

中小企業向けセキュリティ対策 最適化モデル

2024年1月5日

一般社団法人 地域セキュリティ協議会
調査研究委員会



改訂履歴

版数	日付	内容
1.0	2024/1/5	初版発行

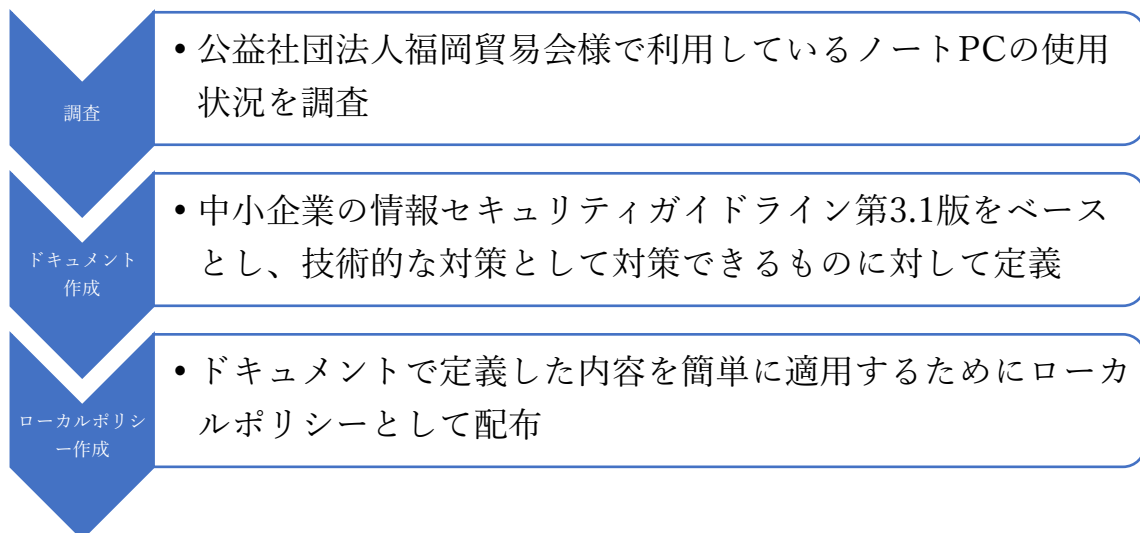
目次

1. はじめに	4
2. 中小企業向けセキュリティ対策最適化モデル	5
2.1. 中小企業の情報セキュリティ対策ガイドライン	6
2.2. 対象システム及び規模	9
2.3.1. ツールマップ	10
2.3.2. 設定項目マップ	11
2.4. 推奨するツール詳細	12
2.4.1. Microsoft Defender	12
2.4.2. MyJVN バージョンチェッカ	13
2.4.3. BitLocker	16
2.4.4. KeePass	18
2.4.5. Windows Defender ファイアウォール	22
2.4.6. Windows Hello	27
2.4.7. 7-zip	31
2.4.8. 脅威情報の取得	33
2.4.9. フォーマットツール	35
2.4.10. Thunderbird	36
2.5. 推奨する設定項目詳細	38
2.5.1. スクリーンロック	38
2.5.2. フィッシングメール対策	42
2.5.3. メールの誤送信防止	45
2.5.4. パスワードポリシー	51
2.5.5. ソフトウェア更新	53
2.5.6. ファイアウォール	57
2.5.7. アカウント管理	62
2.6. 導入にあたっての留意点	67
3. さらにセキュリティを向上させるには	67
4. おわりに	67
5. 参考資料	68

1. はじめに

中小企業に対するサイバー攻撃も増えており、中小企業においてもサイバーセキュリティ対策を進めていく必要があります。しかしながら中小企業においてすぐにサイバーセキュリティ対策の費用を捻出することは困難です。対策の第一歩として少しでも中小企業のセキュリティを向上させるためにコストをかけずに行える対策という点に着眼し、IPAの「中小企業の情報セキュリティガイドライン第3.1版」をベースに「中小企業向けセキュリティ対策最適化モデル」としてまとめました。

本プロジェクトでは、実際の中小企業・団体をモデルケースとして中小企業向けのコストをかけずに行える対策の一助として対策のドキュメントとローカルポリシーの作成を行います。



本プロジェクトのロードマップ

2. 中小企業向けセキュリティ対策最適化モデル

中小企業向けセキュリティ対策最適化モデルでは、対策の第一歩として少しでも中小企業のセキュリティを向上させるためにコストをかけずに行える対策として、ツールを導入することによってセキュリティ対策を行える部分と、設定によってセキュリティ対策を行える部分の2種類に分けて構成しています。また、各項目がIPAの「中小企業の情報セキュリティガイドライン第3.1版」で公開されている「自社診断のための25項目」どの項目にあたるかも記載しています。

なお、現在はドキュメントの作成のみが進んでいますが、今後設定を自動的に反映するためのローカルポリシーの配布等を予定しています。

2.1. 中小企業の情報セキュリティ対策ガイドライン

「中小企業の情報セキュリティ対策ガイドライン」は、独立行政法人情報処理推進機構 (IPA) から個人事業主、小規模事業者を含む中小企業が情報セキュリティ対策に取り組む際の、(1) 経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたドキュメントとして公開されています。また、付録として情報セキュリティハンドブック(ひながた)や情報セキュリティ関連規定(サンプル)、中小企業のためのセキュリティインシデント対応手引き等も公開されており、中小企業における情報セキュリティの取り組みを実践する際に非常に有益な情報が整っています。



図 1 中小企業の情報セキュリティガイドライン第 3.1 版 表紙

引用元: 中小企業の情報セキュリティガイドライン第 3.1 版

表 1 中小企業の情報セキュリティガイドライン第 3.1 版 自社診断のための 25 項目

No	診断内容	
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？

引用元: 中小企業の情報セキュリティガイドライン第 3.1 版【表 5】自社診断のための 25 項目

表 2 本書での対応項目一覧

No	診断内容	本書での対応
基本的対策	1 パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	○
	2 パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	○
	3 パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	○
	4 重要情報に対する適切なアクセス制限を行っていますか？	○
	5 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	○
従業員としての対策	6 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	○
	7 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	○
	8 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	○
	9 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	×
	10 インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？	×
	11 パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	×
	12 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	×
	13 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	○
	14 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	○
	15 関係者以外の事務所への立ち入りを制限していますか？	×
	16 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	×
	17 事務所が無人になる時の施錠忘れ対策を実施していますか？	×
	18 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	○
組織としての対策	19 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	×
	20 従業員にセキュリティに関する教育や注意喚起を行っていますか？	×
	21 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	×
	22 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	×
	23 クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？	×
	24 セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	×
	25 情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？	×

2.2. 対象システム及び規模

本書は中小企業を対象としているため、PCの構成管理やユーザ管理ができておらず、ローカルアカウント等で管理している100人未満の事業所を想定しています。基本的には法人用途での利用のためWindows 10/11 Proを想定していますが、すでにWindows 10/11 Homeを導入してしまっている事業者もあることを考慮してWindows 10/11 Homeについても部分的に対応します。また、構成管理ツールが導入されていない環境を想定しているため、各種設定のポリシーはローカルポリシーとして配布することを想定しています。

種別	内容
OS	Windows 10 Pro Windows 11 Pro Windows 10 Home(部分的対応) Windows 11 Home(部分的対応)
ユーザ管理 (Active Directory 等)	なし
構成管理ツール (Intune 等)	構成管理ツール (Intune 等)
規模	100人未満を想定
ウイルス対策ソフト	Windows Defender

2.3. 中小企業向けセキュリティ対策最適化モデルマップ

本書では、ツールを導入することによってセキュリティ対策を行える部分と、設定によってセキュリティ対策を行える部分の2種類に分けて説明します。

2.3.1. ツールマップ

本書で推奨するツール一覧は下記の通りです。

対策/対象	ツール	自社診断のための25項目
マルウェア対策	Microsoft Defender	2
ソフトウェア更新	MyJVN バージョンチェッカ	1
紛失/盗難	BitLocker	13
パスワード管理	KeePass	3
パスワードポリシー	KeePass	3
ファイアウォール	Windows Defender ファイアウォール	4
認証補助	Windows Hello ※1	4
圧縮・解凍	7-zip ※2	8
脅威情報の取得	推奨する情報収集先をリストアップし Teams,Slack 等に自動的に流す	5
フォーマットツール	Windows 標準のものを利用	18
メール関連	Thunderbird	6,7

※1 対応している Web カメラが必要(外付 or 搭載型)

※2 ZIP 以外の解凍やパスワード付き ZIP の生成の必要がなければ Windows 標準の物のみでよい

2.3.2. 設定項目マップ

本書で推奨する設定は下記の通りです。

対策/対象	設定内容	自社診断のための 25 項目
スクリーンロック	一定時間操作がない場合スクリーンロックをかける	14
フィッシングメール対策	フィッシングメール対策機能を有効にする	6
メールの誤送信防止	メール誤送信対策機能を有効にする	7
パスワードポリシー	英大文字小文字+数字+記号で 10 桁以上 ※1	3
ソフトウェア更新	Windows Update のその他の Microsoft 製品の更新プログラムを有効にして実施	1
ファイアウォール	Windows 利用ポートの端末間アクセスは制限	4
アカウント管理	共通アカウントを利用して いる場合は利用者ごとに個別に発行	4

※1 NISC のインターネットの安全・安心ハンドブックより

※2 利用状況により別途緩和策等を検討

2.4. 推奨するツール詳細

推奨するツールの詳細について説明します。

2.4.1. Microsoft Defender

対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	マルウェア対策
自社診断のための 25 項目	2
URL	https://support.microsoft.com/ja-jp/windows/windows-%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%81%AB%E3%82%88%E3%82%8B%E4%BF%9D%E8%AD%B7%E3%82%92%E5%88%A9%E7%94%A8%E3%81%97%E3%81%BE%E3%81%99-2ae0363d-0ada-c064-8b56-6a39afb6a963

2.4.2. MyJVN バージョンチェッカ

対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	ソフトウェア更新
自社診断のための 25 項目	1
URL	https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

- 概要

MyJVN バージョンチェッカは、PC にインストールされているソフトウェアが最新のものであるかを確認するツールです。定期的にソフトウェアが最新のものであるかを確認し、更新することにより、古いバージョンを利用することによる、既知の脆弱性などのリスクを低減することができます。

● 導入方法

公式サイト (<https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html>) から MyJVN バージョンチェッカ for .NET をダウンロードし、解凍します。

その後、「1_Script_GUI」ディレクトリにある「MyJVN_.NET_GUI_Win10.bat」を実行します。起動すると下記のような画面が表示されるので、上部の実行ボタンを押します。



実行が終わると、下記のようにチェック結果が表示され最新ではないバージョンのソフトウェアが確認できます。また、一覧の表示ボタンを押すことにより詳細を確認することができます。



MyJVNバージョンチェッカ for .NET (v1.1)

MyJVNバージョンチェッカ for .NET 実行 終了 全てを選択 選択をクリア 結果出力

「選択」されたソフトウェア製品を「実行」することで、最新バージョンであるかをチェックします。「最新のバージョンではありません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にして、ベンダから最新のバージョンを入手してください。利用に関する情報は、MyJVNのウェブページ (<https://jvndb.jvn.jp/apis/myjvn/index.htm>)を参照ください。

ソフトウェア製品名 ▲	チェック結果 ▲(○=順)	結果詳細 ▲
<input checked="" type="checkbox"/> Google Chrome	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> Mozilla Firefox	× 最新のバージョンではありません	表示
<input checked="" type="checkbox"/> iTunes	○ 最新のバージョンです	表示
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Adobe Reader	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Adobe Shockwave Player	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Becky! Internet Mail	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> JRE	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Lhaplus	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> LibreOffice	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Lunascape	— インストールされていないか、対象外のバージョンです	
<input checked="" type="checkbox"/> Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	

2.4.3. BitLocker

対象 OS	Windows 10 Pro Windows 11 Pro
対策/対象	紛失/盗難
自社診断のための 25 項目	13
URL	https://learn.microsoft.com/ja-jp/windows/security/operating-system-security/data-protection/bitlocker/

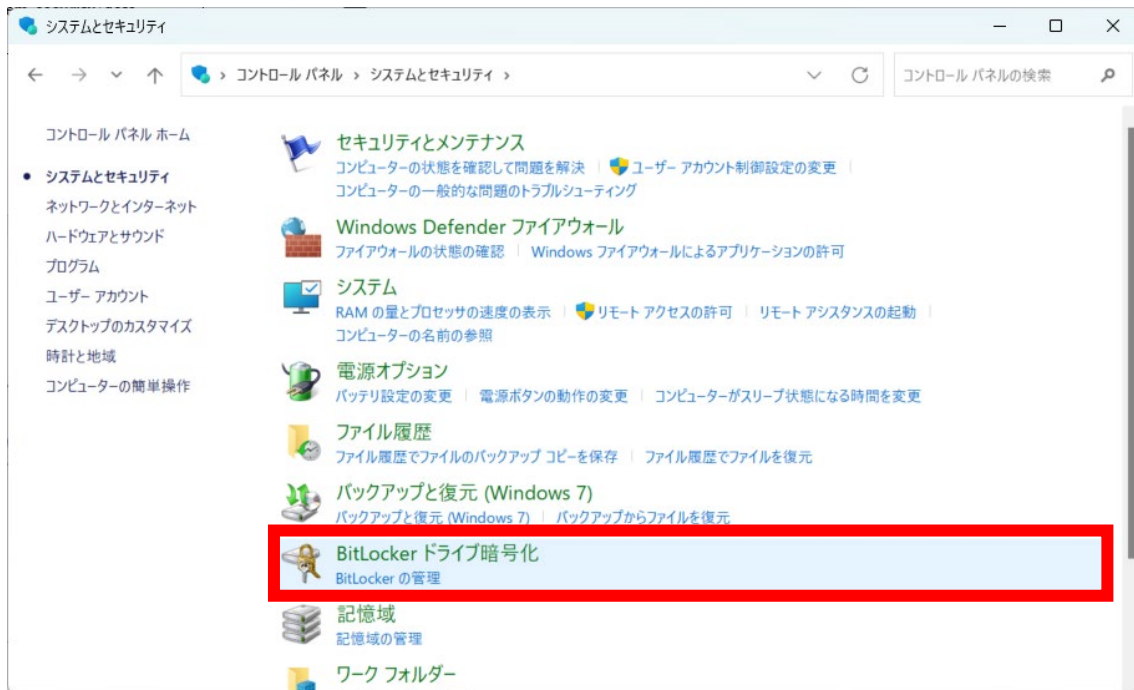
- 概要

BitLocker は、Windows OS で提供されているディスクを暗号化する仕組みです。ディスクを暗号化することにより、万が一 PC の紛失・盗難が発生した場合に、PC からデータ取り出されるリスクを低減することができます。なお、Windows 10/11 Home エディションでは提供されません。

- 導入方法

コントロールパネルを開き、システムとセキュリティ→BitLocker ドライブ暗号化に進んでください。





その後、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、指示に従って暗号化を行い、下記のように「BitLocker が有効です」と表示されれば設定完了です。



2.4.4. KeePass

対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	パスワード管理, パスワードポリシー
自社診断のための 25 項目	3
URL	https://keepass.info/news/n200120_2.44.html

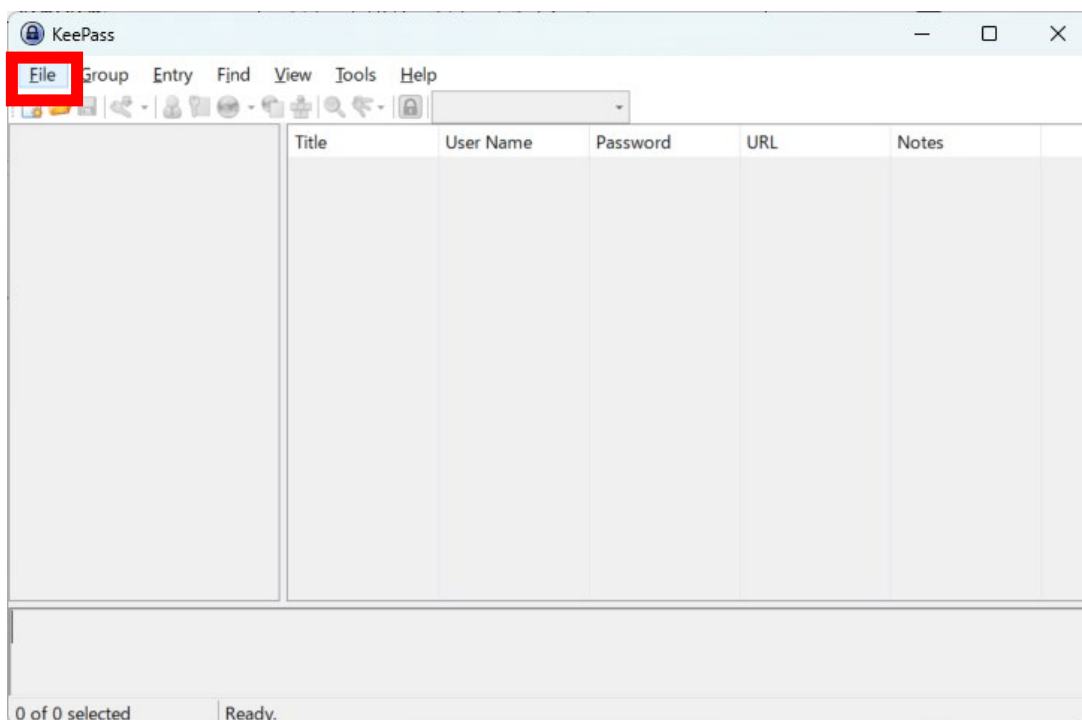
- 概要

KeePass はフリーでオープンソースのパスワードマネージャーです。パスワードマネージャーを利用することにより、パスワードの管理や自動生成を行うことができます。これにより、パスワードの使いまわしの低減や複雑なパスワードポリシーを容易に利用することができます。

