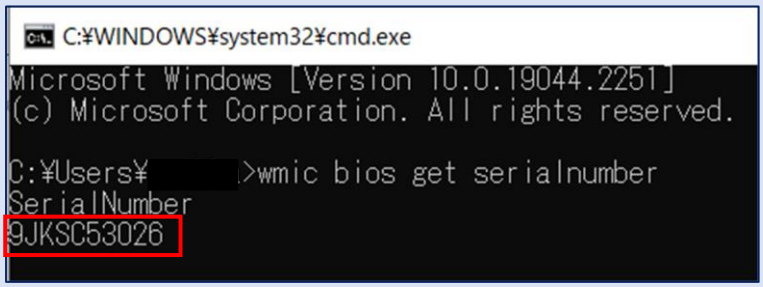
端末のシリアル番号の確認

利用者に貸与するテレワーク端末のシリアル番号を確認します。

【手順①】
テレワーク端末背面に記載のシリアル番号（製造番号）を確認します。

参考　テレワーク端末背面のシリアル番号が見つけられない場合
【手順①】「Windows+」+「R」キーを押し、「cmd」と入力後、「OK」を押下でコマンドプロンプトを開きます
【手順②】「wmic bios get serialnumber」を実行して出力された番号を確認します





3-2　チェックリスト 7-2 への対応

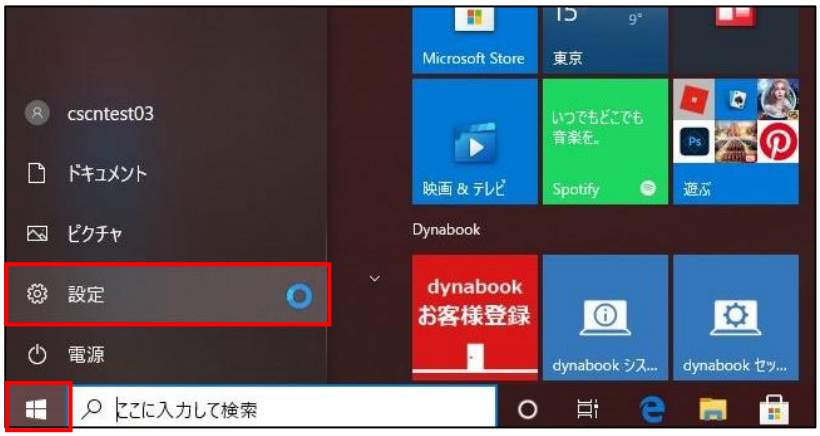
3-2-1　　時刻同期設定

端末とアクセス先の各システムの時刻を同一のものにするため、端末の時刻同期設定を行います。各機器の時刻を一致させることで、**インシデント発生時のアクセスログ等の調査の際に、正確な調査を行う**ことができます。
以下に Windows 標準の時刻同期サーバーとの同期設定と指定の時刻同期サーバーとの時刻同期設定の手順を記載します。

標準時刻同期サーバーとの時刻同期設定

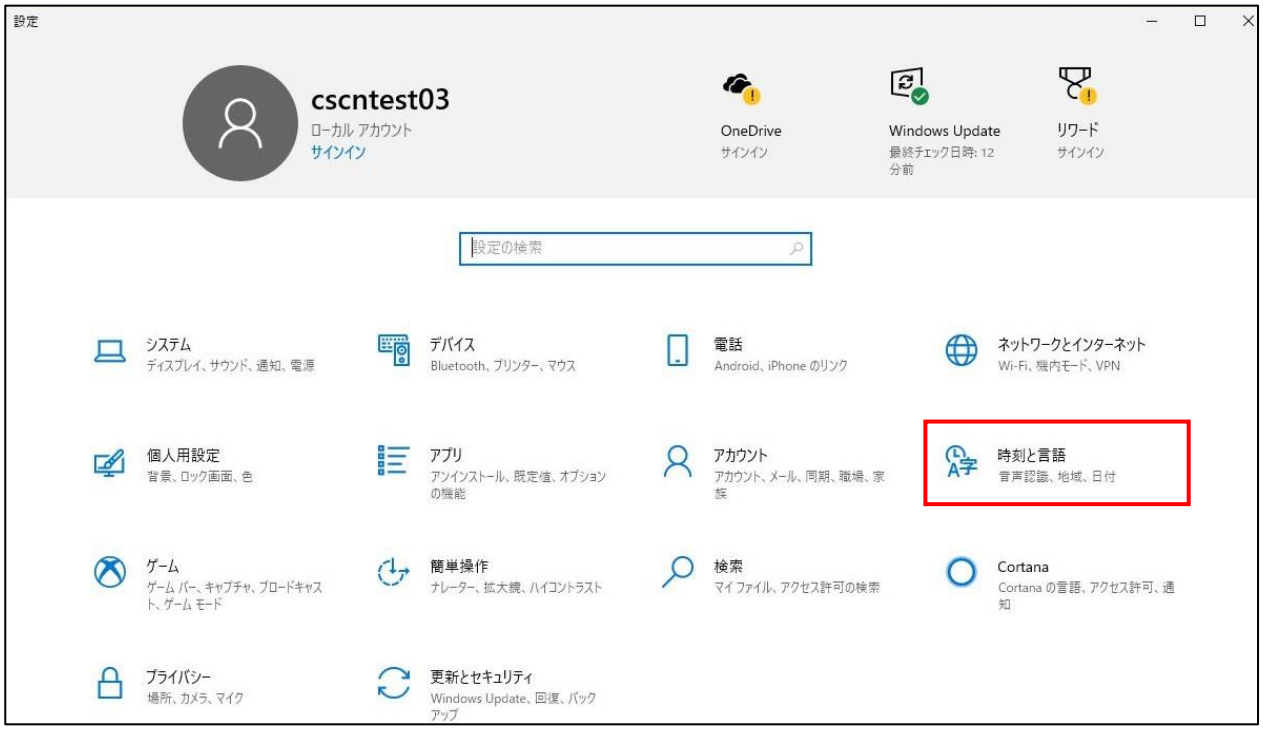
【手順①】

Windows 画面左下のスタートをクリック後、「設定」をクリックします。



【手順②】

下図の画面に遷移後、「時刻と言語」をクリックします。



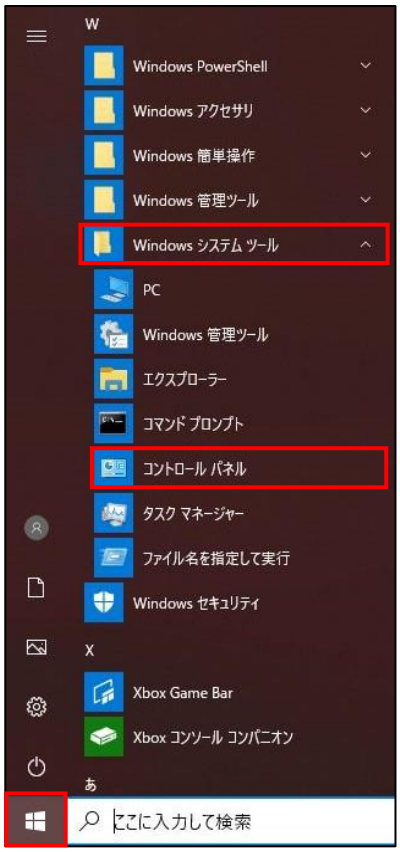
【手順③】

「日付と時刻」を選択後、右ペインにある「時刻を自動的に設定する」をオンにします。

時刻同期サーバーを指定した時刻同期設定

【手順①】

Windows 画面左下のスタートをクリック後、「Windows システムツール」から「コントロールパネル」をクリックします。



【手順②】

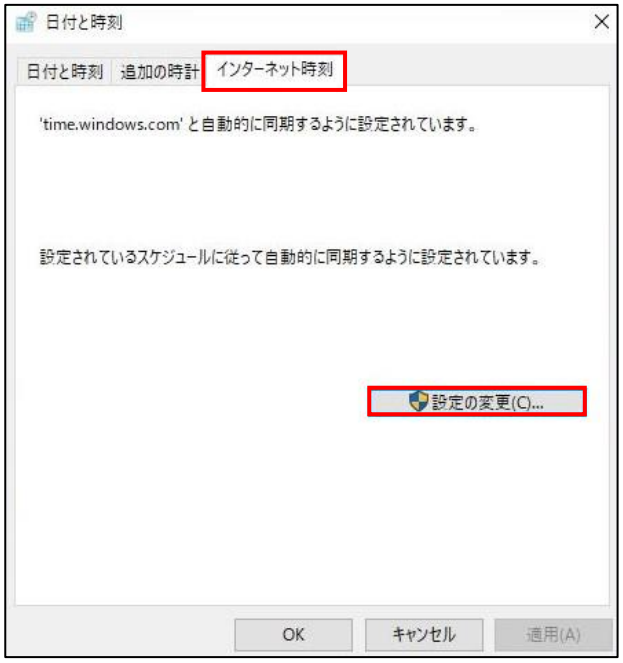
下図の画面に遷移後、「時刻と地域」をクリックします。画像のような画面に進まない場合は「表示方法」をカテゴリに変更してください。

【手順③】

右ペインにある「日付と時刻」をクリックします。

【手順④】

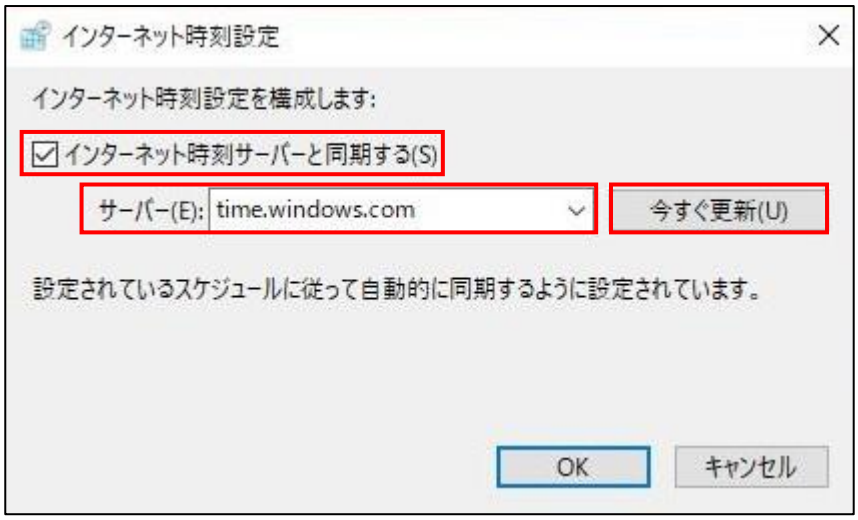
「インターネット時刻」タブに移動し、「設定の変更」をクリックします。



【手順⑤】

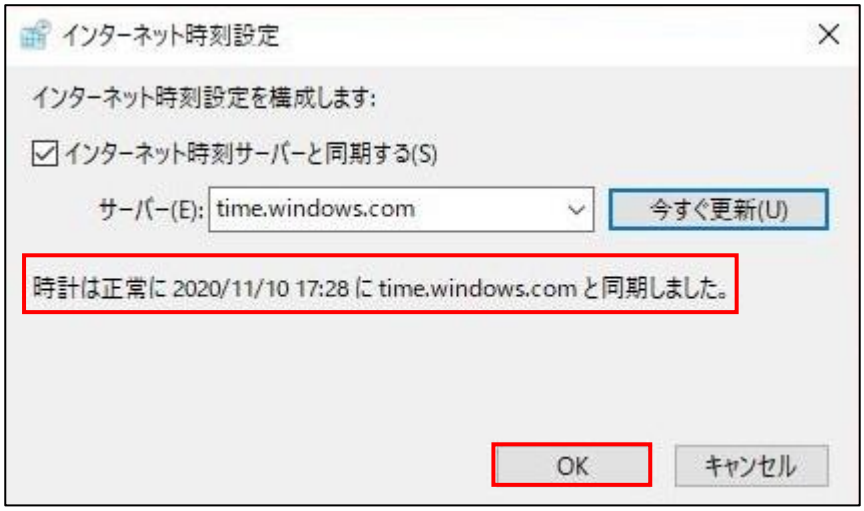
「インターネット時刻サーバーと同期する」にチェックを入れ、「サーバー」に社内の時刻同期サーバー（NTP サーバー）（※）などを入力し「今すぐ更新」をクリックします。