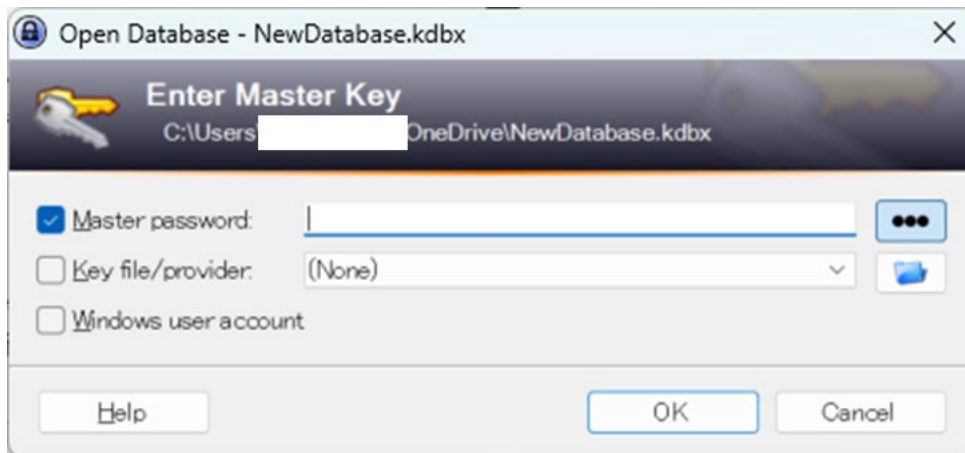
- 導入方法

公式サイト (https://keepass.info/news/n200120_2.44.html) から KeePass のインストーラをダウンロードし、インストールします。インストール完了後、実行します。

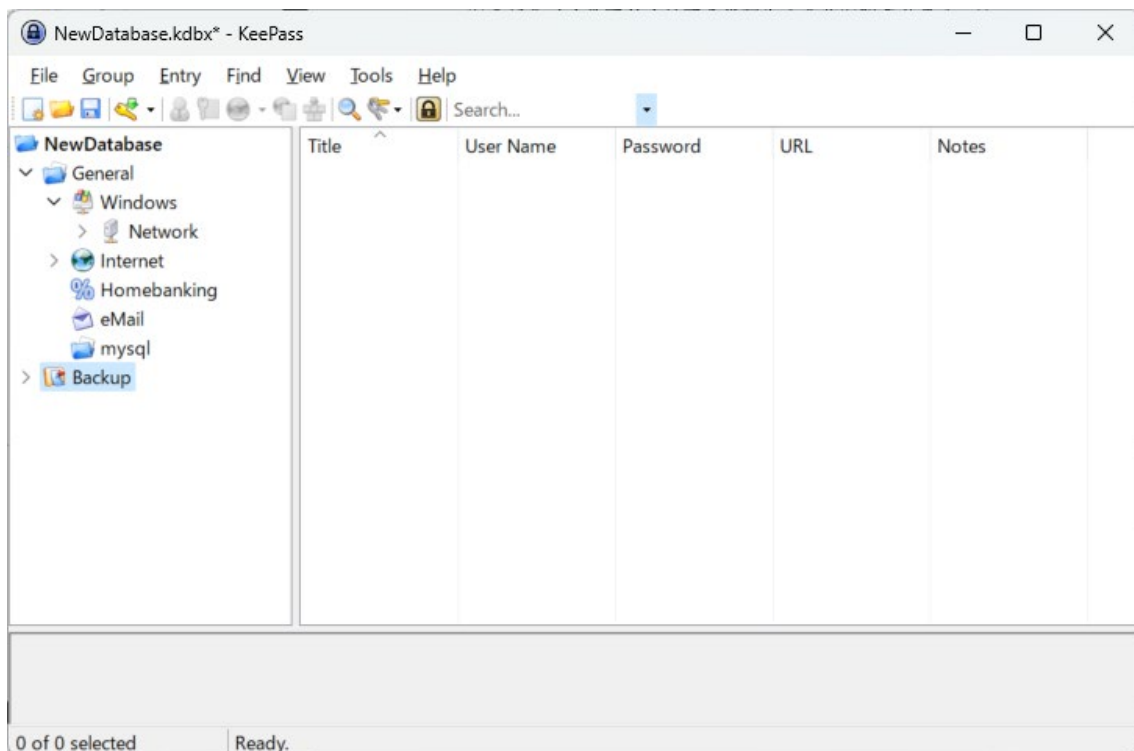
右上の File→New を選択し、データベースを作成します。その際に KeePass を開く際に必要となるマスターパスワードを設定する必要があります。



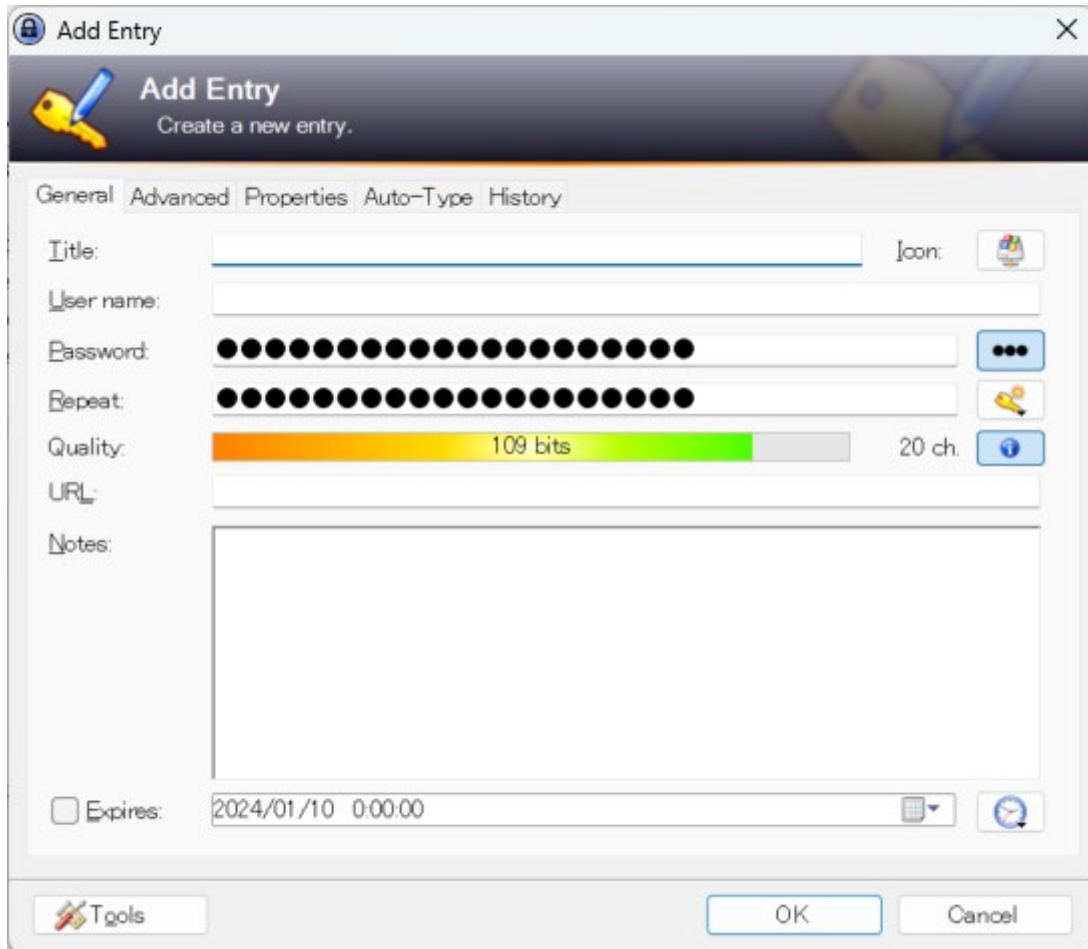
そして、データベースを開く際に、下記のように毎回マスターパスワードを入力する必要があります。



パスワードを入力後、下記のような画面になります。左側のメニューでパスワードをグルーピングすることができ、右側の部分で各種パスワードの一覧の登録等を行うことができます。試しに、右側の部分を右クリックし、Add Entry を押します。



下記のような画面が表示され、タイトル、ユーザ名、パスワード、URL 等を設定することができます。また、パスワード横の、鍵マークからパスワード生成のルールを決めることができます。

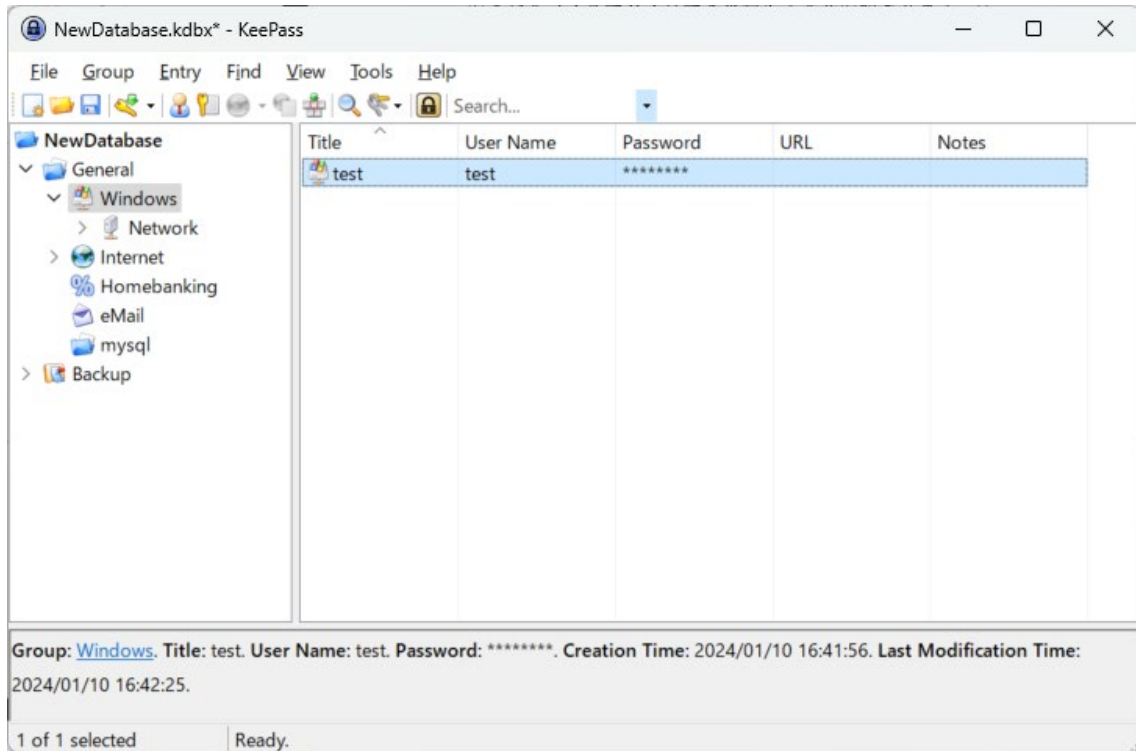


The screenshot shows a dialog box titled "Add Entry" with a close button (X) in the top right corner. Below the title bar is a header area with a key icon and the text "Add Entry" and "Create a new entry.". The main area has five tabs: "General", "Advanced", "Properties", "Auto-Type", and "History". The "General" tab is selected and contains the following fields:

- Title:** A text input field.
- User name:** A text input field.
- Password:** A text input field with 20 black dots for masking. To its right is a button with three dots.
- Repeat:** A text input field with 20 black dots for masking. To its right is a key icon button.
- Quality:** A progress bar showing "109 bits" in a green-to-yellow gradient. To its right is "20 ch." and a blue information button.
- URL:** A text input field.
- Notes:** A large text area.
- Expires:** A checkbox followed by a date/time field set to "2024/01/10 0:00:00" and a calendar icon.

At the bottom of the dialog, there is a "Tools" button with a wrench icon, and "OK" and "Cancel" buttons.

登録後、下記のように一覧で表示されダブルクリックすることによりパスワードがコピーされます。



2.4.5. Windows Defender ファイアウォール

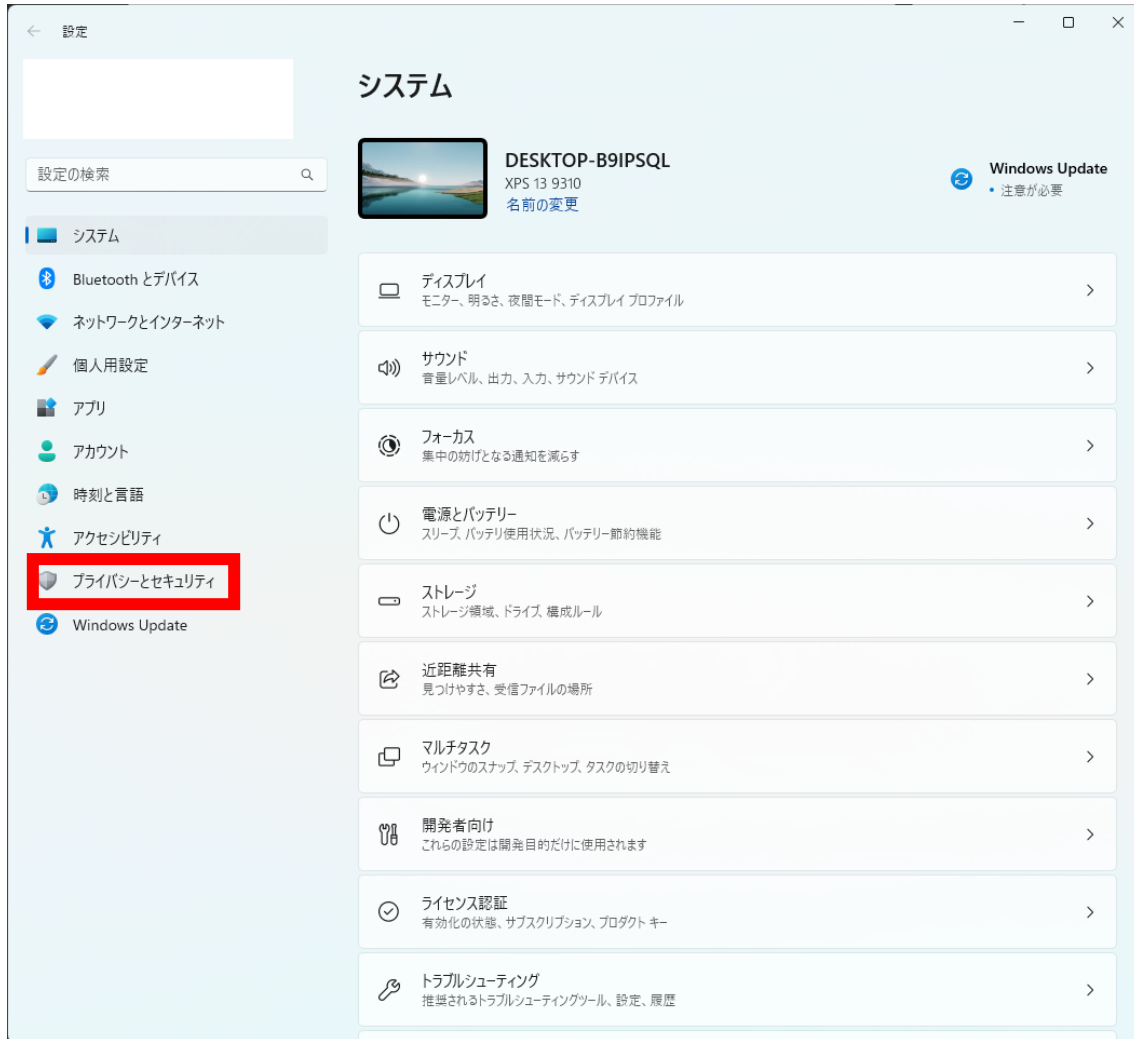
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	ファイアウォール
自社診断のための 25 項目	4
URL	https://support.microsoft.com/ja-jp/windows/microsoft-defender-%E3%83%95%E3%82%A1%E3%82%A4%E3%82%A2%E3%82%A6%E3%82%A9%E3%83%BC%E3%83%AB%E3%82%92%E6%9C%89%E5%8A%B9%E3%81%BE%E3%81%9F%E3%81%AF%E7%84%A1%E5%8A%B9%E3%81%AB%E3%81%99%E3%82%8B-ec0844f7-aebd-0583-67fe-601ecf5d774f