※　下図は便宜的に Windows 標準の時刻同期サーバーを「サーバー」に入力したものです。



【手順⑥】

画面に「時計は正常に YYYY/MM/DD HH:mm（左記は現在の時刻）に{サーバー名}と同期しました。」の表示後、「OK」をクリックします。



3-3　チェックリスト 9-1 への対応

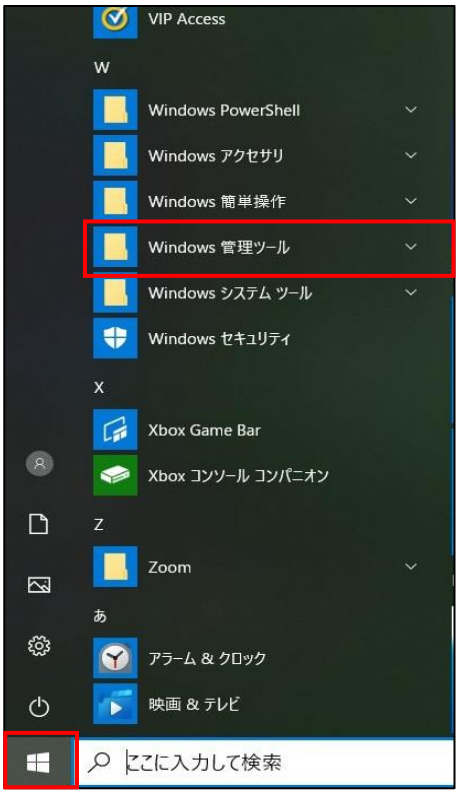
3-3-1　　ログインパスワードポリシー設定

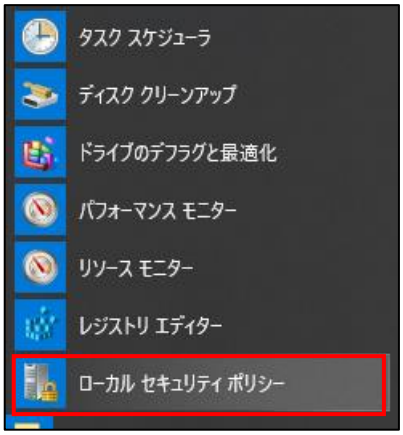
管理者はパスワードポリシーを設定することにより、強度の高いパスワード設定をユーザーに要求できます。**これにより、強度の低いパスワードが使用されるリスクを低減することができます。**

本手順は、外部認証ツールを使用していない場合のパスワードポリシーの設定手順です。Active Directory 等の外部認証ツールを利用している場合は、使用しているツールの設定方法をご参照ください。

【手順①】

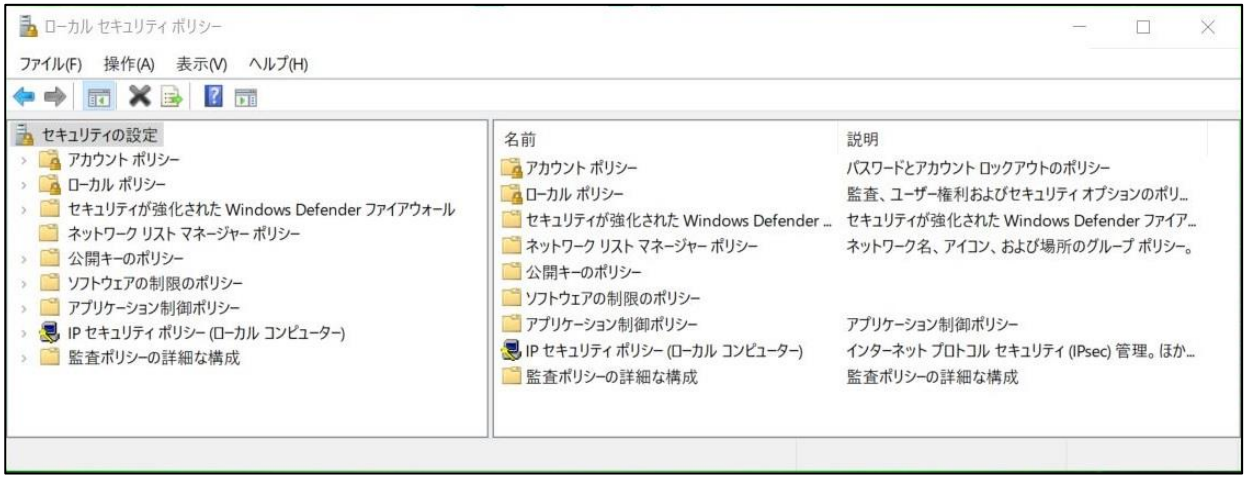
画面左下の Windows スタートメニューをクリックし、「Windows 管理ツール」から「ローカルセキュリティポリシー」をクリックします。





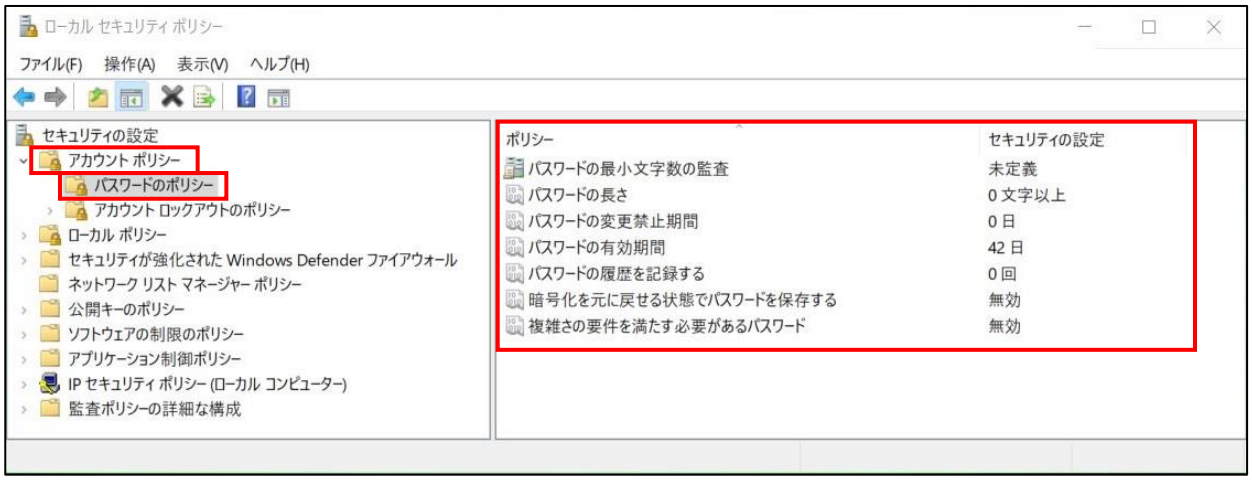
【手順②】

「ローカルセキュリティポリシー」をクリックすると Windows のセキュリティ設定を行えるローカルセキュリティポリシー画面が表示されます。



【手順③】

左ペインにある「アカウントポリシー」をダブルクリックし、「パスワードのポリシー」を選択すると、パスワードに関するポリシー設定画面が表示されます。



【手順④】

パスワードのポリシーは各項目をダブルクリックすることで設定を行います。以下に例として、パスワードの長さと複雑性に焦点を当てた項目の設定方法を記載します。

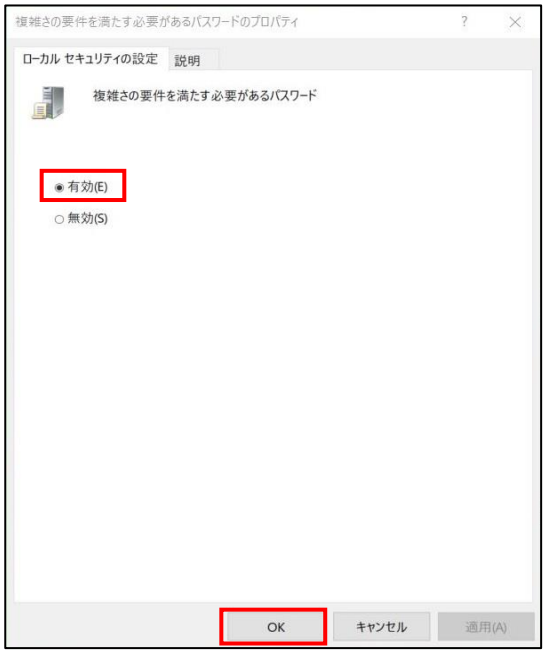
- パスワードの長さ

ユーザーアカウントのパスワードに使用できる最小文字数を決定できます。設定後、「OK」をクリックします。

- パスワードの複雑さ

「有効化」を選択し、「OK」ボタンをクリックします。この設定を有効にすることで Windows の既定ポリシーとして次の 4 種類のうち 3 種類を組み合わせてパスワードを設定することを強制できます。

- 英大文字（A から Z）
- 英子文字（a から z）
- 10 進数の数字（0 から 9）
- アルファベット以外の文字（!、$、#、%など）



3-4　チェックリスト 9-3 への対応

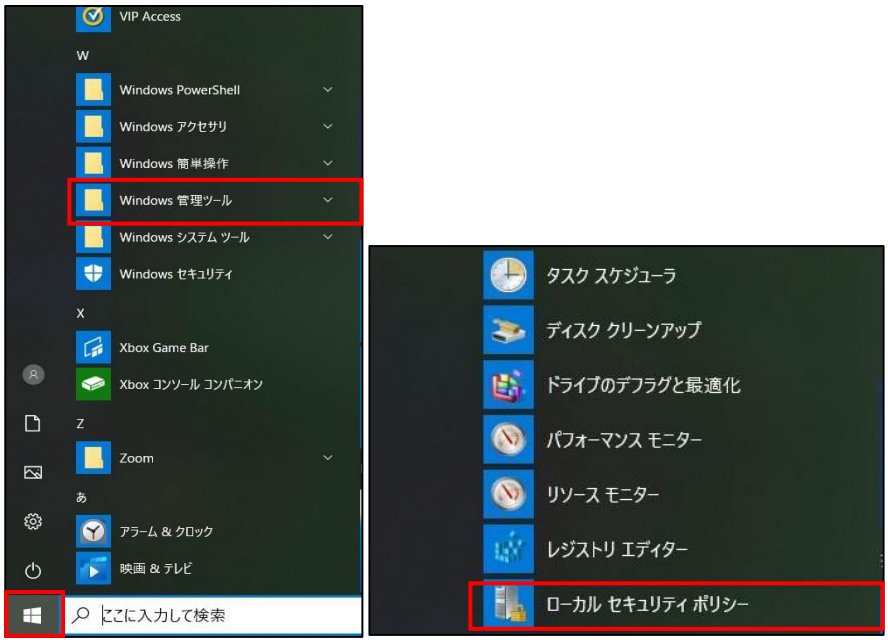
3-4-1　　アカウントロックアウト設定

パスワード入力を一定回数以上間違えるとパスワードを入力できない状態にする、ロックアウト設定を行います。ロックアウト設定を行うことで、**悪意のある第三者にパスワード解除されるリスクを低減**することができます。

以下の手順は、外部認証ツールを使用していない場合のパスワードポリシー設定手順です。Active Directory 等の外部認証ツールを利用している場合は、使用しているツールの設設定方法をご参照ください。

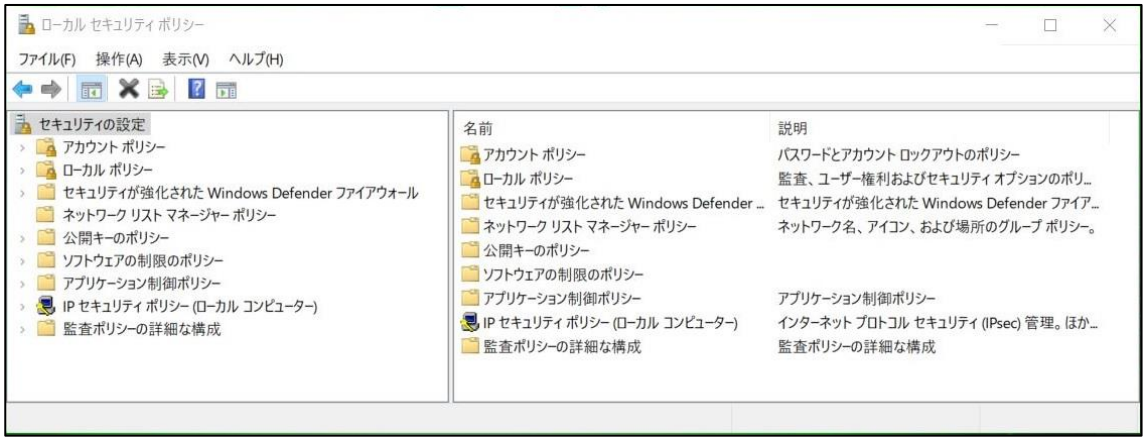
【手順①】

画面左下の Windows スタートメニューをクリックし、「Windows　管理ツール」から「ローカルセキュリティポリシー」をクリックします。



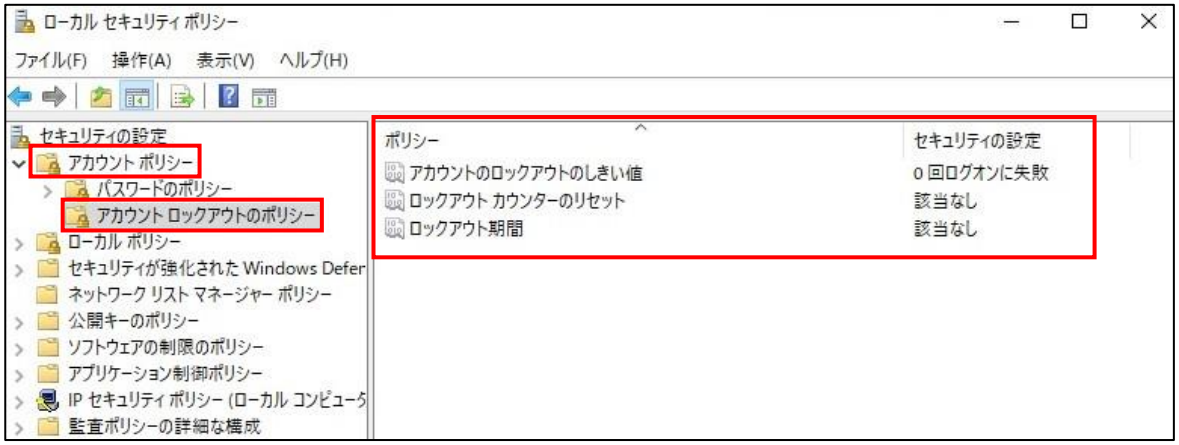
【手順②】

「ローカルセキュリティポリシー」をクリックすると、Windows のセキュリティ設定を行えるローカルセキュリティポリシー画面が表示されます。



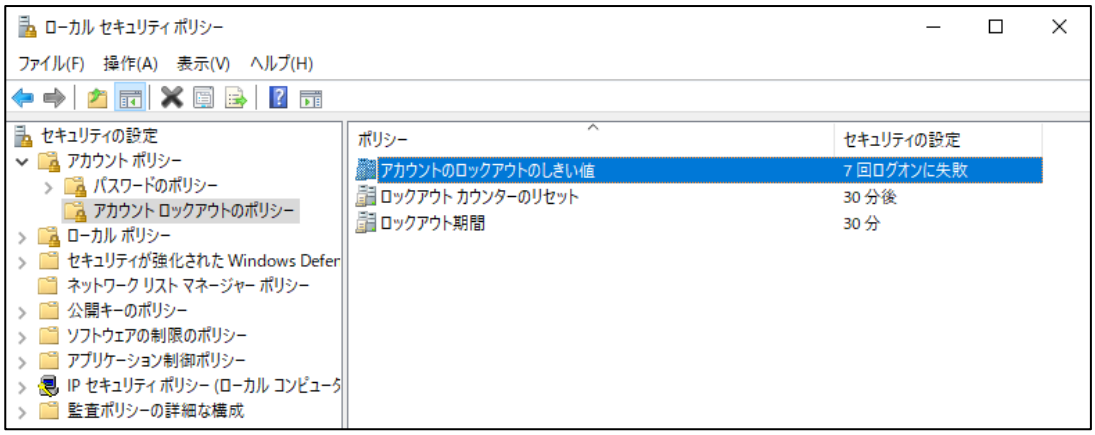
【手順③】

左ペインにある「アカウントポリシー」をダブルクリックし、「アカウントロックアウトのポリシー」を選択するとアカウントロックアウトに関するポリシーの設定画面が表示されます。



【手順④】

アカウントのロックアウトしきい値やロックアウト期間を設定します。以下は、「アカウントのロックのしきい値」を 7 回、「ロックアウトカウンターのリセット」を 30 分、「ロックアウト期間」を 30 分にした場合です。



４利用者向け作業

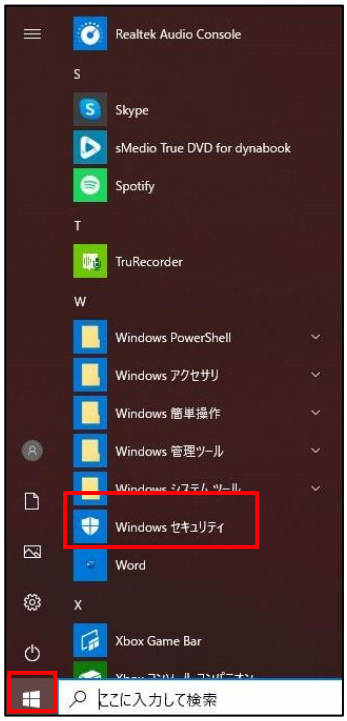
ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

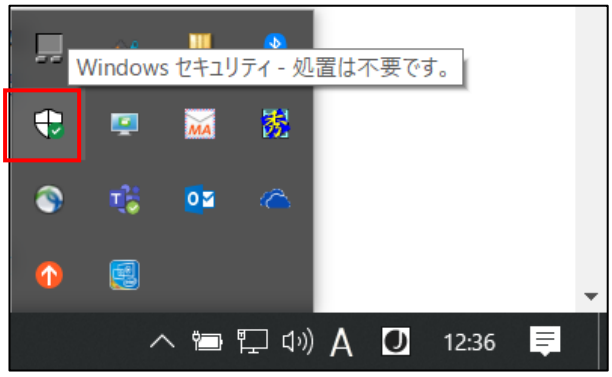
４-１　チェックリスト 2-2 への対応

４-１-１　Microsoft Defender SmartScreen の設定

Microsoft Defender SmartScreen を有効にしておくことで、フィッシングやマルウェアの疑いのある Web サイトやアプリケーションから保護し、悪意がある可能性の高いファイルのダウンロードを防ぐことができます。
デフォルトでは有効になっています。無効（オフ）となっている場合は有効にしてください。

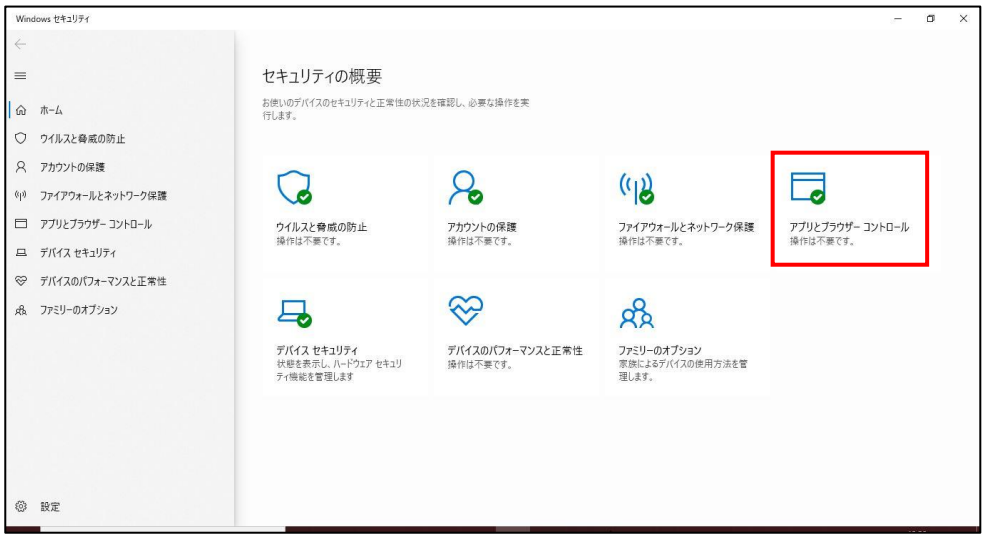
【手順①】
スタートメニューから「Windows セキュリティ」をクリックします。もしくはタスクバーの通知領域の「Windows セキュリティ」アイコンをクリックします。





【手順②】

「Windows セキュリティ」画面から、「アプリとブラウザーコントロール」をクリックします。



【手順③】

デフォルトでは「アプリとファイルの確認」が「警告」、「Microsoft Edge の SmartScreen」が「オン」、「Microsoft Store アプリの SmartScreen」が「警告」と設定されています。**「オフ」になっている項目がある場合**は、各項目の設定を有効（「警告」や「オン」）にしてください。

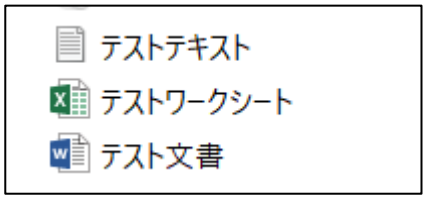
【参考】Microsoft Defender SmartScreen
URL：https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview

【参考】Microsoft Defender SmartScreen の Microsoft Edge サポート
URL：https://docs.microsoft.com/ja-jp/deployedge/microsoft-edge-security-smartscreen

4-1-2　ファイル拡張子の表示設定

メールに添付されているファイルやローカルディスク、ファイルサーバなどに保管されているファイルが、怪しいファイルか見分ける方法として、ファイル名拡張子（ファイルの種類を区別するためにファイル名の末尾につけられる文字列）を確認する方法があります。

しかし、デフォルトでは下記のように非表示となっており、ファイルの拡張子確認することができません。



注意事項

拡張子を表示させた場合、拡張子の削除や変更が出来てしまいます。誤って拡張子の削除や変更をした場合、ファイルを開くことができない等の問題が起きますので注意してください。拡張子を誤って変更した場合は、元の拡張子に戻すことで、ファイルを元に戻すことができます。

下記手順により、ファイル名拡張子が表示され、ファイルの拡張子を確認することができるようになります。

【手順①】

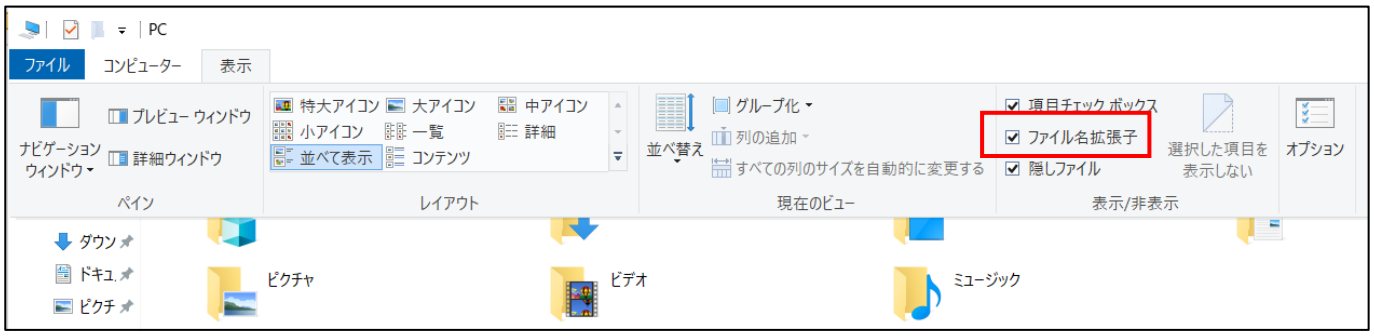
タスクバーの「エクスプローラー」をクリックし、エクスプローラーを表示します。

【手順②】

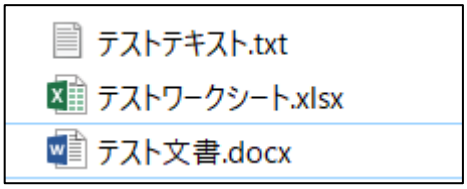
「表示」をクリックします。

【手順③】

「ファイル名拡張子」にチェックを入れます。



ファイル名拡張子が表示されるようになります。



4-2　チェックリスト 4-1 への対応

4-2-1　　第三者からの盗聴・のぞき見の対策

テレワークはオフィスワークに比べ、第三者（家族を含む）に盗聴・のぞき見されるリスクが高くなります。そのため、**オフィス外で端末を利用する場合は第三者からの盗聴・のぞき見されないよう注意する必要があります。**端末に投影されている会情報がのぞき見されないように**のぞき見防止フィルム**を利用する、端末から離れる際は、**画面ロックをかける**等の対策が必要です。