- 概要

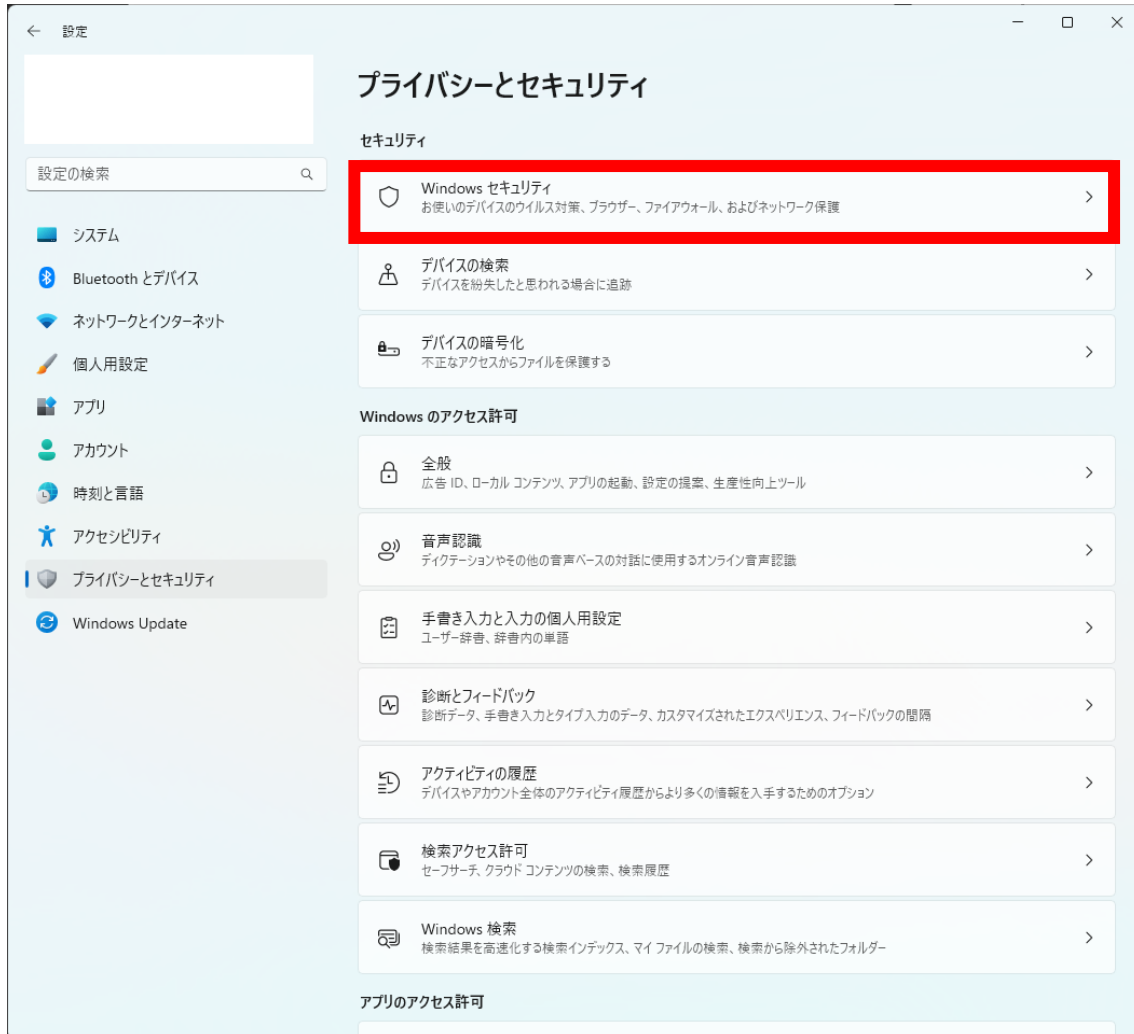
Windows Defender ファイアウォールは、Windows 標準で搭載されているファイアウォールでクライアント PC を不正なアクセスから保護するものです。

● 導入方法

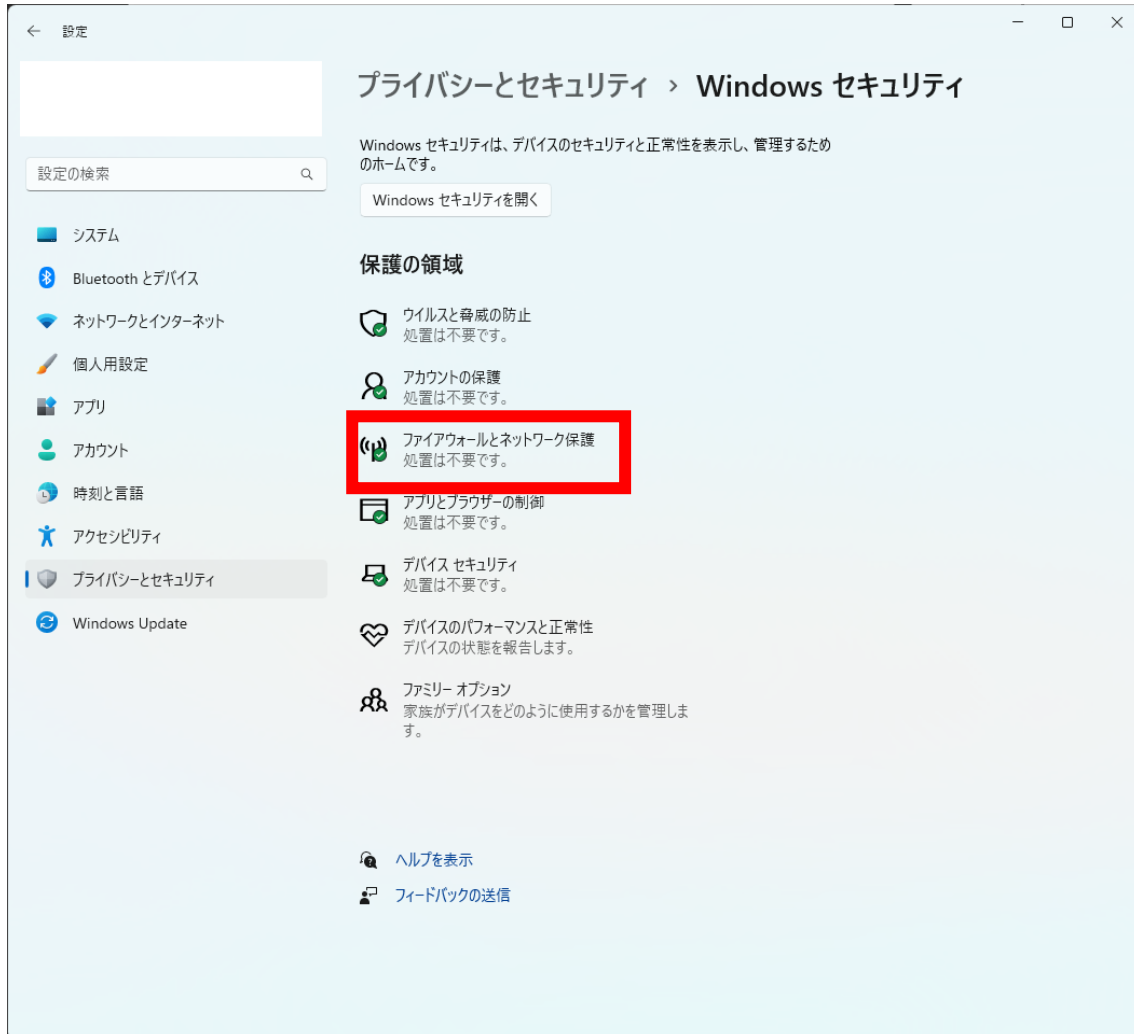
設定を開き、プライバシーとセキュリティを選択します。



Windows セキュリティを選択します。



ファイアウォールとネットワーク保護を選択します。



この画面でファイアウォールが有効になっていない場合、有効になっていないものをクリックし有効に変更します。



2.4.6. Windows Hello

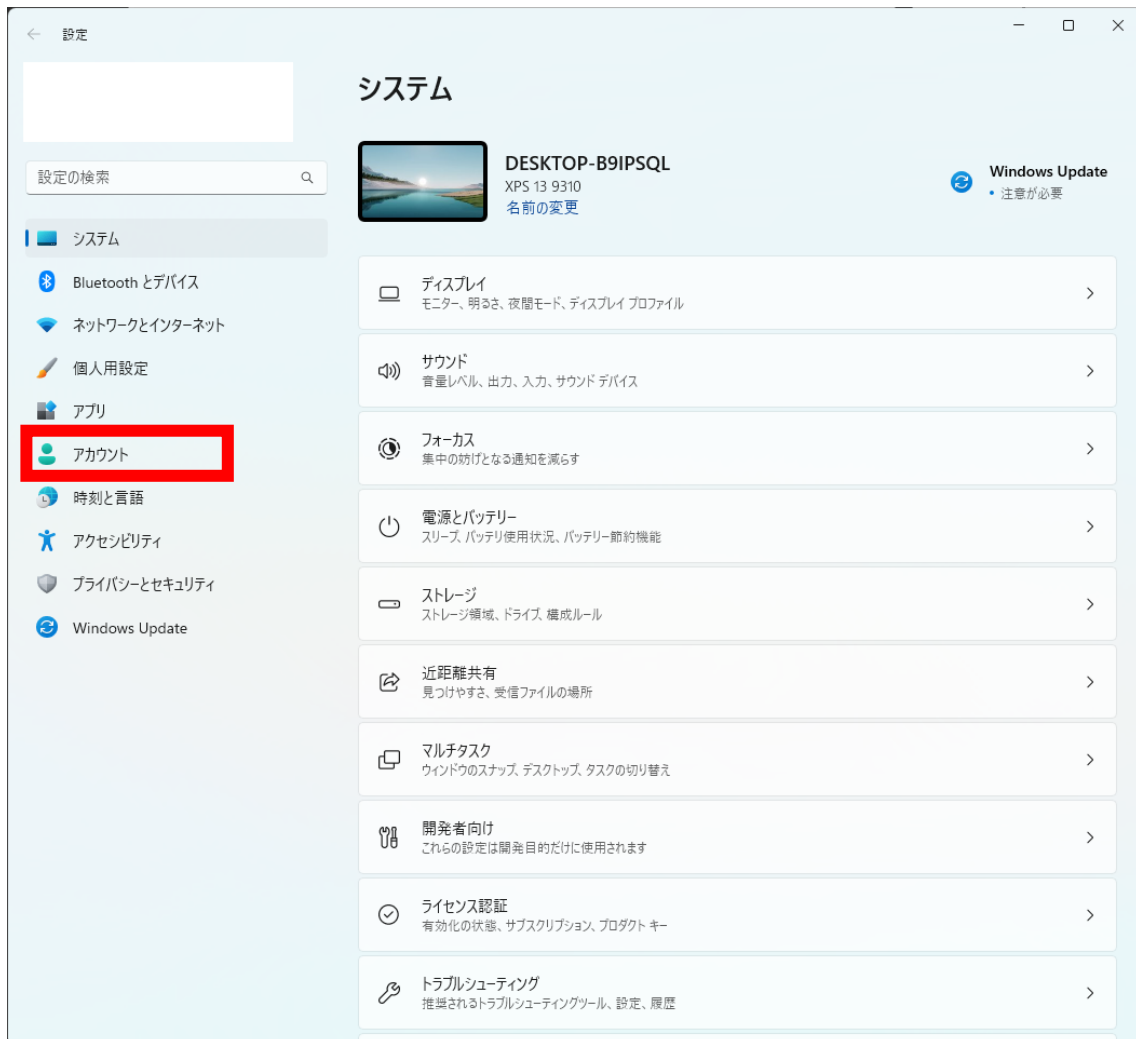
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	認証補助
自社診断のための 25 項目	4
URL	https://support.microsoft.com/ja-jp/windows/windows-hello-%E3%81%AE%E6%A6%82%E8%A6%81%E3%81%A8%E3%82%BB%E3%83%83%E3%83%88%E3%82%A2%E3%83%83%E3%83%97-dae28983-8242-bb2a-d3d1-87c9d265a5f0

- 概要

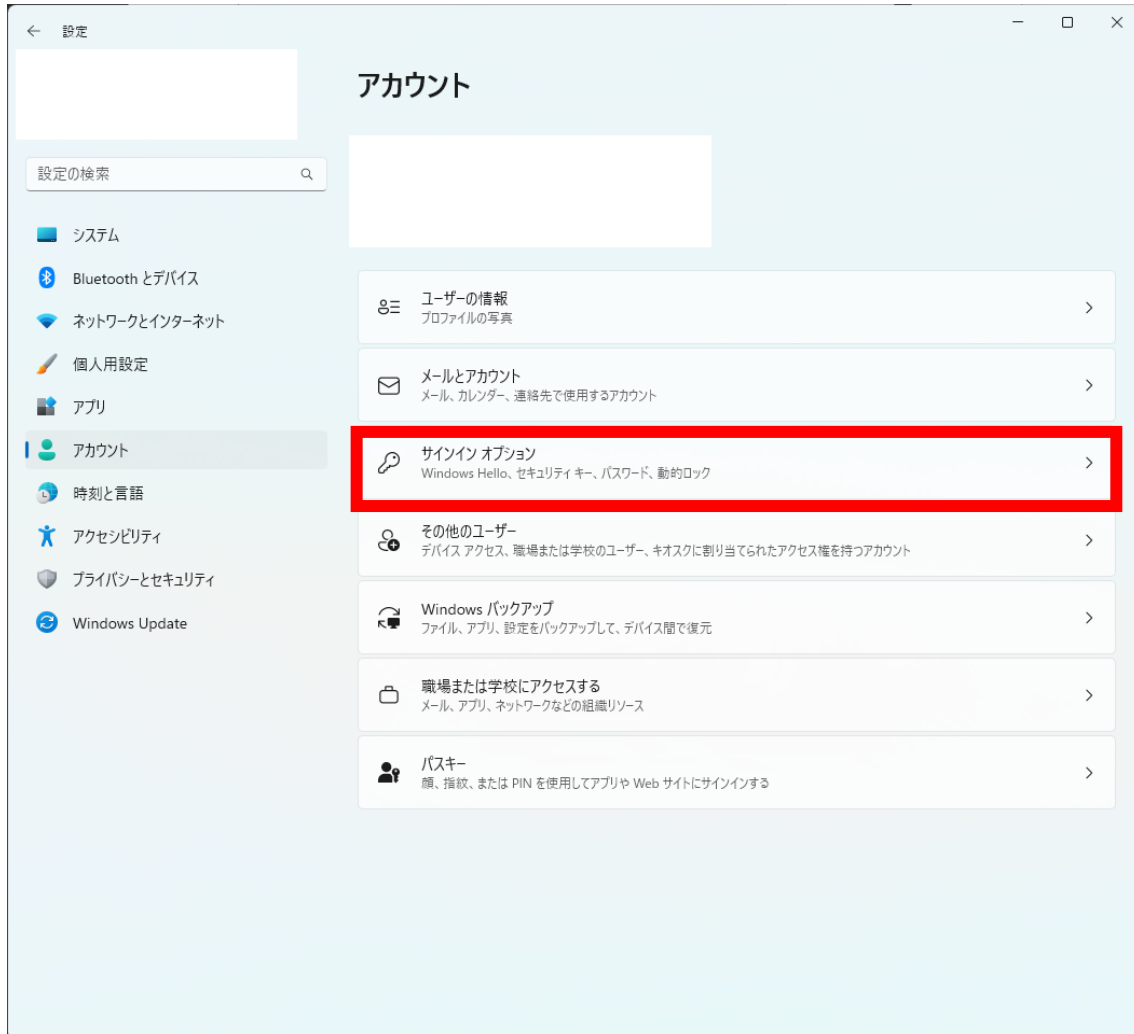
Windows Hello は、PIN や顔認識、指紋を使ってデバイスにログインする方法です。これを用いることでログイン時のパスワード入力の手間を低減することができます。