手動スクリーンロックのかけ方

テレワーク端末から離れるときは、Windows キーを押しながら「L」キーを入力し、使用している端末をロックします。

自動スクリーンロック設定

ロックをせずに端末から離れてしまう場合に備え、一定時間操作しない場合に自動的にロックする設定を行います。

【手順①】

デスクトップで右クリックを行い、個人用設定をクリックします。

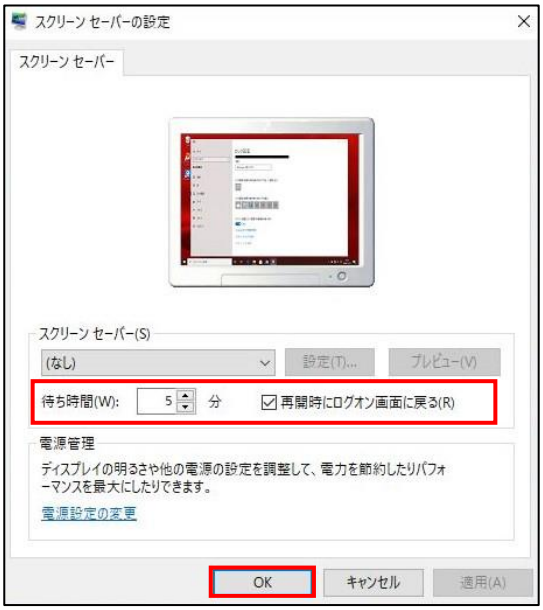
【手順②】

左ペインにある「ロック画面」から「スクリーンセーバー設定」へと進みます。

【手順③】

スクリーンセーバーの設定画面の表示後、「再開時にログオン画面に戻る」にチェックを入れ、任意の待ち時間（※）を入力し、「OK」をクリックすることで、任意の待ち時間で自動的にスクリーンロックが行われます。

※　待ち時間が長いと離席時にのぞき見されるリスクが高まります。下記では一例として待ち時間を 5 分としています。



4-3　チェックリスト 5-1 に対する利用者向け作業

4-3-1　　メーカーサポートの確認

利用する端末の OS やアプリケーションは、製品提供元からサポートのあるバージョンを利用します。サポート切れの OS やアプリケーションを使用していると不具合や脆弱性が修正されないため、不正アクセスの起点となってしまう恐れがあり、セキュリティ上のリスクとなります。OS のサポート期間については、Microsoft 社のサイト（※）を確認するか、Windows OS 端末の取引のある SI ベンダーや代理店に確認してください。

※　Microsoft ライフサイクルポリシー（https://docs.microsoft.com/ja-jp/lifecycle/）

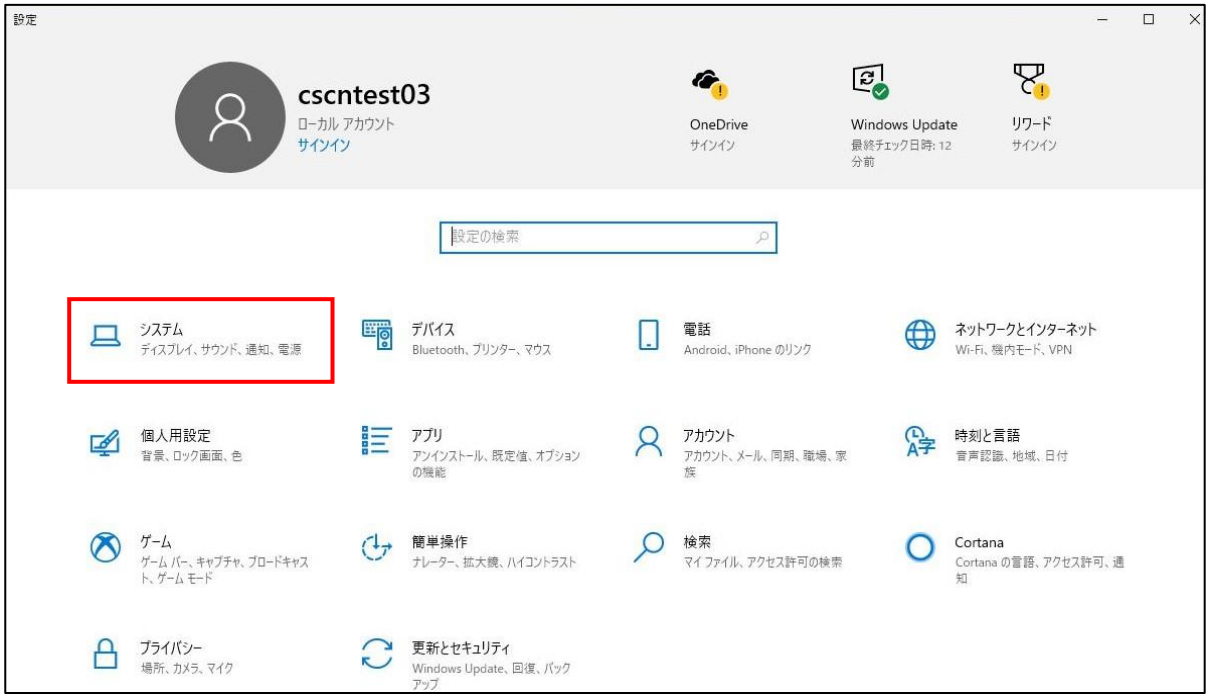
OS バージョンの確認方法

【手順①】

Windows 画面左下のスタートをクリック後、「設定」をクリックします。

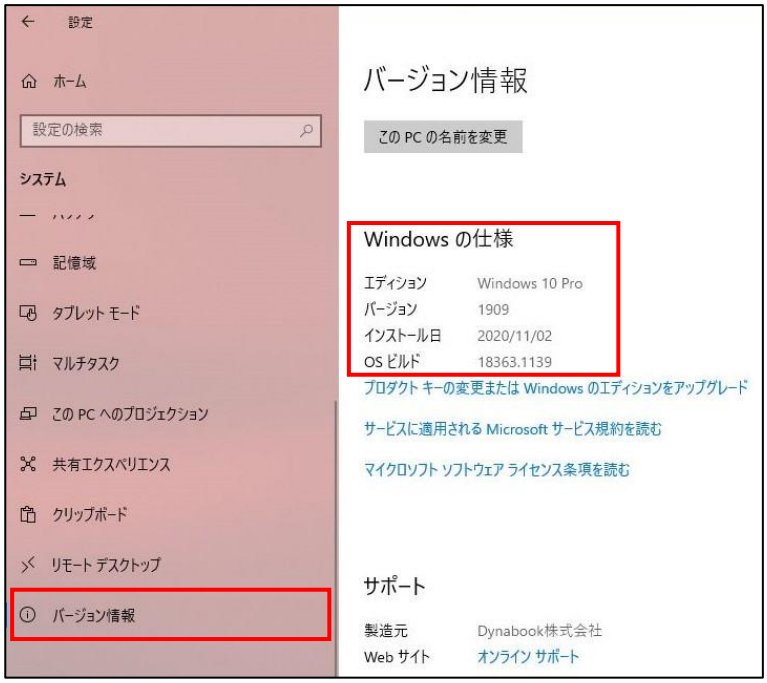
【手順②】

下図の画面に遷移後、「システム」をクリックします。



【手順③】

「バージョン情報」を選択後、右ペインにある「Windows の仕様」から現在のバージョンを確認します。



アプリケーションバージョン確認

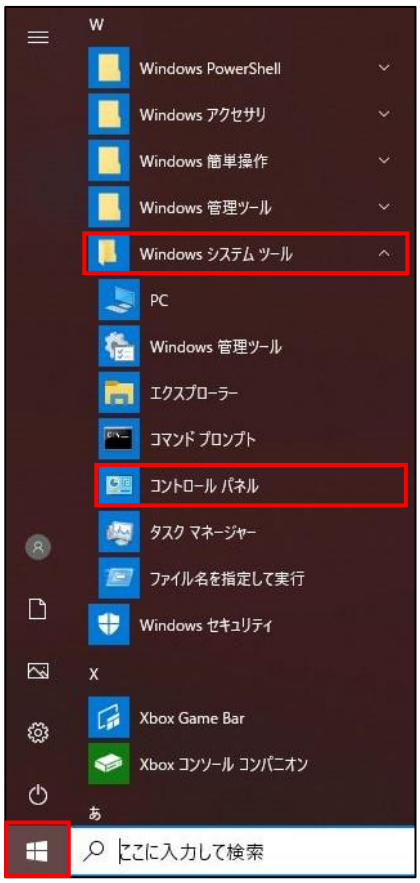
端末内にインストールしているアプリケーションが最新となっているか確認します。

＜参考情報－各種 Web ブラウザの場合＞

・ Microsoft Edge/Google Chrome/Firefox の場合
デフォルトでは自動アップデートが有効になっているので自動でアップデートされます。

【手順①】

Windows 画面左下のスタートをクリック後、「Windows システムツール」から「コントロールパネル」をクリックします。



【手順②】

下図の画面に遷移後、「プログラム」をクリックします。画像のような画面に進まない場合は「表示方法」をカテゴリに変更してください。

【手順③】

「プログラムと機能」をクリックします。

【手順④】

「プログラムのアンインストールまたは変更」の一覧からプログラム名とバージョンを確認します。

4-4　チェックリスト 5-2 への対応

4-4-1　　OS 及びアプリケーションの最新化

OS やアプリケーションを最新の状態にアップデートして利用します。アップデートをすることは、OS やアプリケーションの脆弱性が修正され、**脆弱性をついたサイバー攻撃に対して有効な対策となります。**そのため、定期的にアップデートがないか確認をすることを推奨します。Windows にインストールされている各アプリケーションのアップデートは、アプリケーションの更新機能、各製品の公式 HP 等で確認するか、対象製品の取引のある SI ベンダーや代理店に確認を行ってください。

ここでは以下の手順を記載します。

- Windows Update 確認
- Windows Update 自動インストール設定
- Windows Update 手動インストール

Windows Update 確認

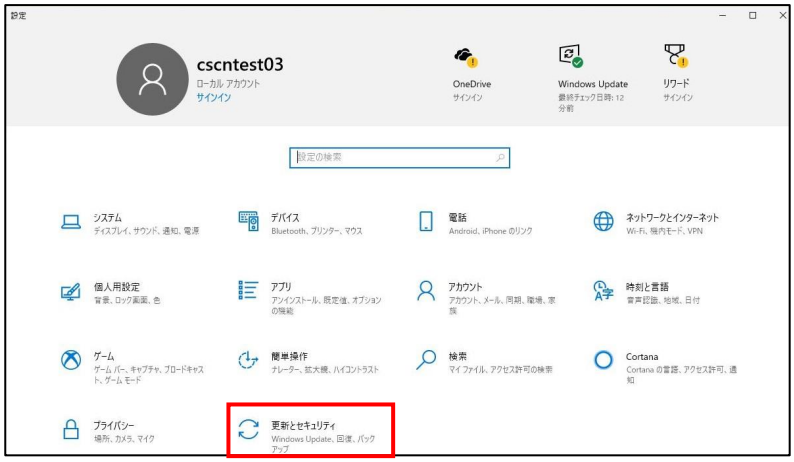
Windows Update 更新プログラムが最新となっているかを確認します。

【手順①】

Windows 画面左下のスタートをクリック後、「設定」をクリックします。

【手順②】

下図の画面に遷移後、「更新とセキュリティ」をクリックします。



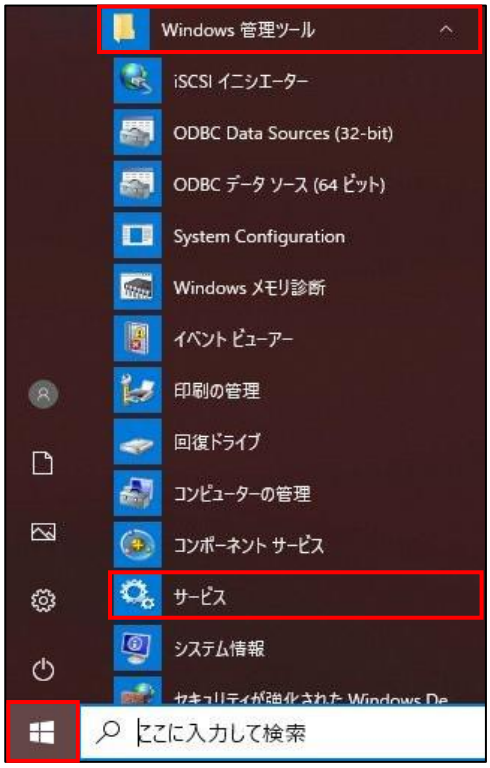
【手順③】

「Windows Update」を選択後、右ペインにある「Windows Update」に「最新の状態です」と記載があることを確認します。最新ではない場合、更新プログラムのインストールが行われます。

Windows Update 自動インストール設定

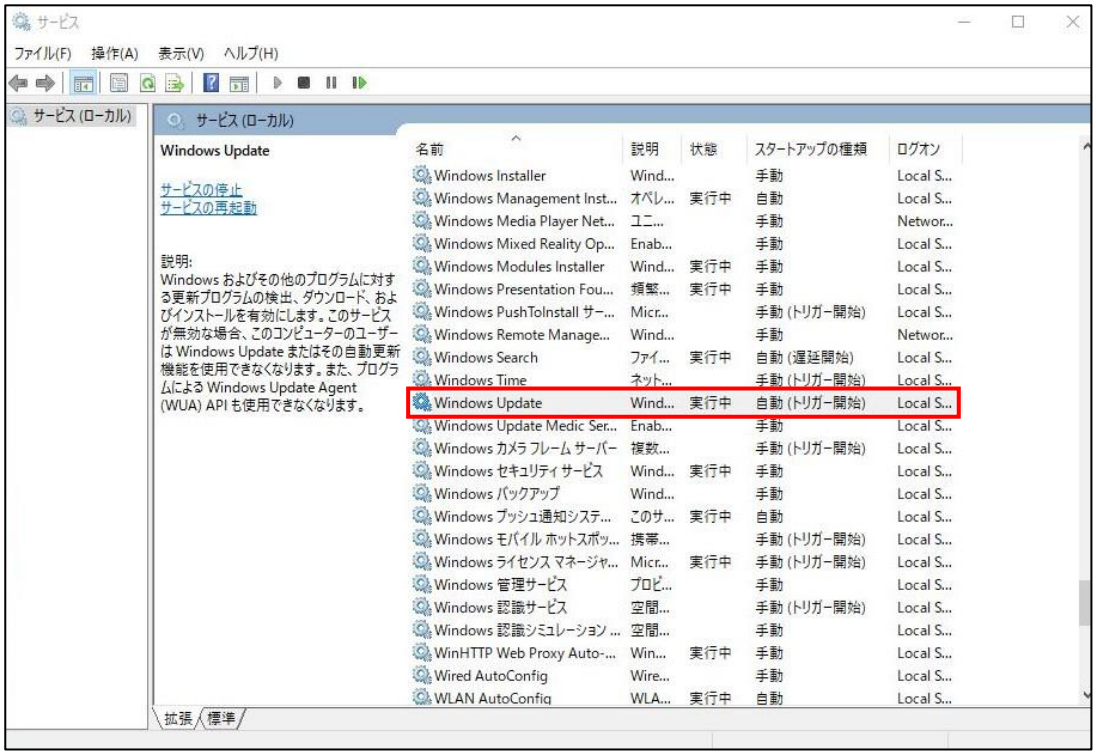
【手順①】

Windows 画面左下のスタートをクリック後、「Windows 管理ツール」から「サービス」をクリックします。



【手順②】

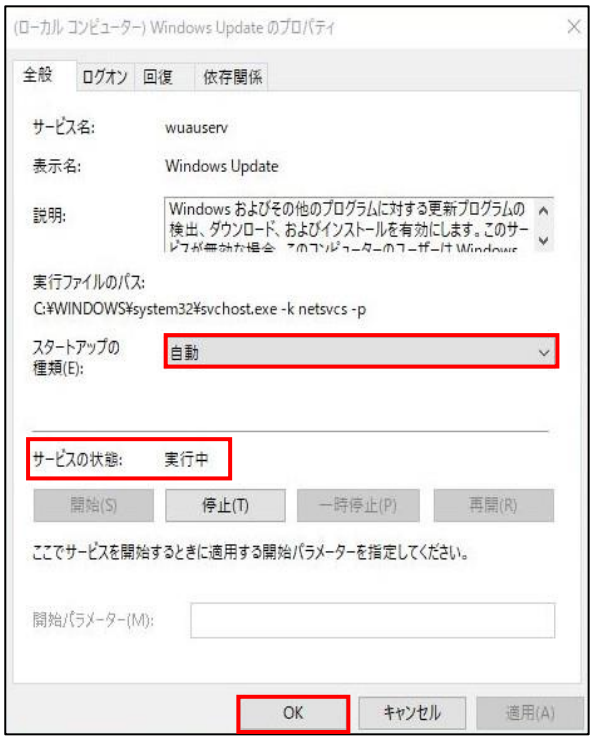
サービス（ローカル）一覧の中にある「Windows Update」をダブルクリックします。



【手順③】

「全般タブ」にある「スタートアップの種類」が「自動」になっており、「サービスの状態」が「実行中」となっていることを確認します。
自動になっていない場合は、「スタートアップの種類」を「自動」に変更します。また「サービスの状態」が「停止中」の場合は、「開始」をクリックします。

「OK」をクリックして設定終了です。



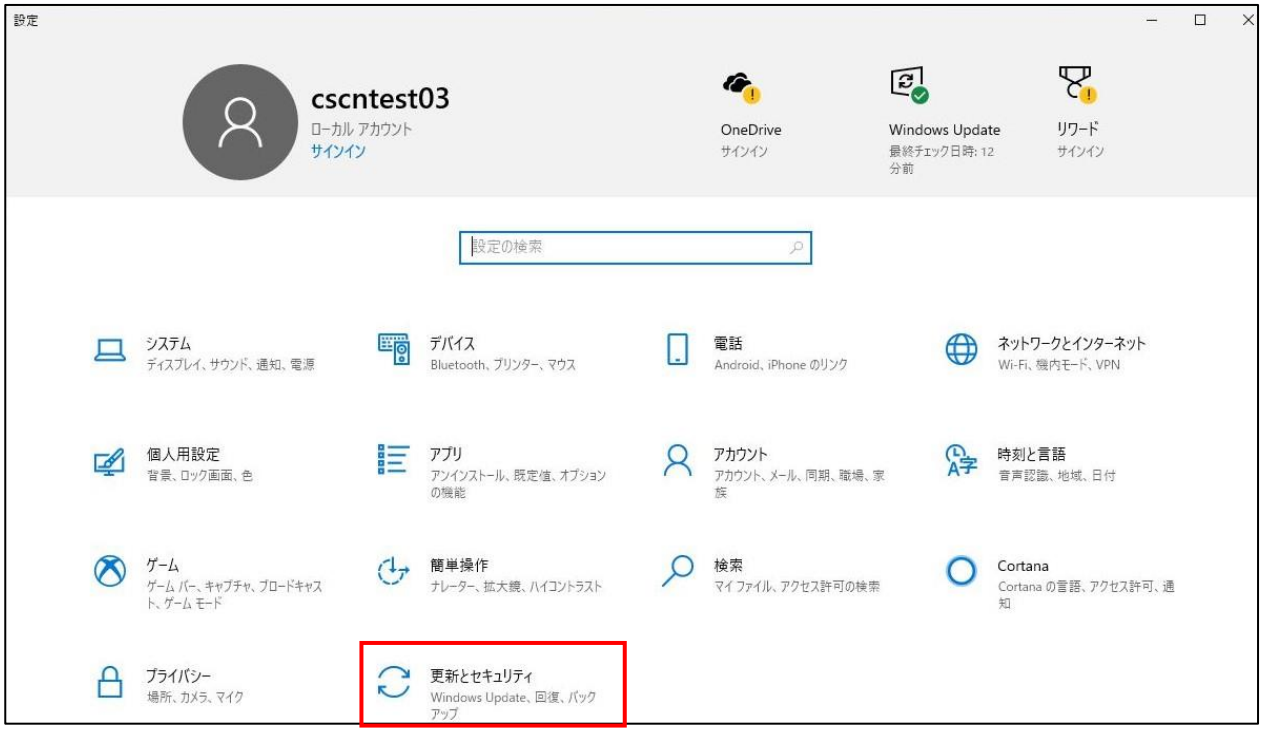
Windows Update 手動インストール

【手順①】

Windows 画面左下のスタートをクリック後、「設定」をクリックします。

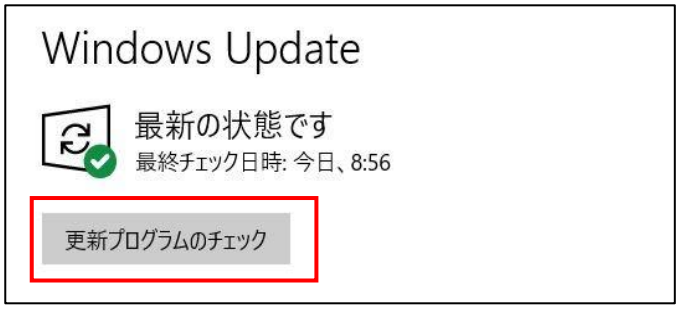
【手順②】

下図の画面に遷移後、「更新とセキュリティ」をクリックします。

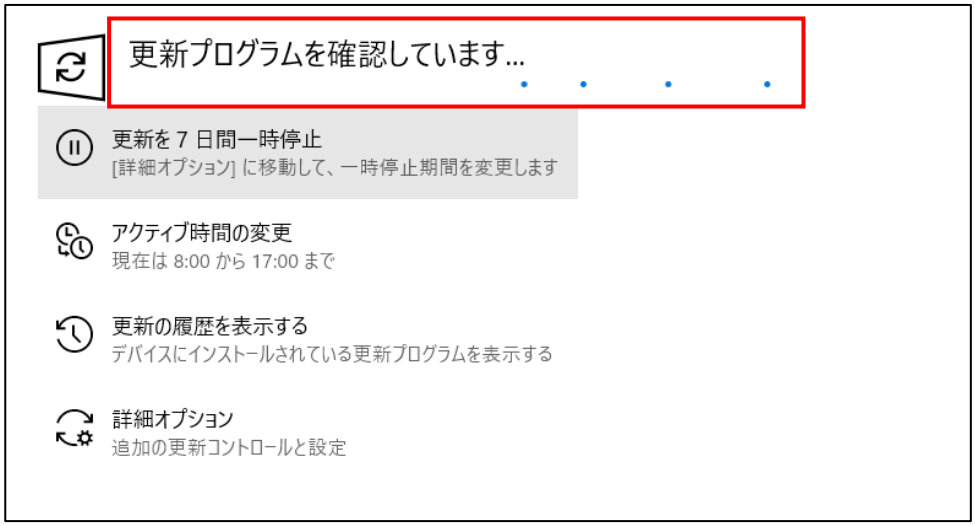


【手順③】

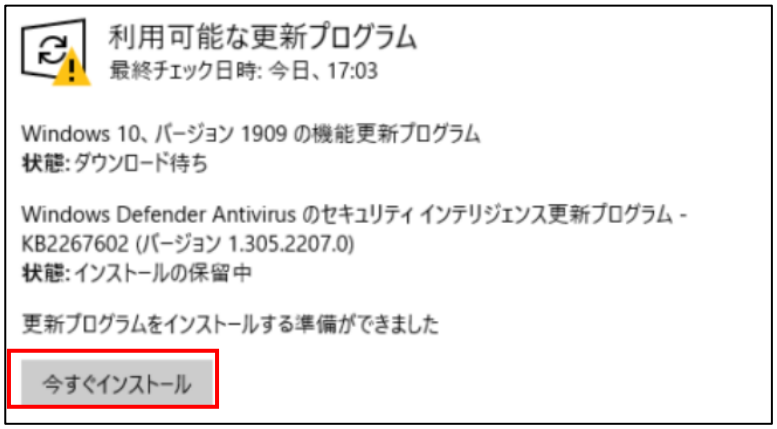
「Windows Update」を選択後、右ペインにある「更新プログラムのチェック」をクリックします。