● 導入方法

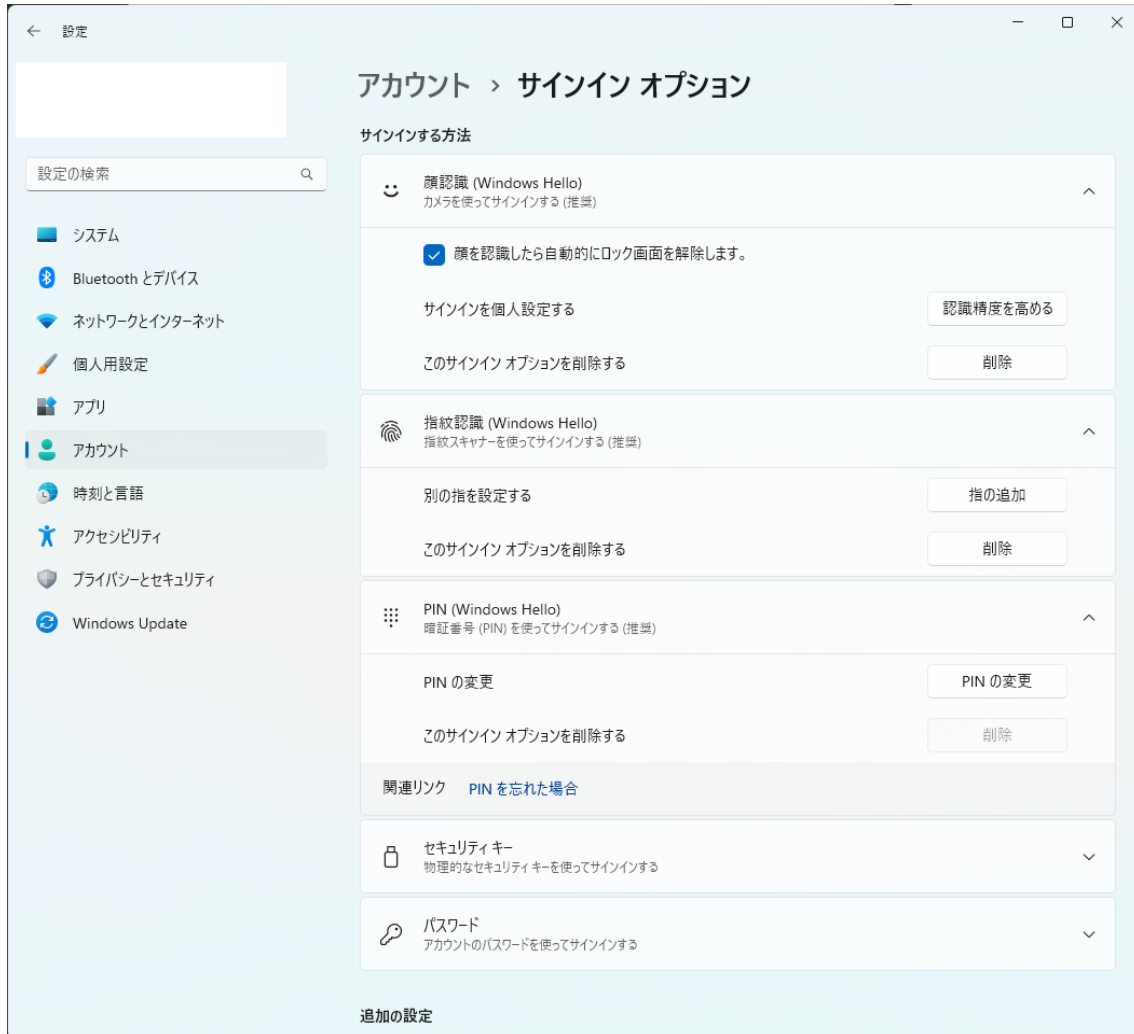
設定を開き、アカウントを選択します。



そして、サインインオプションを選択します。



顔認証、指紋認証、PIN のいずれかで設定を行います。



2.4.7. 7-zip

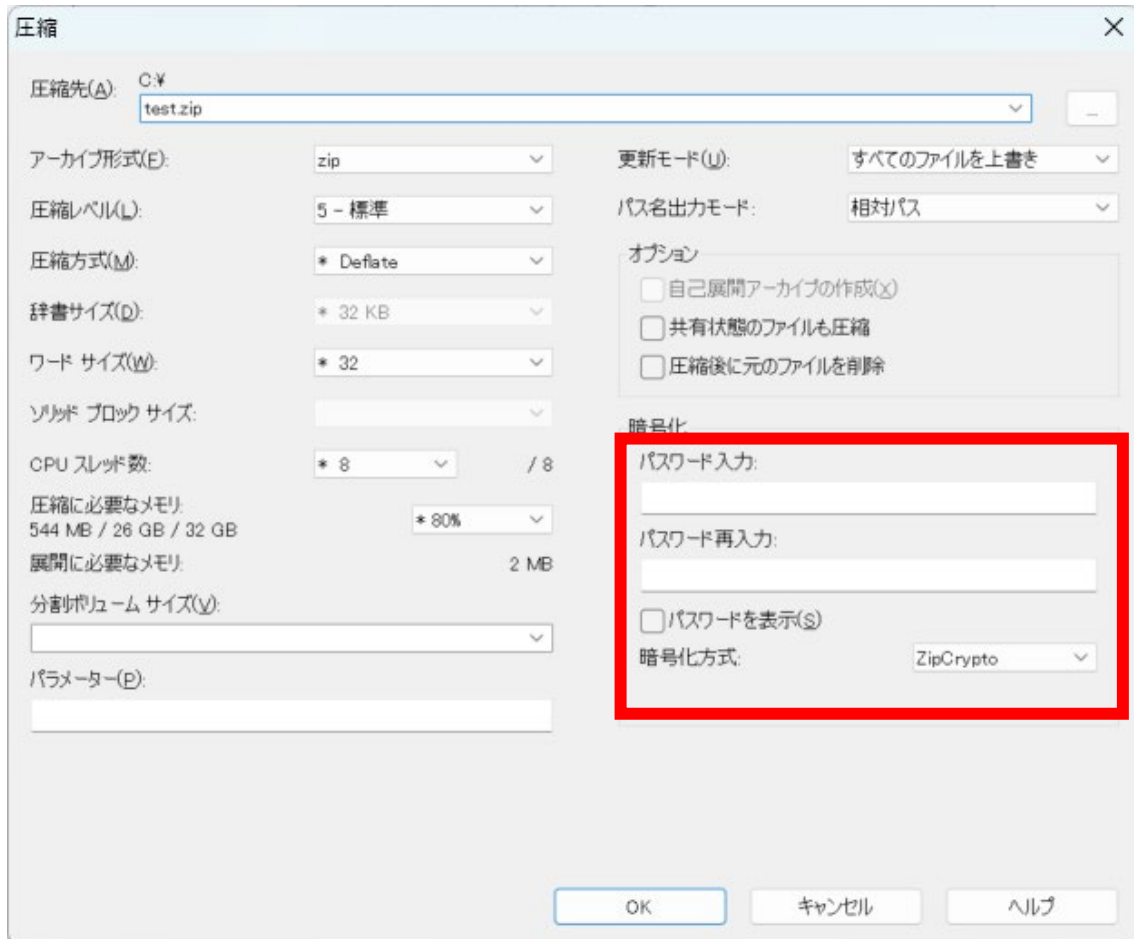
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	圧縮・解凍
自社診断のための 25 項目	8
URL	https://7-zip.opensource.jp/

- 概要

フリーでオープンソースの圧縮解凍ソフトです。様々な形式のファイルを圧縮解凍することができ、パスワードを設定した ZIP 等を生成することができます。ただし、様々な形式のファイルの解凍やパスワード付き ZIP の生成の必要がなければ Windows 標準の物のみで良いです。

- 導入方法

公式サイト(<https://7-zip.open-source.jp/>)からダウンロードし、インストーラを実行します。インストール後、ZIP を暗号化して圧縮する際は、圧縮するファイルを右クリックし、7-Zip→圧縮を選択します。暗号化する際のパスワードを設定し、OK を押すことで暗号化 ZIP を作成することができます。



2.4.8. 脅威情報の取得

対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	脅威情報の取得
自社診断のための 25 項目	5
URL	-

● 概要

社内で利用している Teams など脅威情報の RSS を取得することにより、脅威情報をリアルタイムに収集することができます。それらを確認し、対象となるものが社内にあるかを確認することにより、既知の脆弱性に対するリスクを低減することができます。

RSS の取得元の例

- <https://www.jpccert.or.jp/> の 注意喚起
<https://www.jpccert.or.jp/rss/jpccert.rdf>
- <https://www.jpccert.or.jp/> の 脆弱性関連情報
<https://jvn.jp/rss/jvn.rdf>
- <https://www.ipa.go.jp/security/index.html> の 重要なセキュリティ情報
<https://www.ipa.go.jp/security/alert-rss.rdf>

- 導入方法

Teams の場合、通知用のチャンネルを作成し、アプリから RSS を追加します。そして、通知先のチャンネルを設定します。そして、各 RSS の情報を入力し、保存を押します。

 **RSS** フィードバックの送信

RSS コネクタは、RSS フィードからの定期的な更新情報を送信します。コネクタを設定するには、更新情報を受け取りたいフィードのアドレスが含まれているリンクを入力します。


*** が付いているフィールドは必須です**
RSS 接続の名前を入力してください。 *

RSS フィードのアドレス *

ダイジェストの頻度
ダイジェストを受信する頻度を選択します。

6 時間

設定後、下記のようにチャンネルに投稿されます。

 **RSS** 13:52

[Intel製品に複数の脆弱性（2024年1月）](#)
Intelから各製品向けのアップデートが公開されました。

[Siemens製品に対するアップデート（2024年1月）](#)
Siemensから各製品向けのアップデートが公開されました。

[Cambium Networks製ePMP Force 300-25におけるコードインジェクションの脆弱性](#)
Cambium Networksが提供するePMP Force 300-25には、コードインジェクションの脆弱性が存在します。

[表示数を減らす](#)

2.4.9. フォーマットツール

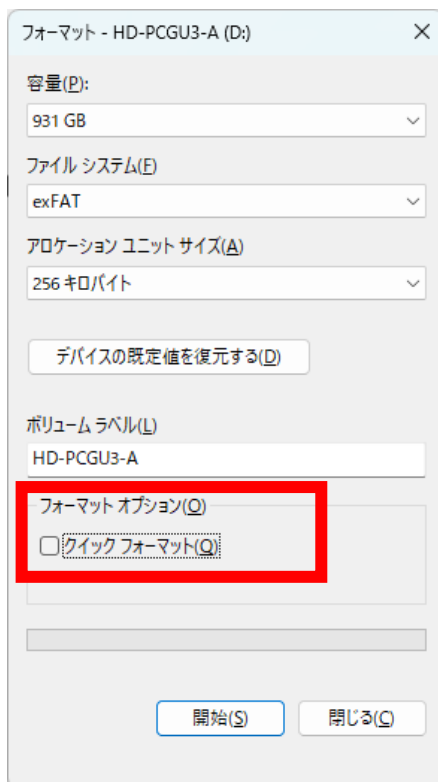
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	フォーマットツール
自社診断のための 25 項目	18
URL	-

● 概要

利用が終わったデータを保存している外付け HDD や USB メモリは、紛失や盗難のリスクを避けるためにフォーマットする必要があります。また、クイックフォーマットでは、データを復元できる恐れがあるため、フルフォーマットを行うことを推奨します。

● 導入方法

エクスプローラーからフォーマットする USB メモリ等を、右クリックし、フォーマットを選択します。その後、クイックフォーマットのチェックを外し、フォーマットを行います。



2.4.10. Thunderbird

対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
対策/対象	メール関連
自社診断のための 25 項目	6, 7
URL	https://www.thunderbird.net/ja/

● 概要

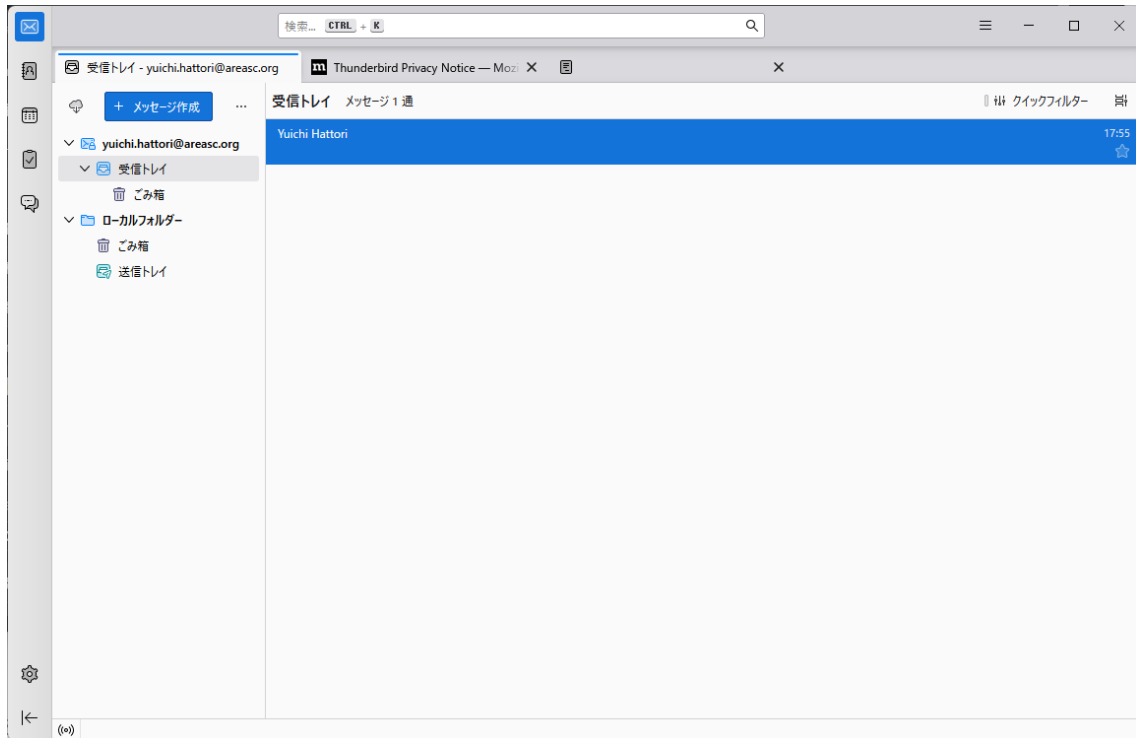
Thunderbird は、オープンソースでフリーのメーラーです。様々な拡張機能が公開されており、それらを用いることで誤送信防止等のセキュリティ対策を行うことができます。

● 導入方法

公式サイト(<https://www.thunderbird.net/ja/>)からインストーラをダウンロードし、実行します。インストール完了後、起動し、利用しているメールの設定を登録します。



設定完了後、メールの送受信が行えます。※セキュリティに関する設定は設定項目の方で説明します。



2.5. 推奨する設定項目詳細

推奨するツールの詳細について説明します。

2.5.1. スクリーンロック

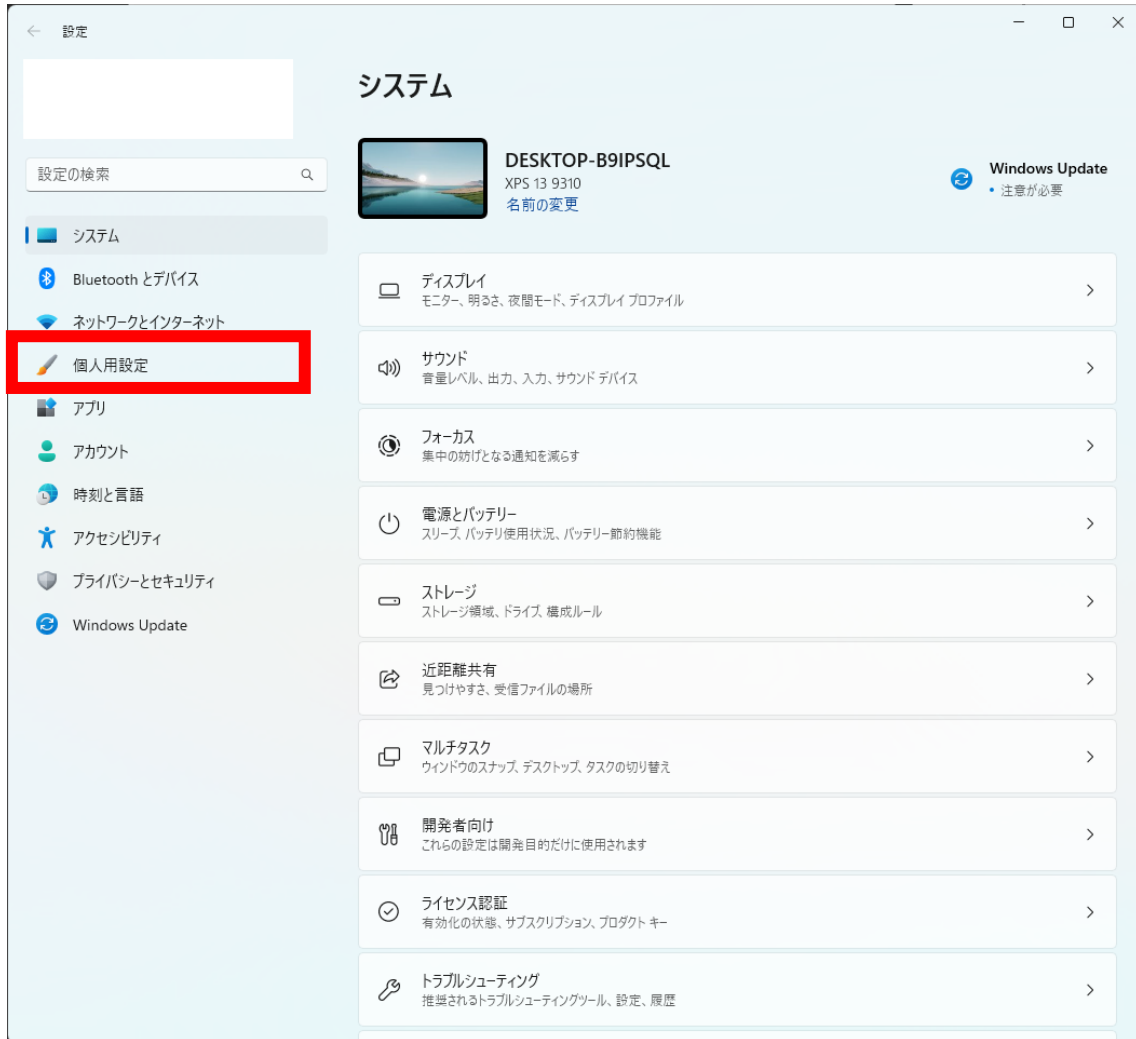
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	一定時間操作がない場合スクリーンロックをかける
自社診断のための 25 項目	14
対象ツール	OS

● 概要

スクリーンロックは、離席時に PC を不正に利用されないようにロックする機能です。離席時にロックすることはもちろんですが、それを忘れた場合に一定時間操作がない状態の際にロックをかける設定を入れることにより、離席時に不正利用されるリスクを低減することができます。

● 導入方法

設定を開き、個人用設定を選択します。



次にスクリーンセーバーを選択します。



待ち時間と再開時にログオン画面に戻るにチェックを入れ適用ボタンを押せば
設定完了です。



2.5.2. フィッシングメール対策

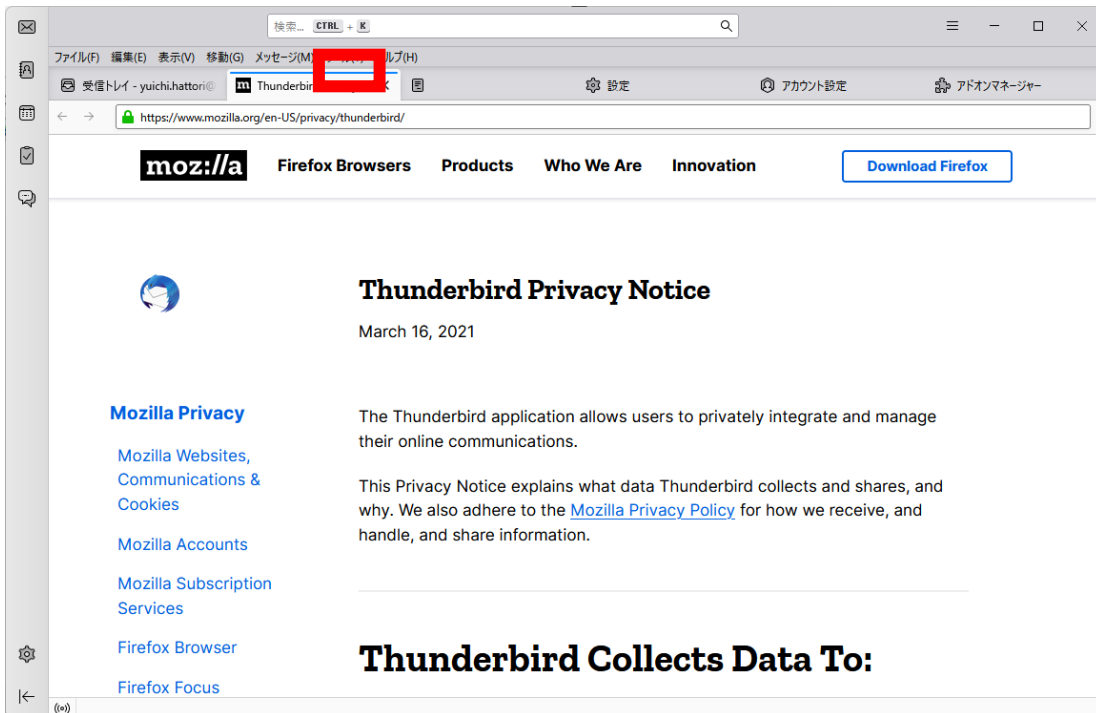
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	フィッシングメール対策機能を有効にする
自社診断のための 25 項目	6
対象ツール	Thunderbird

● 概要

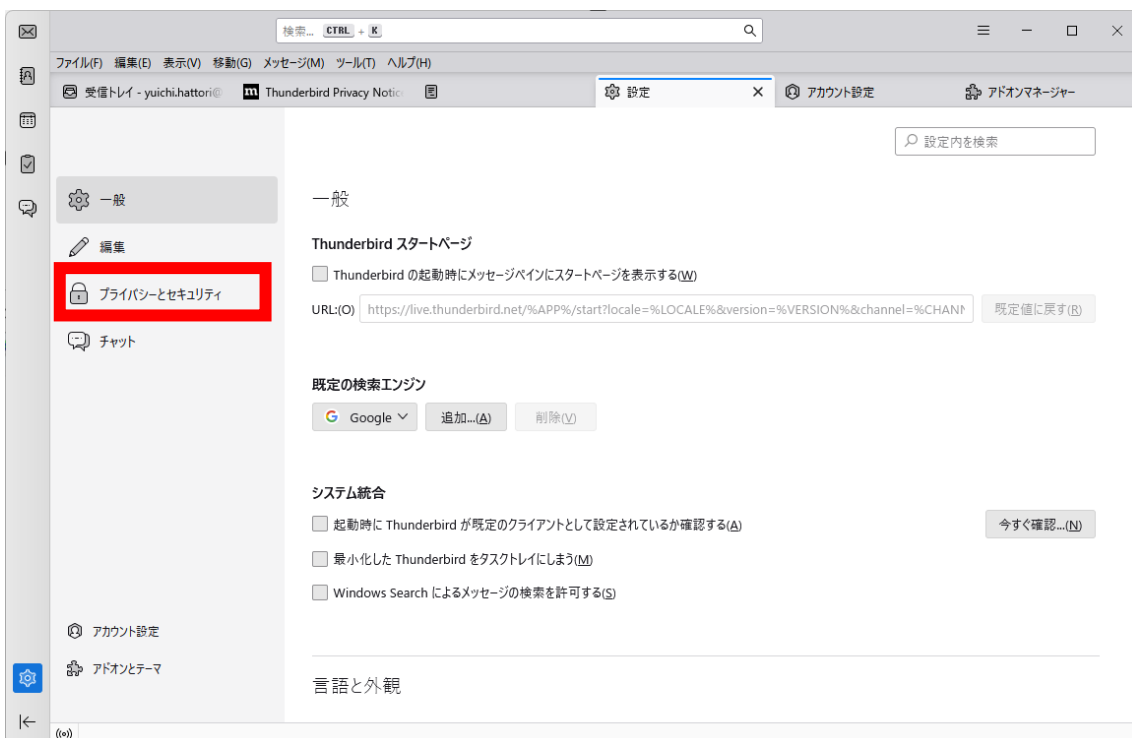
現在、フィッシングメールは高度化しており、様々な方法で利用者を騙してメールのリンクにアクセスさせたり、QRコードを読み込ませたりします。利用者の注意だけでは、対策にも限界があるため、メーカーに搭載されているフィルタリング機能等を有効にすることで、フィッシングメールに対して一定の効果が期待できます。

● 導入方法

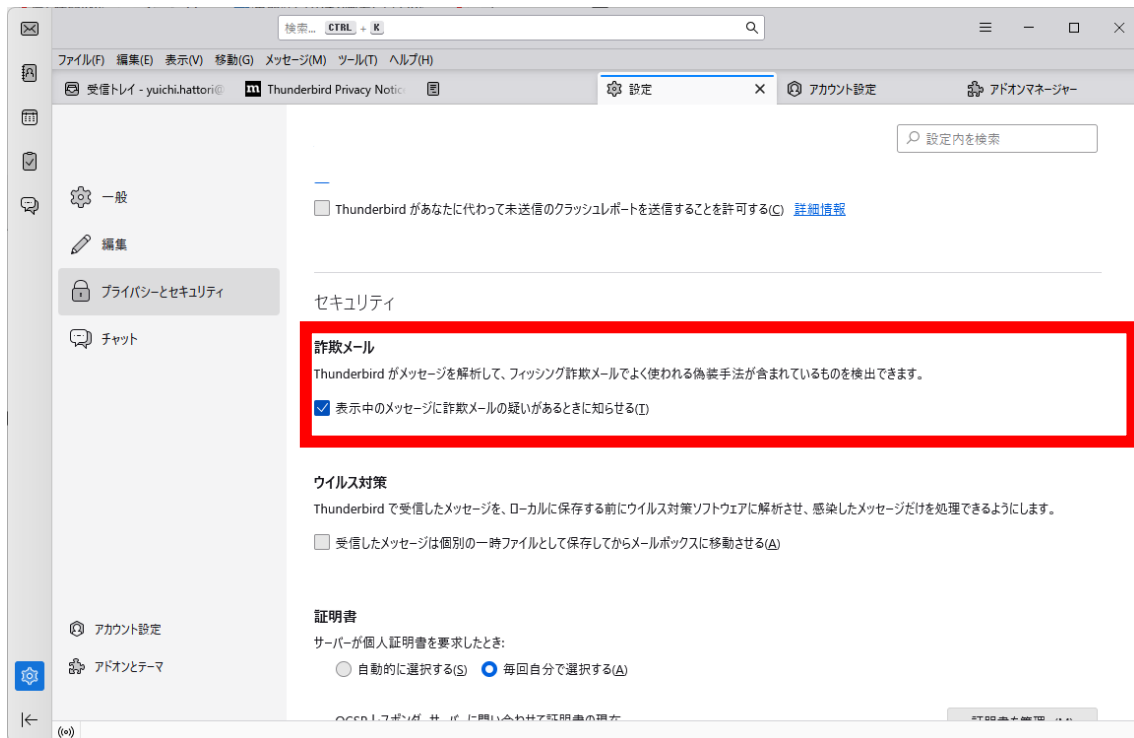
Thunderbird を開き、ツール→設定を選択します。



プライバシーとセキュリティを選択します。



詐欺メールの表示中のメッセージに詐欺メールの疑いがあるときに知らせるにチェックを入れれば設定完了です。



2.5.3. メールの誤送信防止

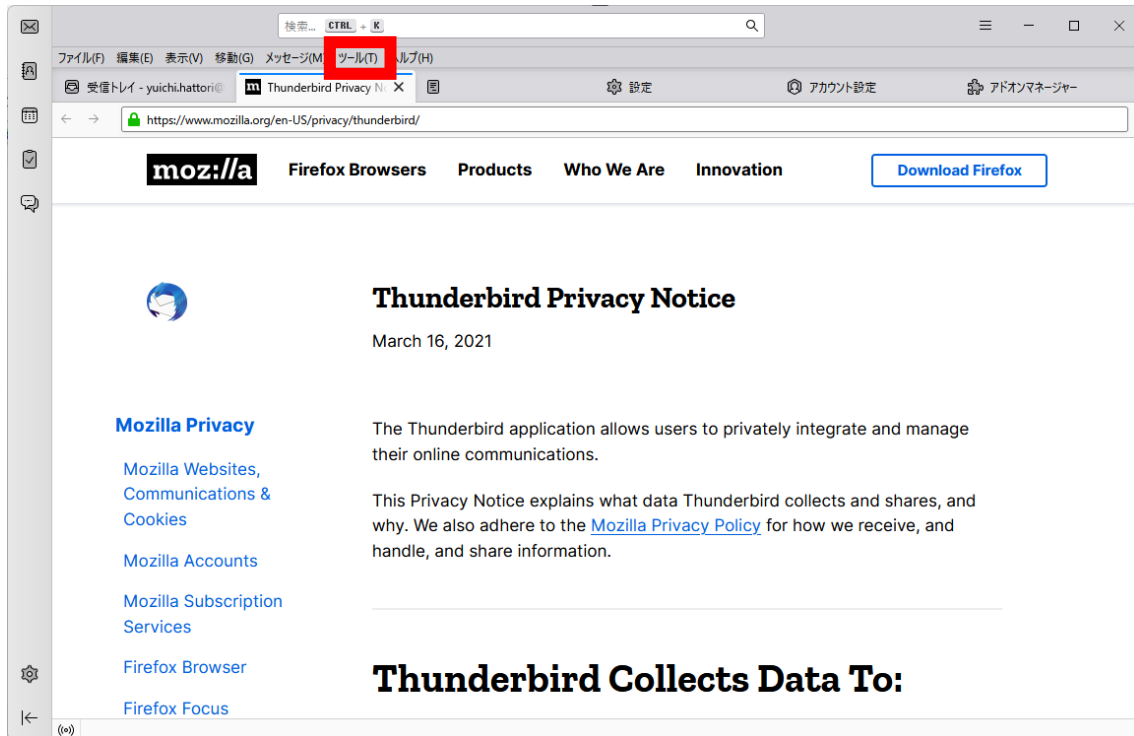
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	誤送信防止機能を有効にする
自社診断のための 25 項目	7
対象ツール	Thunderbird

- 概要

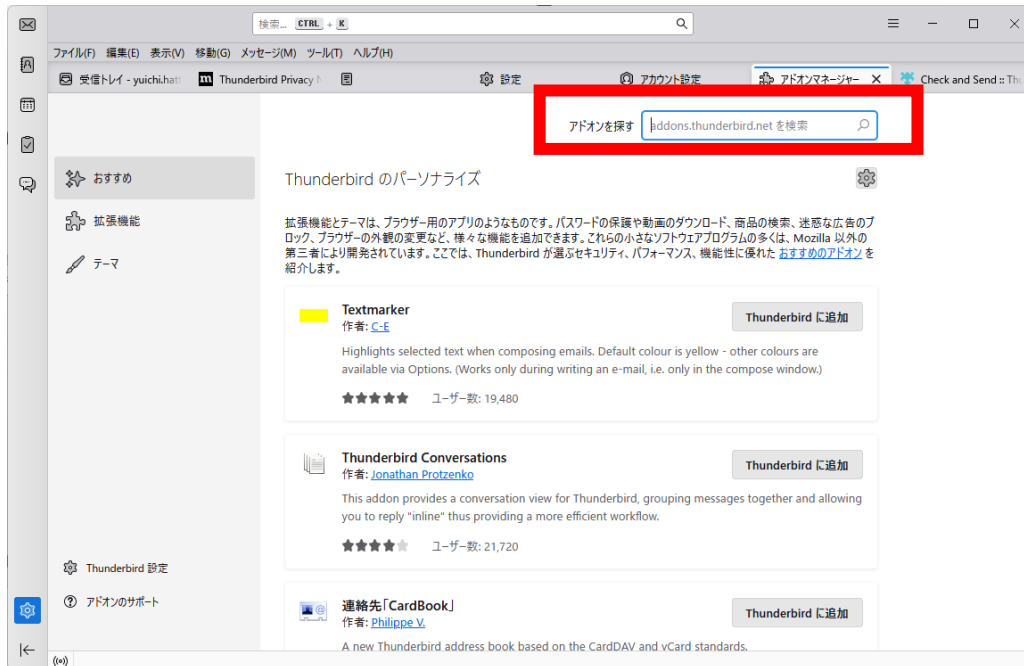
BCC と間違えて CC で送って、メールアドレスを漏えいしたり、宛先を間違えてメールを送り重要情報を漏えいするなどメールの誤送信に関する情報漏えい事例はあとを絶ちません。メーラー側で誤送信防止の機能を有効にすることで、それらのリスクを低減します。