「更新プログラムを確認しています…」と表示されます。



利用可能な更新プログラムが表示された場合は、自動でダウンロードが始まります。自動でダウンロード始まらない場合は、「今すぐインストール」ボタンが表示されますので、「今すぐインストール」をクリックします。



更新プログラムのダウンロード/インストールはバックグラウンドで処理されますが、インストール後に再起動が必要になる場合もあります。

4-5　チェックリスト 6-1 への対応

4-5-1　　サービスへの接続確認

インターネットの通信は、通信内容をどこかで盗み見られたり、改ざんされたりする可能性があります。そのため、通信内容が暗号化されている「HTTPS」通信で接続しているかを確認します。Web サイトにアクセスする場合は、ブラウザの接続先 URL 入力欄（アドレスバー）を確認し、接続先のサイトが「https://」から始まっているかどうかを確認します。

＜参考情報－主要ブラウザの URL 入力欄（アドレスバー）の確認場所＞

・ Microsoft Edge の場合

・ Google Chrome の場合

・ Firefox の場合

4-6　チェックリスト 6-2 への対応

4-6-1　　無線 LAN のセキュリティ方式の確認

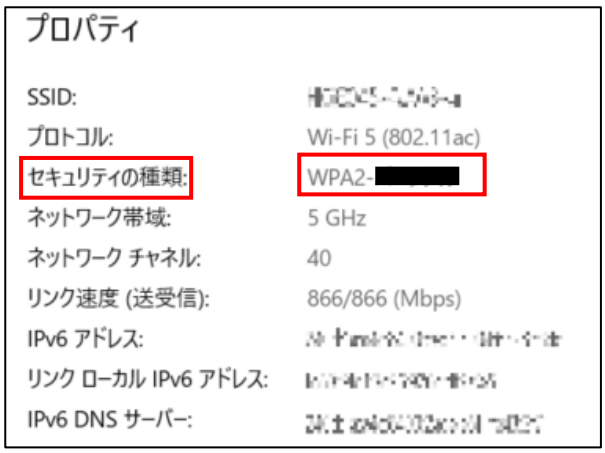
無線 LAN の暗号化方式**「WEP」や「WPA」は脆弱性があり、通信内容を盗み見られる危険性があります。**そのため、より安全な暗号化方式である「WPA2」や「WPA3」を用いて、無線 LAN を利用していることを確認します。

【手順①】

デスクトップの右下にある「」マークを左クリックします。接続済の Wi-Fi の「プロパティ」を左クリックします。

【手順②】

下記画面の画面が表示されます。「プロパティ」の「セキュリティの種類」が「WPA2」または「WPA3」になっていることを確認します。「WEP」や「WPA」で接続していた場合は別の Wi-Fi に繋ぎ直すことを推奨します。



4-7　チェックリスト 8-1 への対応

4-7-1　　端末位置の把握

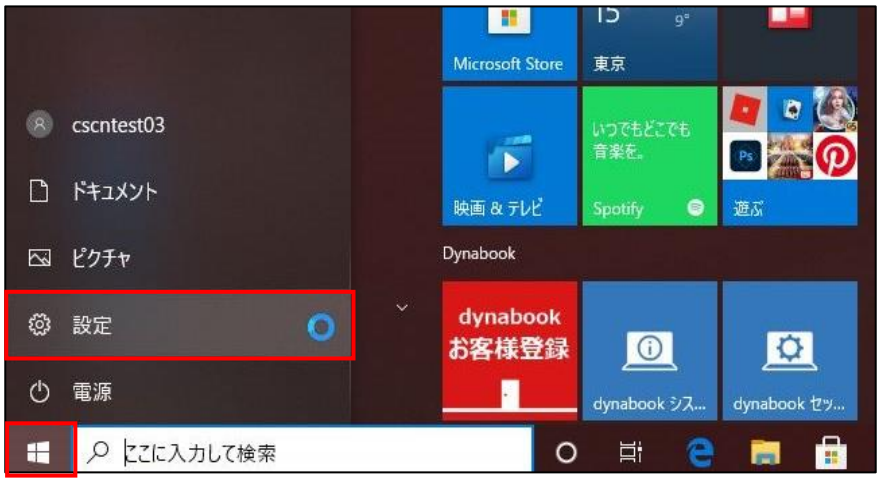
端末の紛失・盗難に備えて位置情報を検出できるように設定します。端末の位置情報を検出できるように設定することにより、**紛失・盗難時に端末の位置を特定できる可能性が高まり、情報漏洩のリスクを低減することができます。**
端末の位置情報を検出するには、下記の端末の位置情報の設定を有効しておくことに加え、端末に Microsoft アカウント（下部に解説あり）を管理者として追加し、連携しておく必要があります。対象端末の位置情報は、連携している Microsoft アカウント保有者のみが確認することができます。

この手順は、利用者が自身のテレワーク端末の位置を確認できるようにする方法です。**管理者側で一律に管理を行いたい場合は、別途 MDM 製品の導入を検討してください**。

位置情報の取得設定

この設定を行うことで、端末の場所を調べられるようにする機能を有効化します。

【手順①】
Windows 画面左下のスタートをクリック後、「設定」をクリックします。

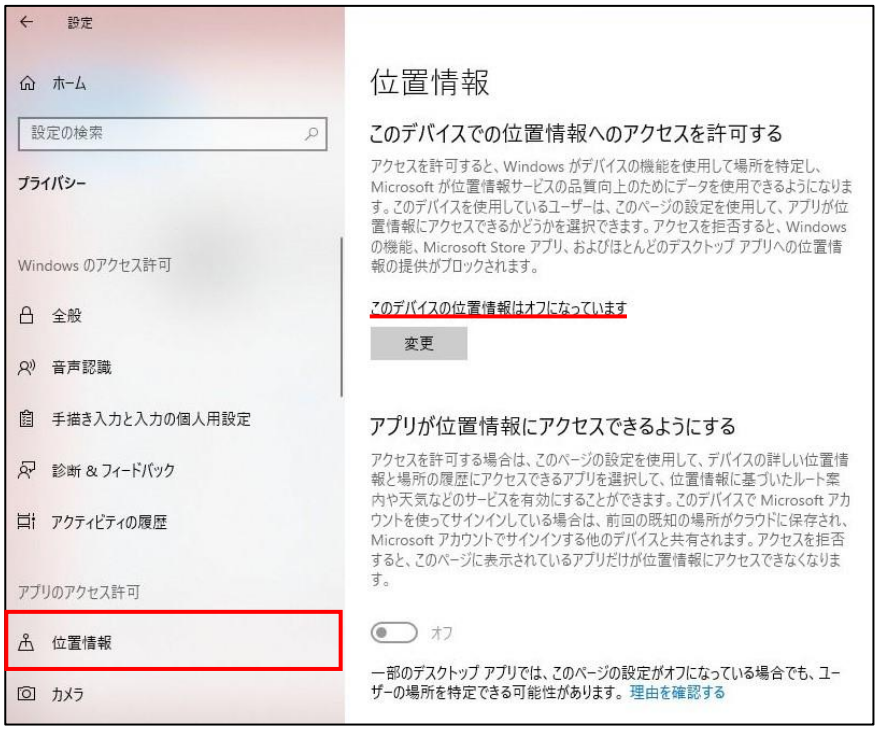


【手順②】

次の画面に遷移後、「プライバシー」をクリックします。

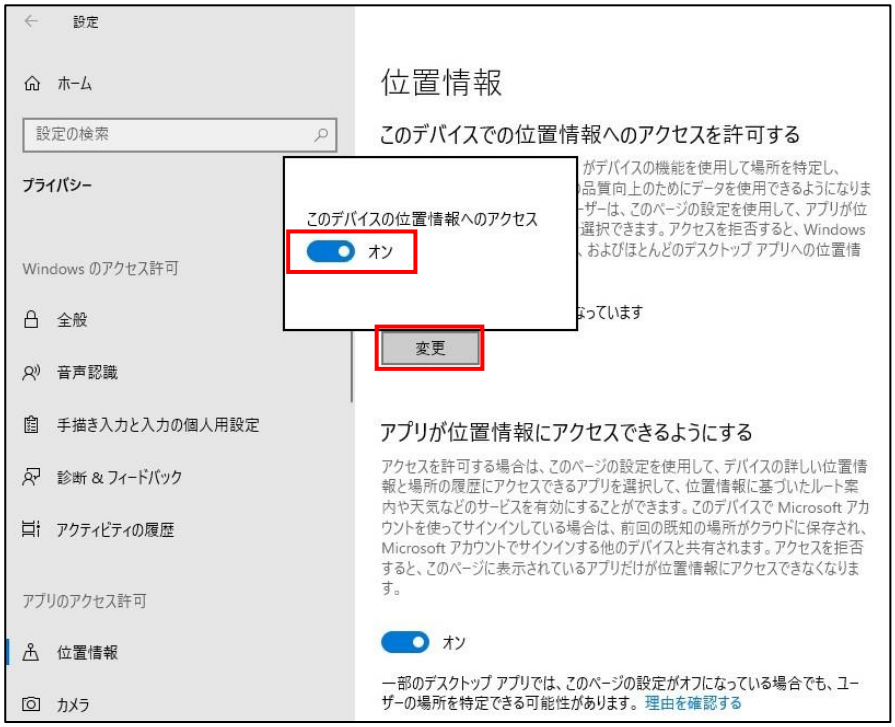
【手順③】

「位置情報」を選択後、右ペインにある「このデバイスでの位置情報へアクセスを許可する」を確認します。「このデバイスの位置情報はオフになっています」という表示があった場合、【手順④】を実施し、設定を有効化します。