● 導入方法

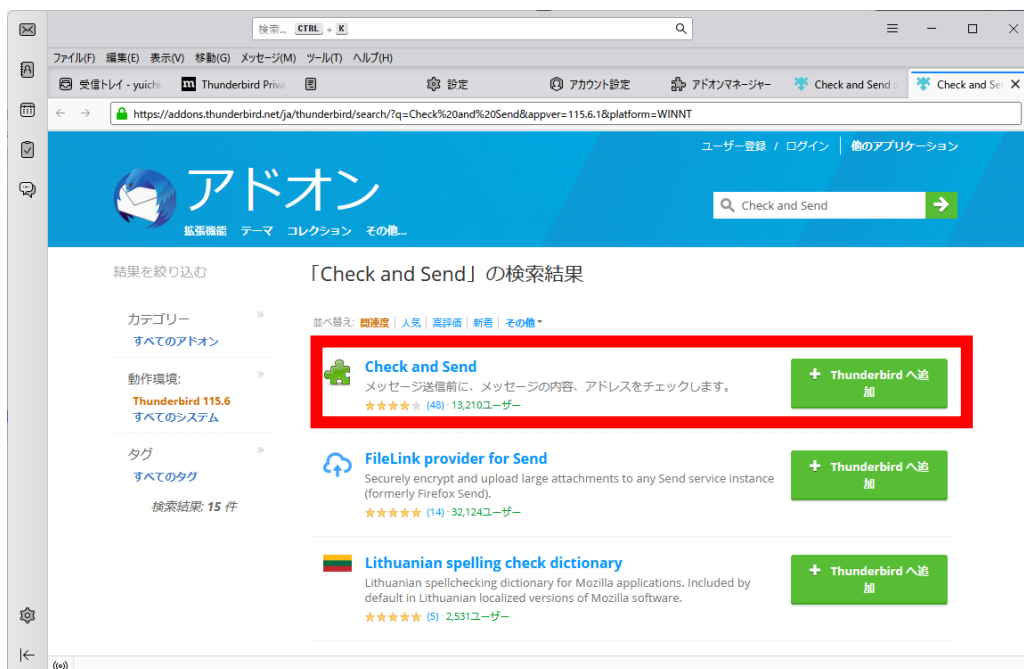
まずは、Thunderbird を開き、ツール→アドオンとテーマを選択します。



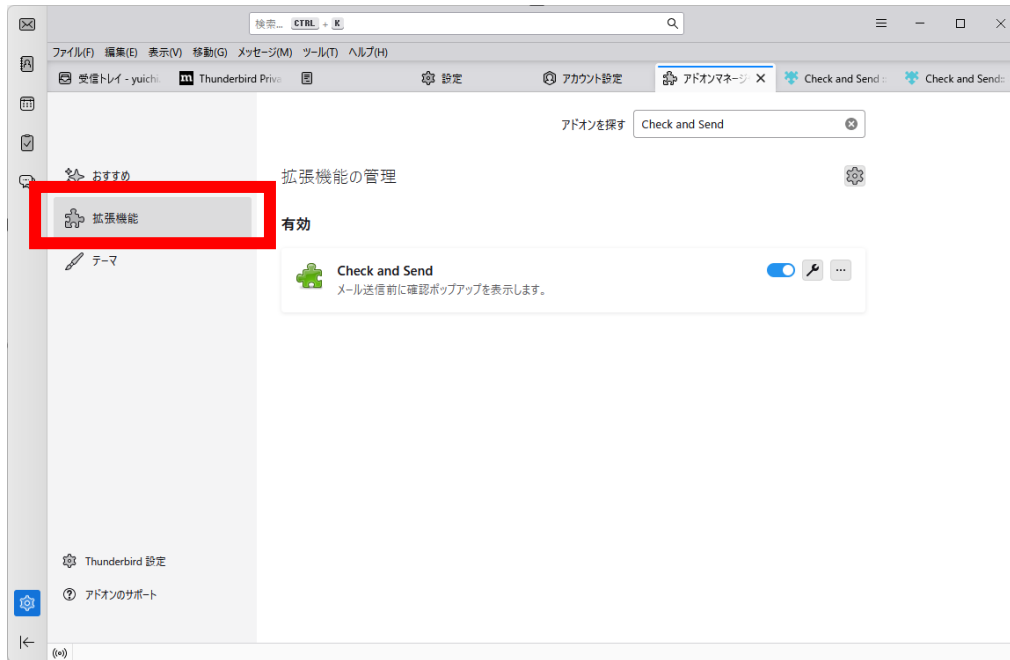
アドオンを探すに「Check and Send」と入力し確定します。



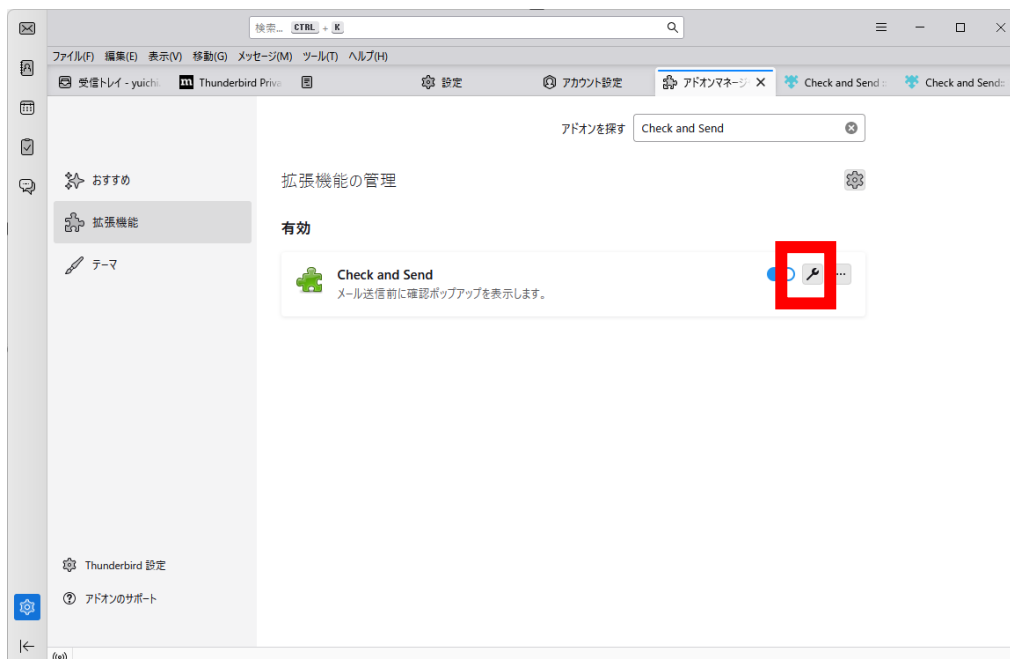
「Check and Send」を追加します。



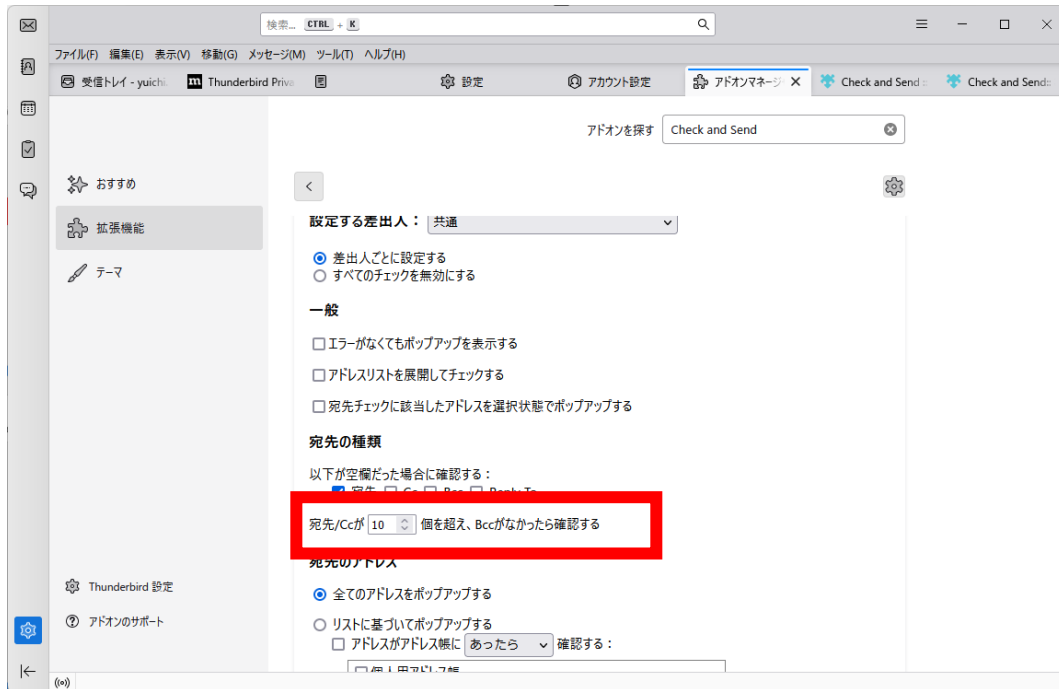
先ほどと同様にツール→アドオンとテーマへ移動し、拡張機能を選択します。



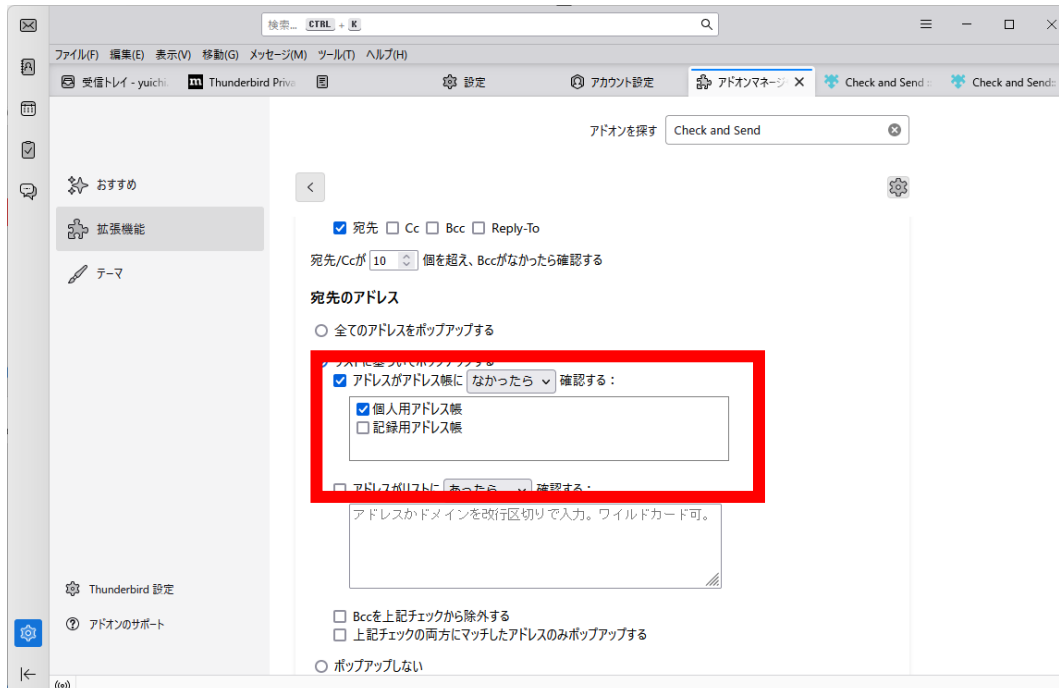
Check and Send の設定画面に移動します。



例として、いくつか設定を行います。宛先が多い場合に BCC 出ない場合、確認するようにします。宛先の種類の宛先が〇個を超え、BCC がなかったら確認するを 10 に設定します。



宛先のアドレスがアドレス帳になかったら確認するようにします。リストに基づいてポップアップするにチェックを入れアドレスがアドレス帳に・・・にチェックを入れなかったらに変更し、個人用アドレス帳にチェックを入れます。



遅延送信を有効にします。送信前に○秒待機するに 60 秒を設定します。



2.5.4. パスワードポリシー

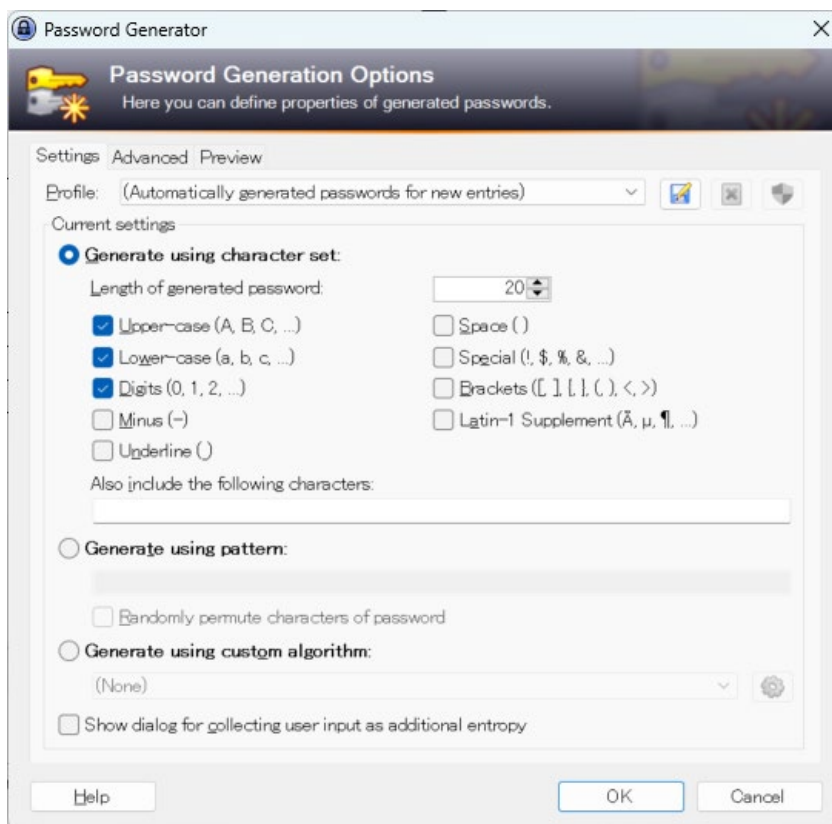
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	英大文字小文字+数字+記号で 10 桁以上
自社診断のための 25 項目	7
対象ツール	KeePass

- 概要

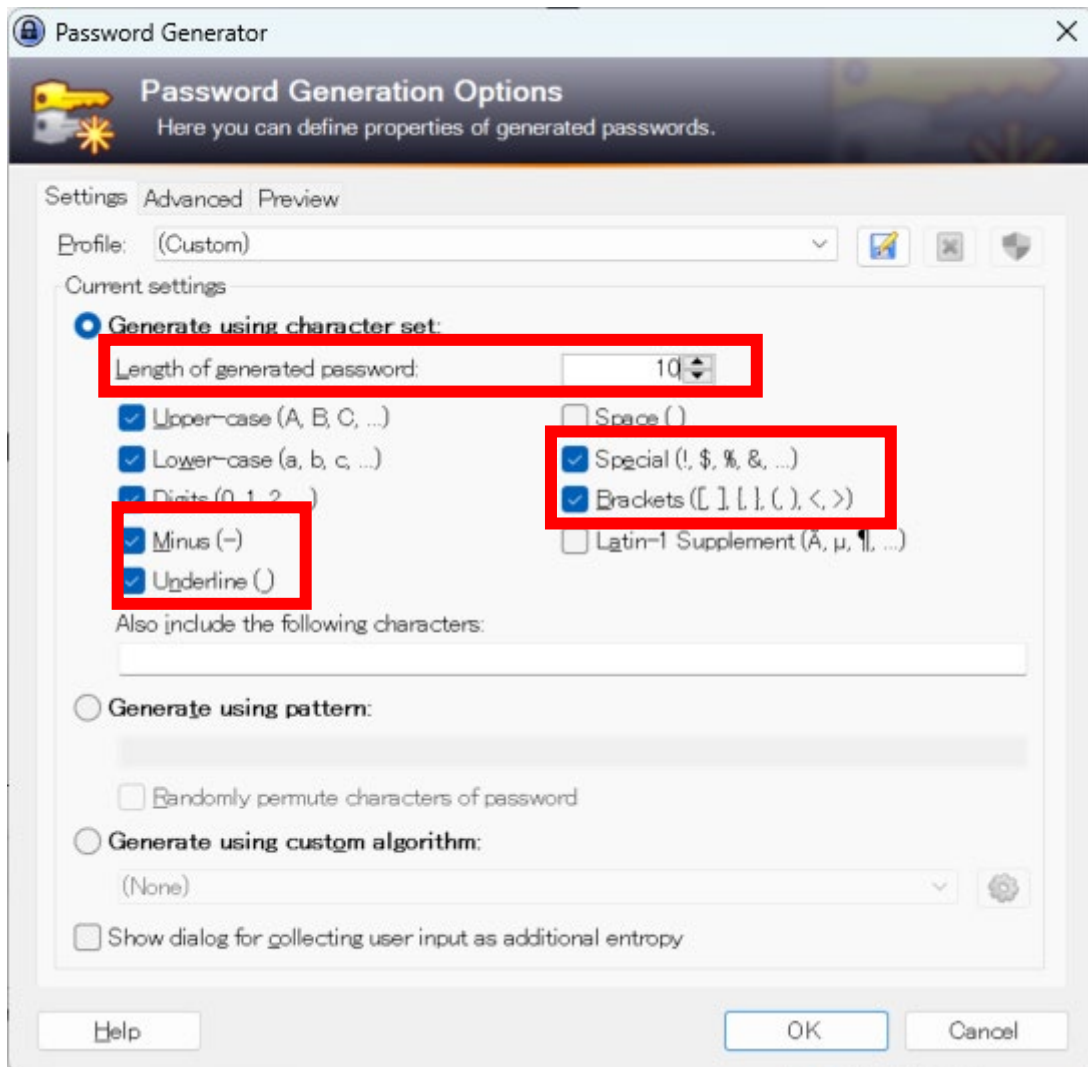
パスワードポリシーを導入することで安易なパスワードを利用することによるアカウント乗っ取り等のリスクを低減することができます。今回はパスワードマネージャーを利用したパスワードポリシーの設定について述べます。

- 導入方法

KeePass を開き、Tools→Generate Password を選択します。



Length of Generated password を 10、Minus, Underline, Special, Brackets のチェックを入れ OK を押せば、パスワード生成する際のルールが英大文字小文字+数字+記号で 10 桁以上で生成されるようになります。



2.5.5. ソフトウェア更新

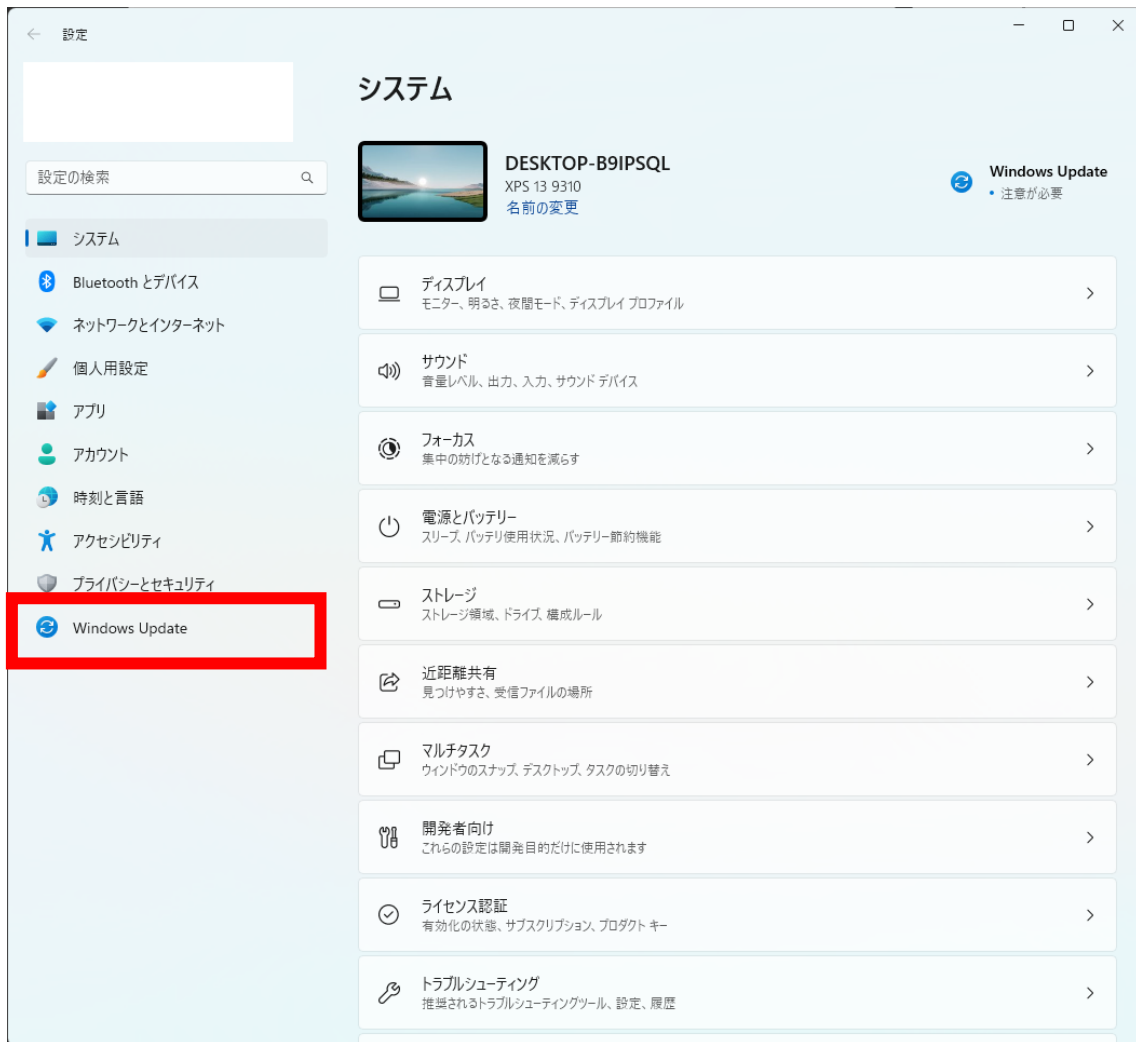
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	Windows Update のその他の Microsoft 製品の更新プログラムを有効にして実施
自社診断のための 25 項目	1
対象ツール	OS

- 概要

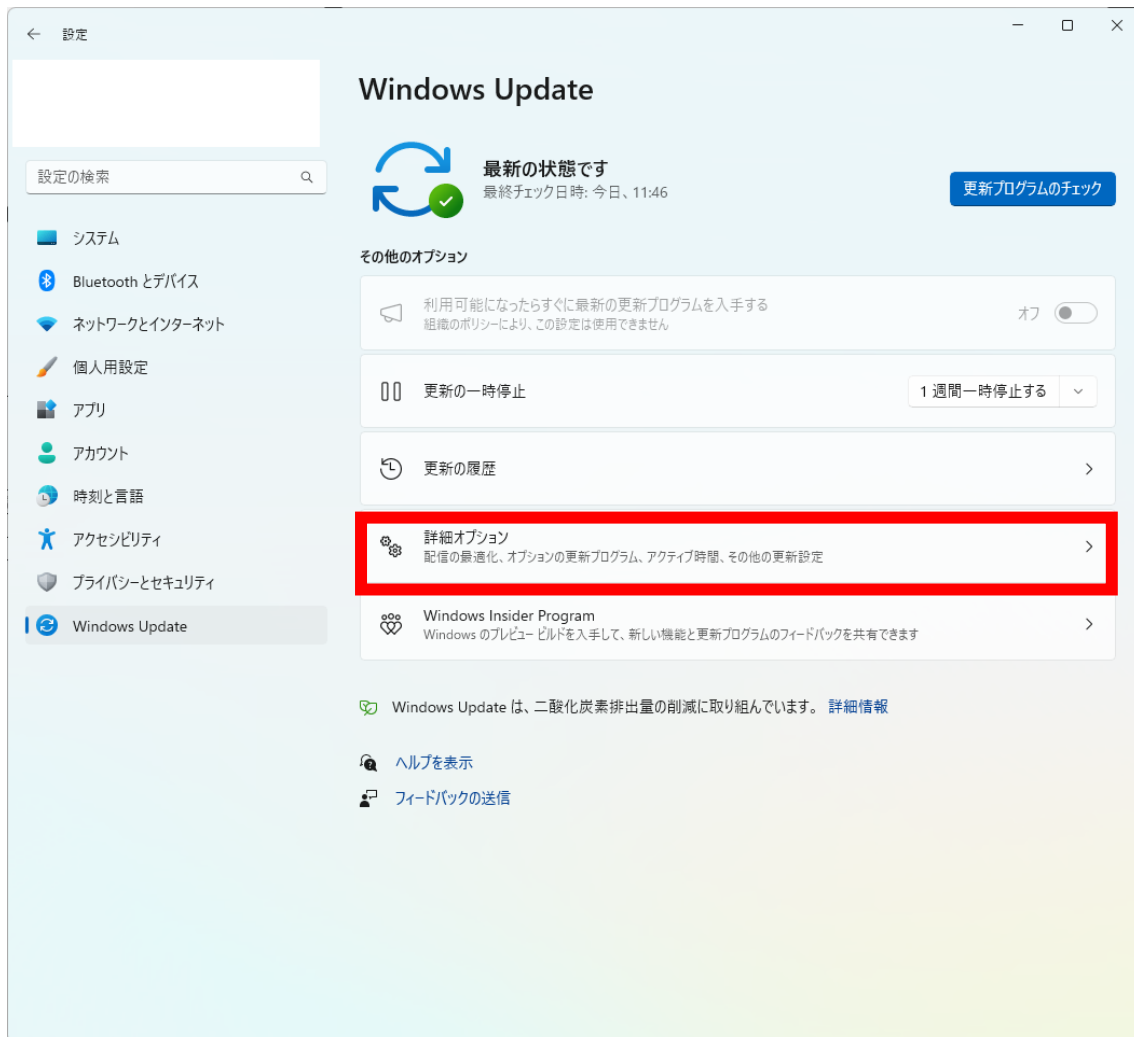
OS やその他ソフトウェアの自動更新は、既知の脆弱性に対する対策として有効です。最近の Windows Update では OS 以外の Microsoft 製品の更新も取得することができます。

● 導入方法

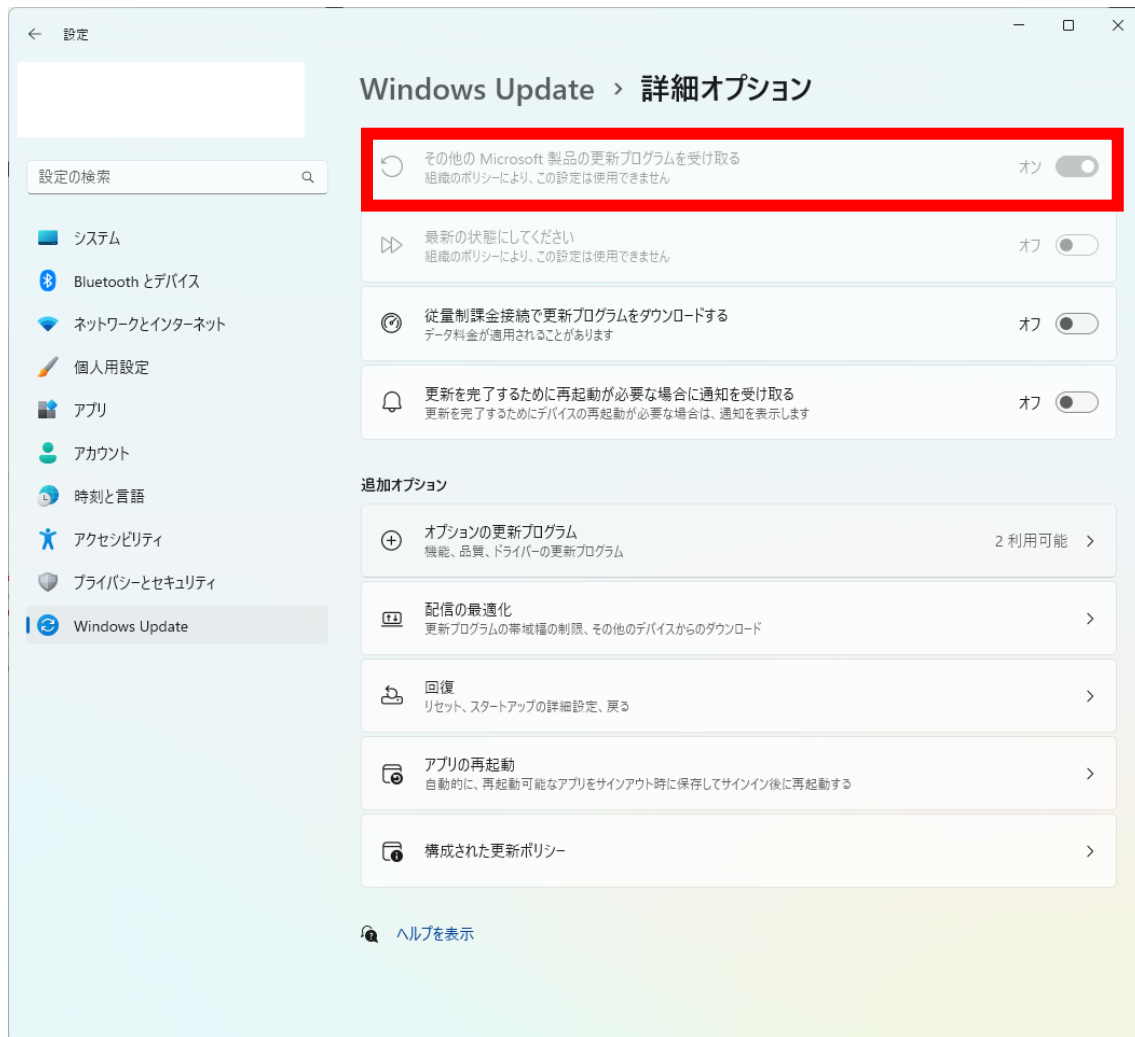
設定を開き、個人用設定を選択します。



次に詳細オプションを選択します。



その他の Microsoft 製品の更新プログラムを受け取るを ON にすれば設定完了です。



2.5.6. ファイアウォール

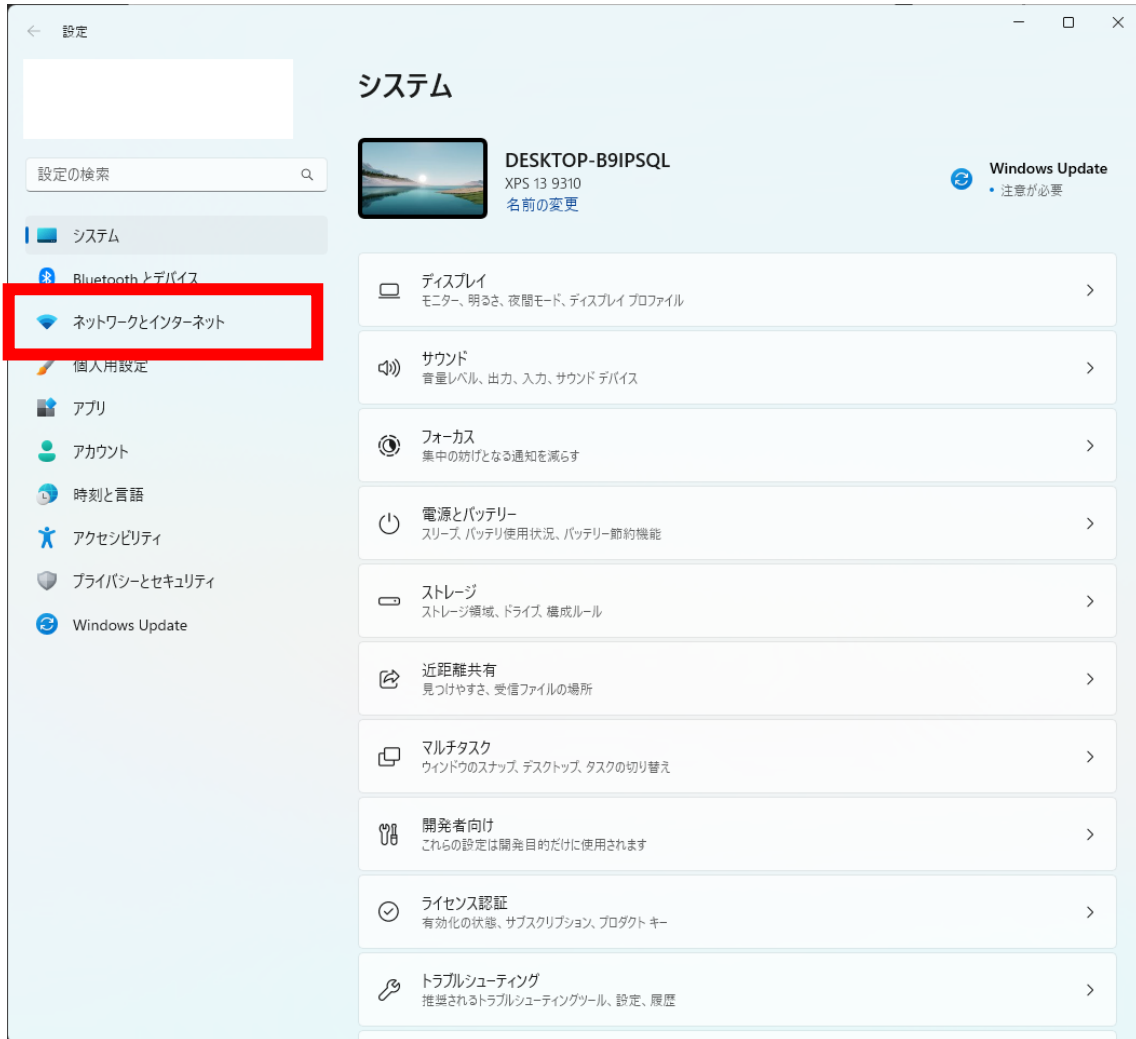
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	Windows 利用ポートの端末間アクセスは制限
自社診断のための 25 項目	4
対象ツール	OS