【手順④】

「変更」をクリックし、位置情報をオンにします。

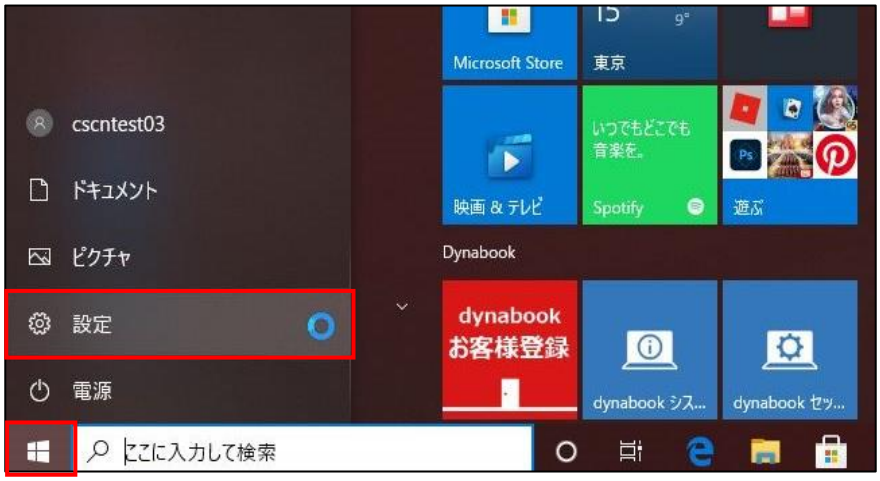


Microsoft アカウントを管理者として端末に追加

Microsoft アカウントを管理者として端末に追加します。

【手順①】

Windows 画面左下のスタートをクリック後、「設定」をクリックします。

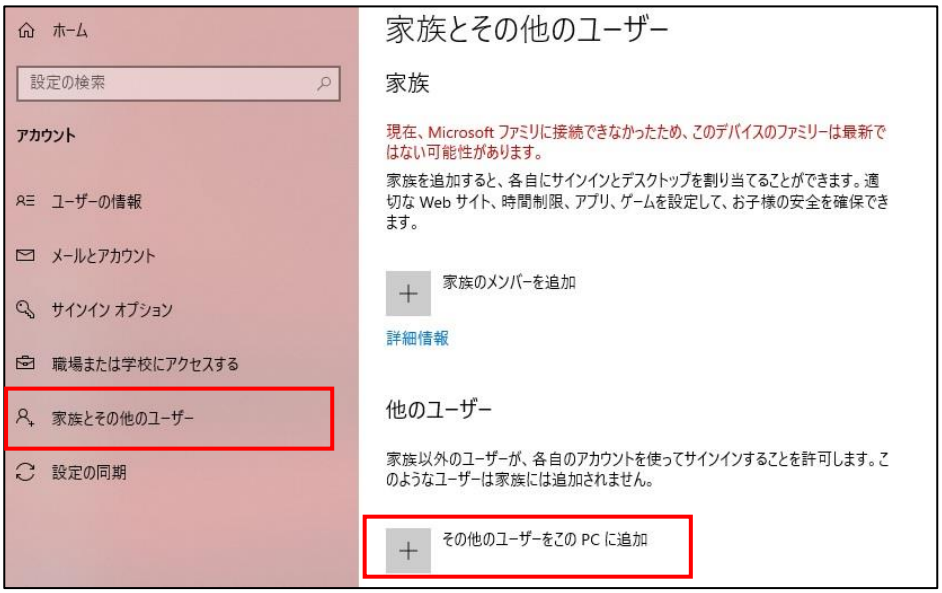


【手順②】

次の画面に遷移後、「アカウント」をクリックします。

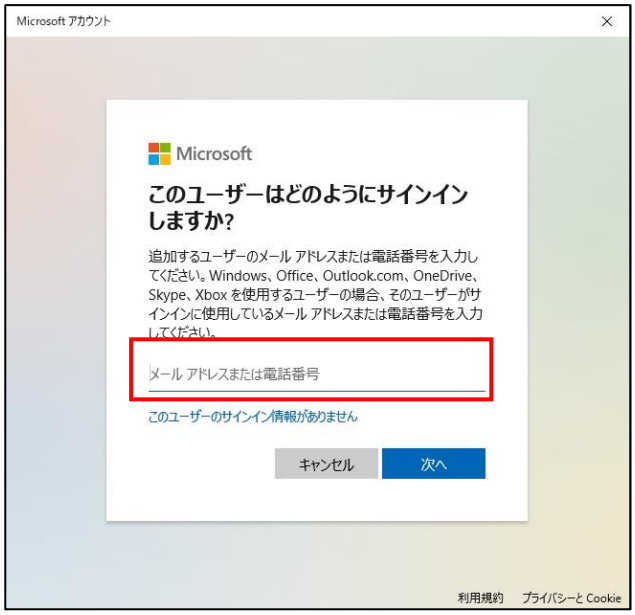
【手順③】

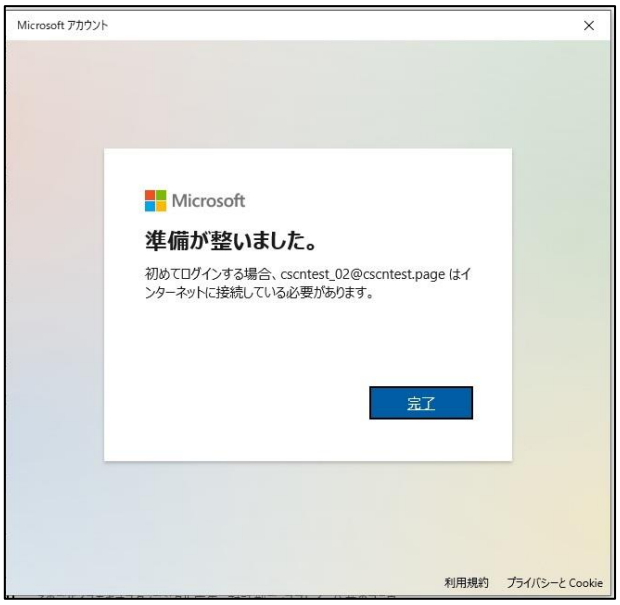
「家族とその他のユーザー」の「その他のユーザーをこの PC に追加」をクリックします。



【手順④】

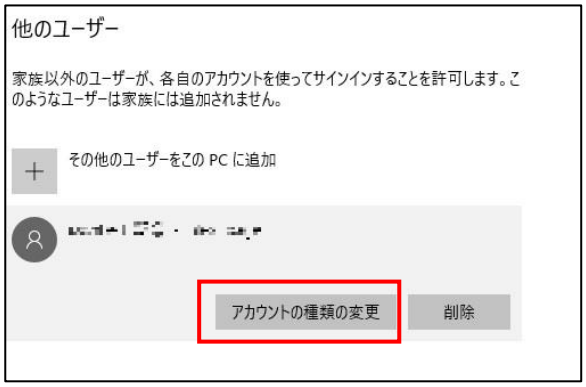
追加する Microsoft アカウントを入力し、「次へ」をクリックします。「準備が整いました。」の画面に遷移後、「完了」をクリックします。

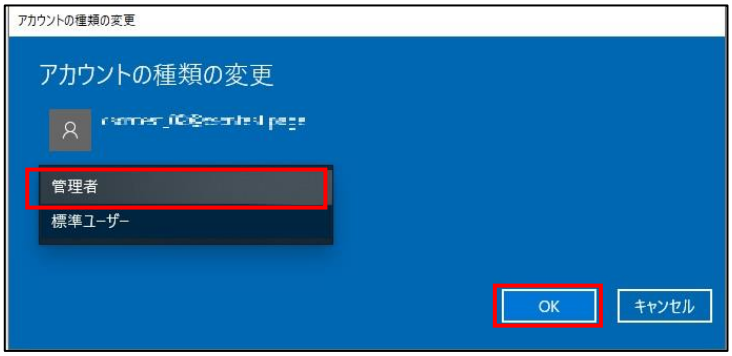




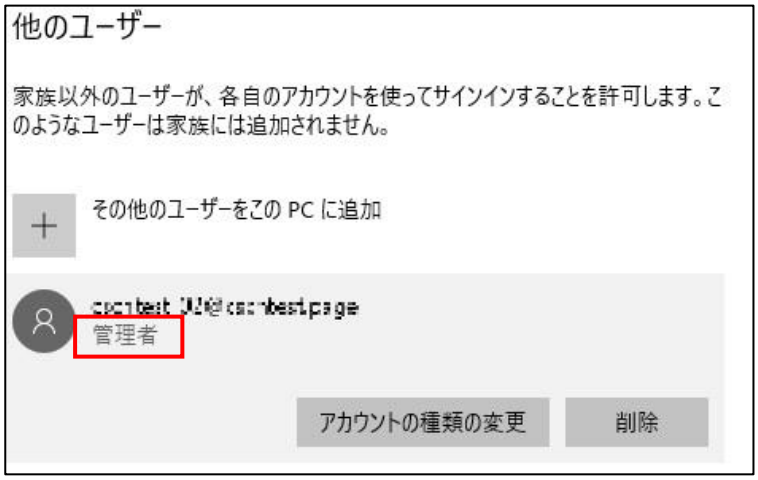
【手順⑤】

「アカウントの種類の変更」をクリックし、管理者を選択後、「OK」をクリックします。





追加した Microsoft アカウントが、端末の管理者となります。



【手順⑥】

現在サインインしているアカウントからサインアウトします。インターネットに接続し、追加した Microsoft アカウントで端末にサインインします。これにより、端末と Microsoft アカウントの連携が完了します。

端末位置の確認方法

【手順①】

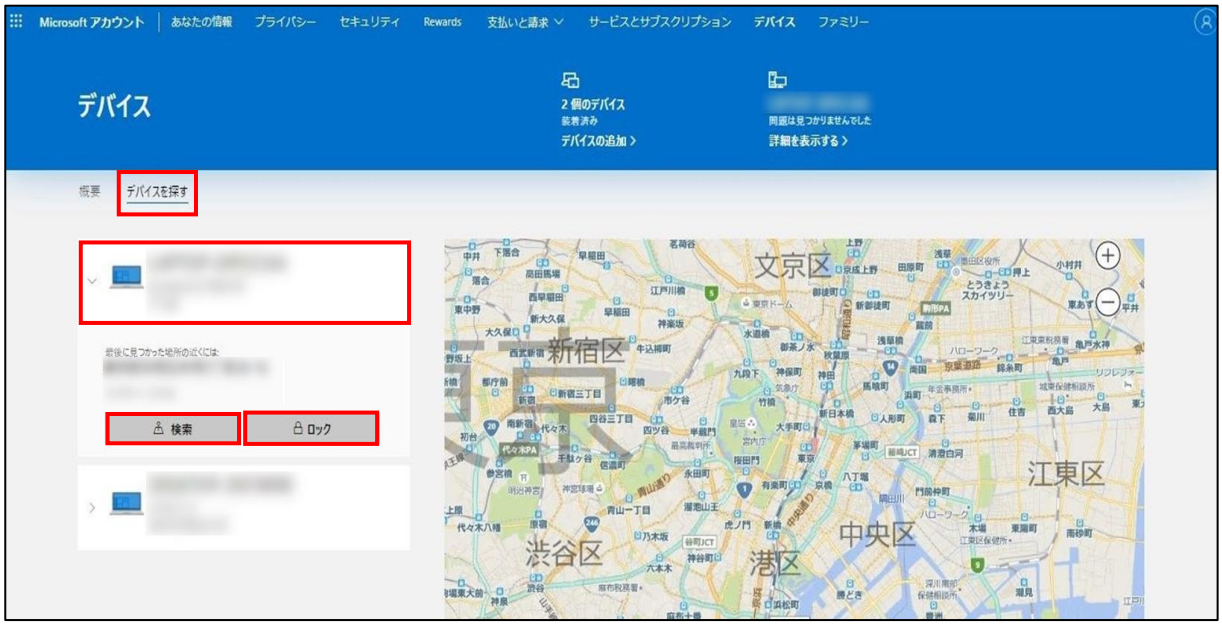
別の端末から Web ブラウザから下記サイトへアクセスし、端末に追加した Microsoft アカウントでログインします。

https://account.microsoft.com/devices

【手順②】

アクセス後、画面真ん中にある「デバイスを探す」を選択し、該当の端末名をクリックします。「検索」をクリックすると、端末の現在地が表示されます。また、同じ画面内の「ロック」をクリックすると、リモートで対象端末をロックすることができます（検出時点でログインしているユーザーをサインアウトさせてロック画面に切り替えることができます）。

ただし、対象端末の状況（電池切れ等）によっては、位置情報を検索できないことがあります。



【参考】Microsoft アカウントについて

貸与端末の「Windows へのログインアカウント」と「Microsoft アカウント」は、下記の通り、アカウントとしては異なるものです。

- Microsoft アカウント（※）：個人が作成して個人が管理するアカウント
- 貸与端末の Windows へのログインアカウント
  - 組織アカウント：組織の管理者が作成して組織で管理するアカウント
  - ローカルアカウント：端末毎にユーザー名と任意のパスワードを登録する端末固有のアカウント

※ Microsoft アカウントは任意のメールアドレスを利用して作成できますが、組織アカウントのメールアドレスを使用して作成することは出来ません。

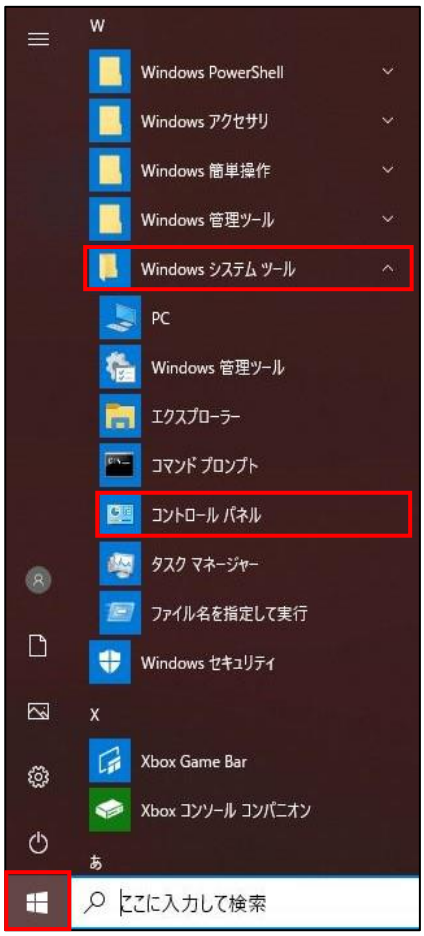
4-8　チェックリスト 8-3 への対応

4-8-1　　BitLocker による暗号化設定

端末が、紛失・盗難によって悪意のある第三者にわたってしまった場合、端末からデータを盗まれ、悪用される恐れがあります。Windows にロックがかかっている場合でも HDD を抜き出してデータが盗まれる可能性があるため、Windows に導入されている、HDD の保護を目的とした暗号化ソフトウェア「BitLocker」を有効化します。**BitLocker を有効にすることで HDD 内のデータを暗号化することができ、紛失時に端末からデータを盗まれるリスクを低減することができます。**

【手順①】

Windows 画面左下のスタートをクリック後、「Windows システムツール」から「コントロールパネル」をクリックします。



【手順②】

下図の画面に遷移後、「システムとセキュリティ」をクリックします。画像のような画面に進まない場合は、右上の表示方法を「カテゴリ」に変更してください。

【手順③】

右ペインにある「BitLocker ドライブ暗号化」をクリックします。

【手順④】

オペレーティングシステムドライブに「BitLocker が有効です」と表示があれば、HDD の暗号化が有効になっています。

有効化されていなかった場合は、【手順③】に続けて、以下の手順を実施します。

【手順⑤】

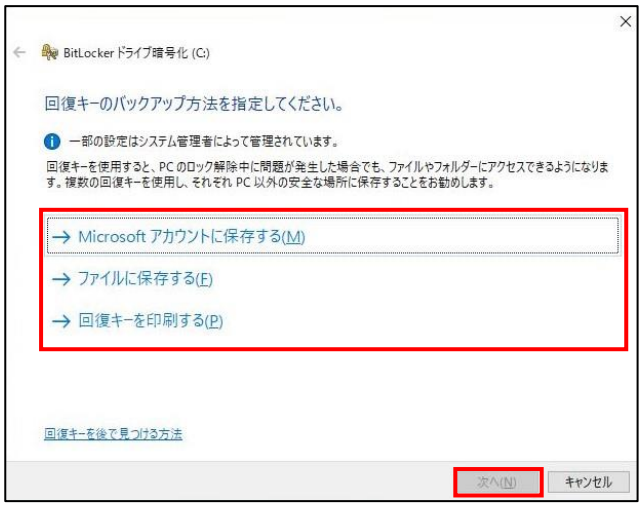
「オペレーティングシステムドライブ」の「BitLocker を有効にする」をクリックします。BitLocker 暗号化処理は、ドライブのサイズによっては時間がかかることがあります。暗号化を行っている最中は、動作が遅くなる場合もありますが、他作業と並行して暗号化を実施することができます。

【手順⑥】

「PIN を入力する（推奨）」を選択し、BitLocker を解除するための PIN を入力後、「PIN の設定」をクリックします。

【手順⑦】

BitLocker を解除するために必要となる 48 桁の数字の回復キーの保存場所を指定します。回復キーは、下図の 3 種類から保存できます。この情報は、任意の場所で大切に保管してください。保存ができたら「次へ」をクリックします。

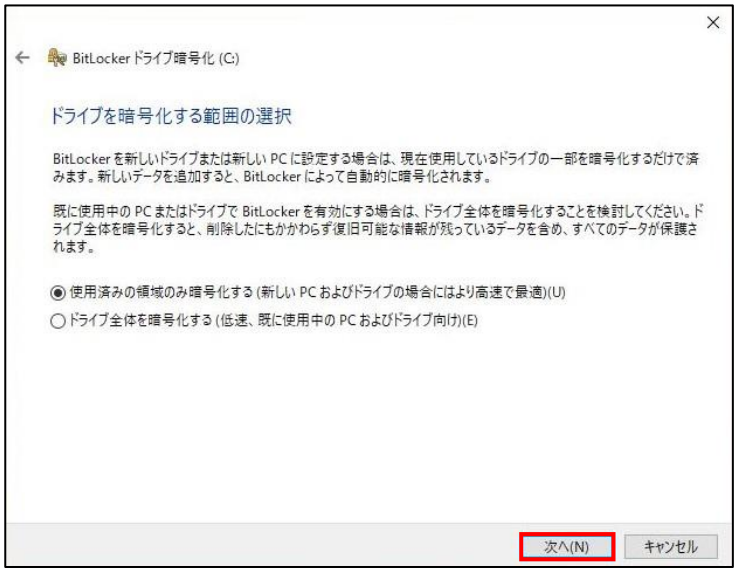


【手順⑧】

ドライブを暗号化する範囲を選択します。

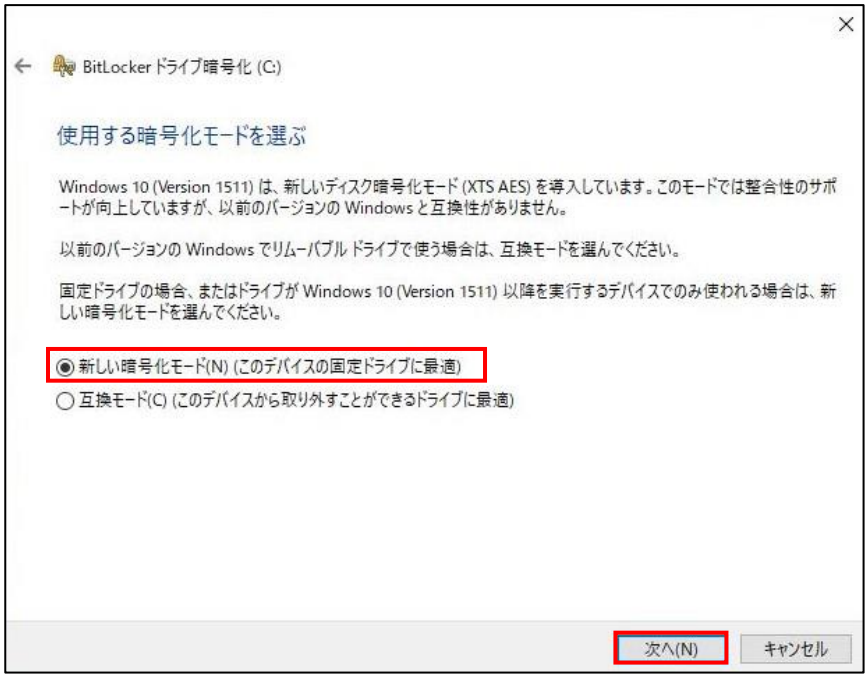
新しい PC の場合は、「使用済みの領域のみ暗号化する」を選択します。

既存の PC の場合は、「ドライブ全体を暗号化する」を選択し、「次へ」をクリックします。



【手順⑨】

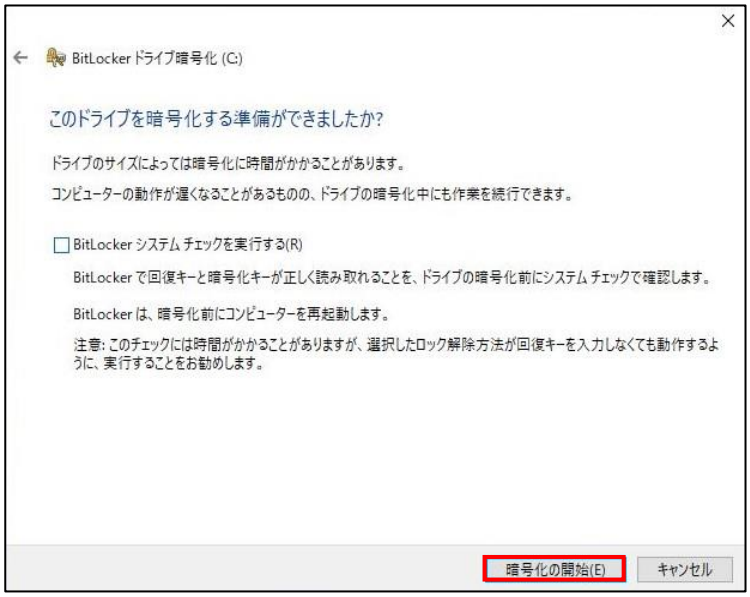
使用する暗号化モードを選択します。「新しい暗号化モード」を選択し、「次へ」をクリックします。



【手順⑩】

「暗号化の開始」をクリックすると暗号化が開始されます。

回復キーが実際に使用できるかどうかを確認したい場合は「BitLocker システムチェックを実行する」にチェックを入れ、「続行」をクリックします。チェックを入れた場合は再起動が必要です。



【手順⑪】

下図のように「BitLocker が有効です」と表示があれば HDD の暗号化が有効になっています。

4-9　チェックリスト 9-2 への対応

4-9-1　　初期パスワード設定変更

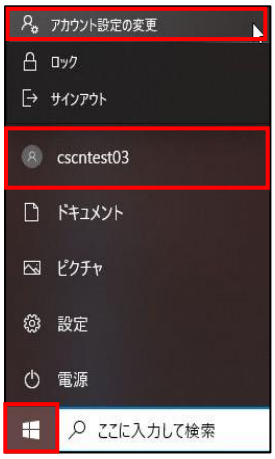
初期パスワードは、誰が把握しているかわからないので、速やかにパスワード要件を満たすものに変更することで、**悪意のある第三者から不正アクセスされるリスクを低減することができます。**

職場環境によっては、以下の手順で変更できない場合があります。その場合は、職場のパスワード変更手順に従ってパスワードを変更してください。

【手順①】

画面左下の Windows スタートメニューをクリックし、「cscntest03」（※）をクリック後、「アカウント設定の変更をクリック」し、アカウントの設定変更画面を表示させます。

本手順ではアカウント名を「cscntest03」としています。

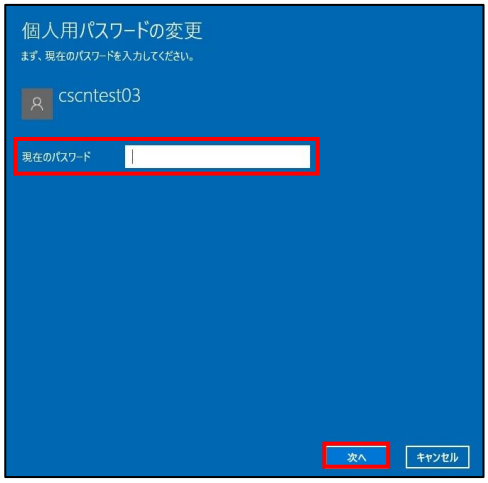


【手順②】

左ペインの「サインインオプション」を選択し、デバイスへのサインイン方法の管理から「パスワード」-「変更」をクリックします。

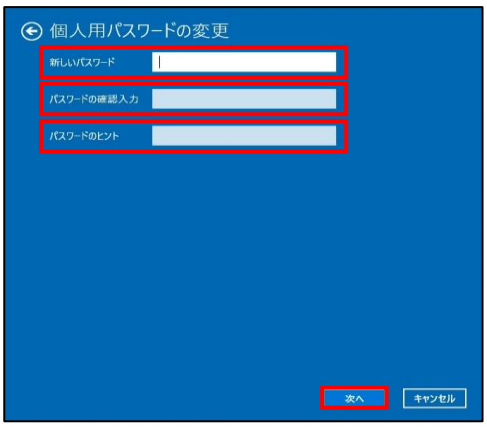
【手順③】

画面に従って「現在のパスワード」を入力し、「次へ」をクリックします。



【手順④】

「新しいパスワード」「パスワードの確認入力」「パスワードのヒント」を入力し、「次へ」をクリックします。



【手順⑤】

現在ログインしているアカウント名が表示されるので、「完了」をクリックするとパスワードの変更が完了します。