- 概要

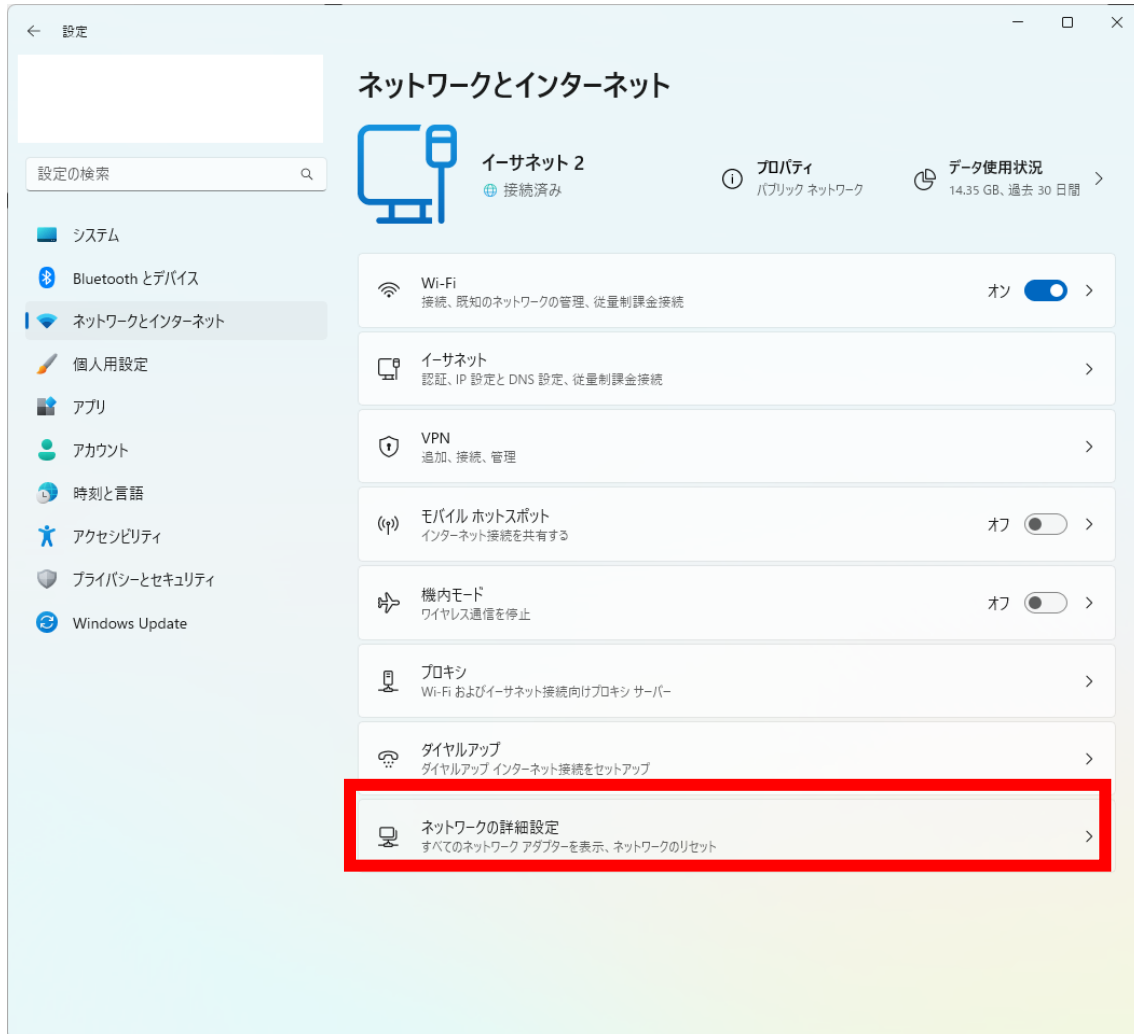
不要なファイル共有のための端末間アクセスは、マルウェアの感染等の際に攻撃者に悪用されるリスクがあるため制限することを推奨します。もし、共有が必要な場合は、適切な認証と必要最低限の設定を行きましょう。

● 導入方法

設定を開き、ネットワークとインターネットを選択します。



ネットワークの詳細設定を選択します。



共有の詳細設定を選択します。

The screenshot shows the Windows Settings application. The left sidebar contains various settings categories, with 'Network and Internet' selected. The main area is titled 'ネットワークとインターネット > ネットワークの詳細設定'. Under the 'ネットワーク アダプター' section, several network adapters are listed, each with a '無効にする' button. The 'その他の設定' section at the bottom contains several options, with '共有の詳細設定' (Shared Settings) highlighted by a red rectangular box. Below it are 'データ使用状況', 'ハードウェアと接続のプロパティ', and 'ネットワークのリセット'.

設定

設定の検索

システム

Bluetooth とデバイス

ネットワークとインターネット

個人用設定

アプリ

アカウント

時刻と言語

アクセシビリティ

プライバシーとセキュリティ

Windows Update

ネットワークとインターネット > ネットワークの詳細設定

ネットワーク アダプター

Wi-Fi 未接続 Killer(R) Wi-Fi 6 AX1650s 160MHz Wireless Network Adapter (201D2W)	無効にする
イーサネット 10 VirtualBox Host-Only Ethernet Adapter	無効にする
イーサネット 6 VirtualBox Host-Only Ethernet Adapter	無効にする
Bluetooth ネットワーク接続 Bluetooth Device (Personal Area Network)	無効にする
イーサネット 2 ネットワーク 4 Dell Giga Ethernet	無効にする
イーサネット 9 VirtualBox Host-Only Ethernet Adapter	無効にする

その他の設定

- 共有の詳細設定**
ネットワークの検出と共有の設定を変更する >
- データ使用状況 >
- ハードウェアと接続のプロパティ >
- ネットワークのリセット
すべてのネットワーク アダプターを出荷時の設定にリセットする >

関連設定

利用しているプロファイルのネットワーク探索とファイルとプリンターの共有をオフにします。



2.5.7. アカウント管理

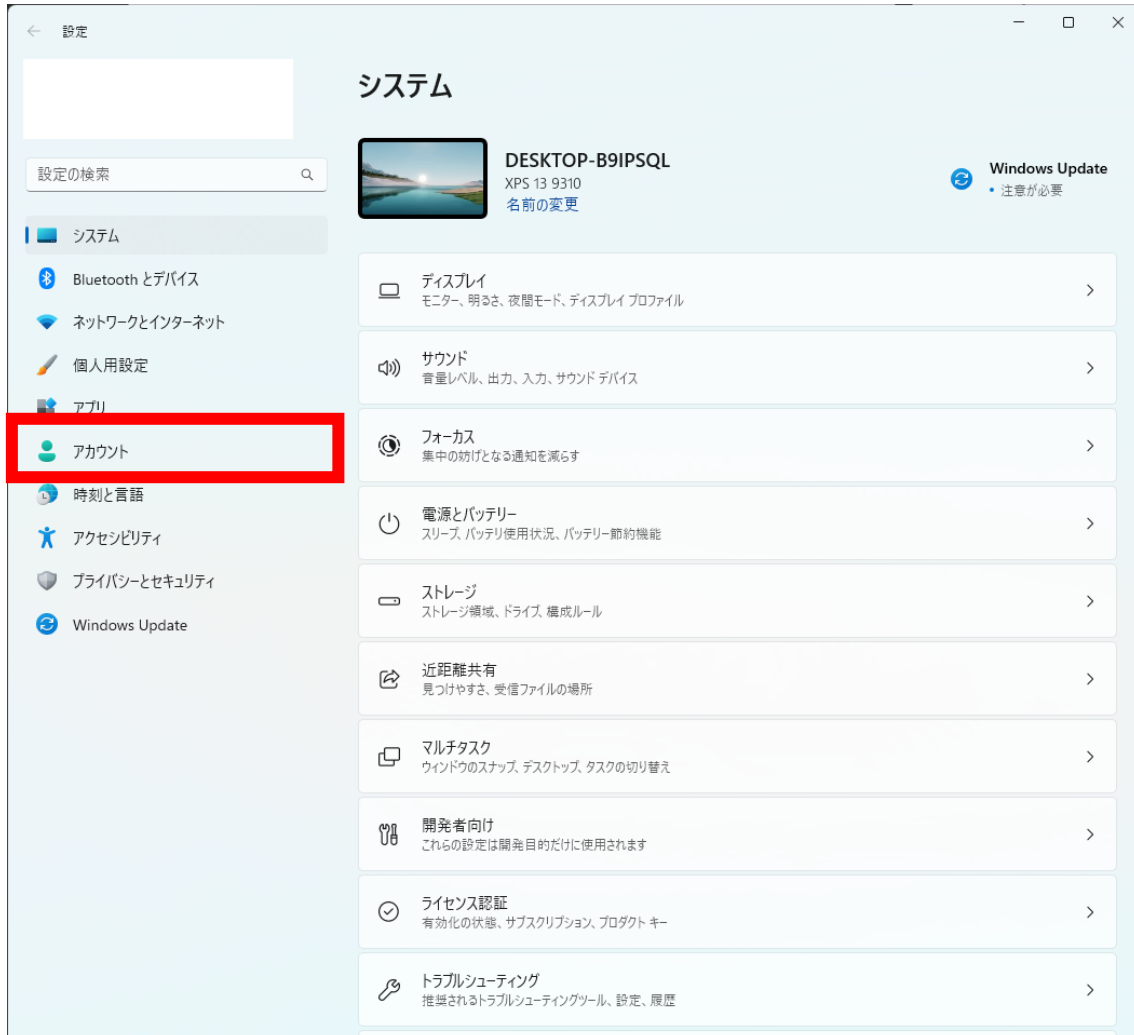
対象 OS	Windows 10 Pro Windows 11 Pro Windows 10 Home Windows 11 Home
設定内容	共通アカウントを利用している場合は利用者ごとに個別に発行
自社診断のための 25 項目	4
対象ツール	OS 等

- 概要

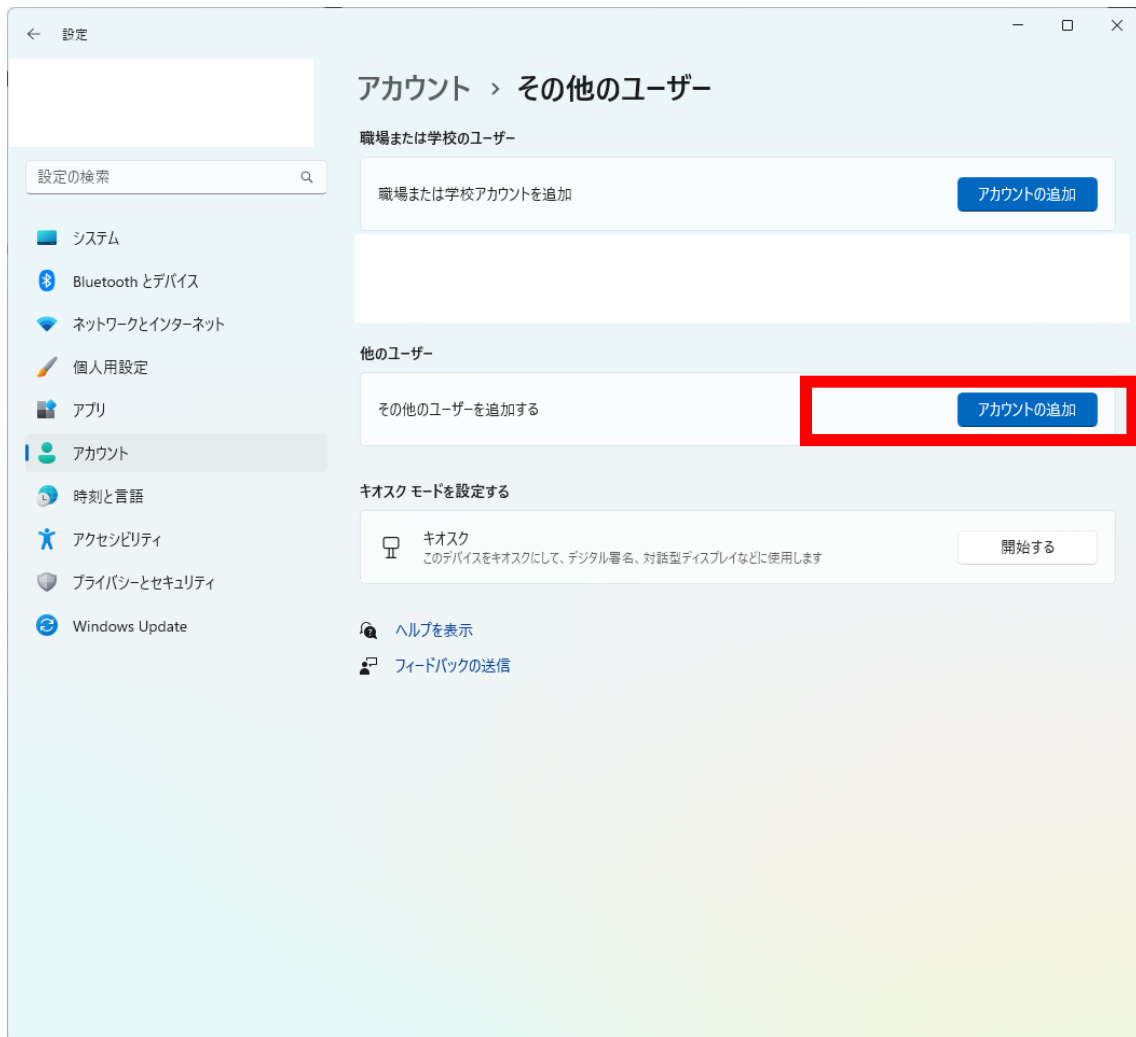
共有アカウントの利用は、利用している利用者の一人が退職した際にパスワードを変更する手間が増えるだけでなく、パスワードが変更されなかった場合に退職者等からアクセスされるリスクがあります。PC のユーザや Web サービスのアカウントは共通ユーザの利用は避け、人ごとにアカウントを発行しましょう。

- 導入方法

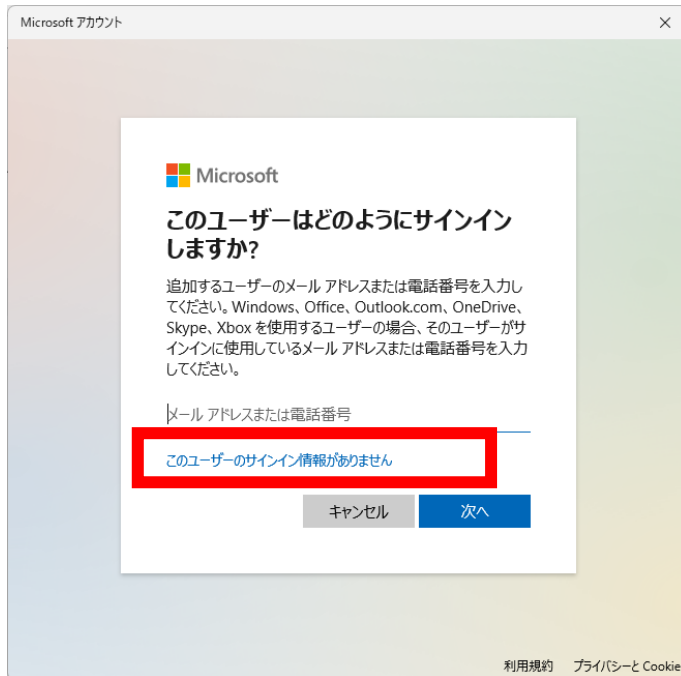
Windows の場合は、下記のメニューでアカウントを追加できます。今回はローカルアカウントを追加する方法について述べます。設定を開きアカウントを選択します。



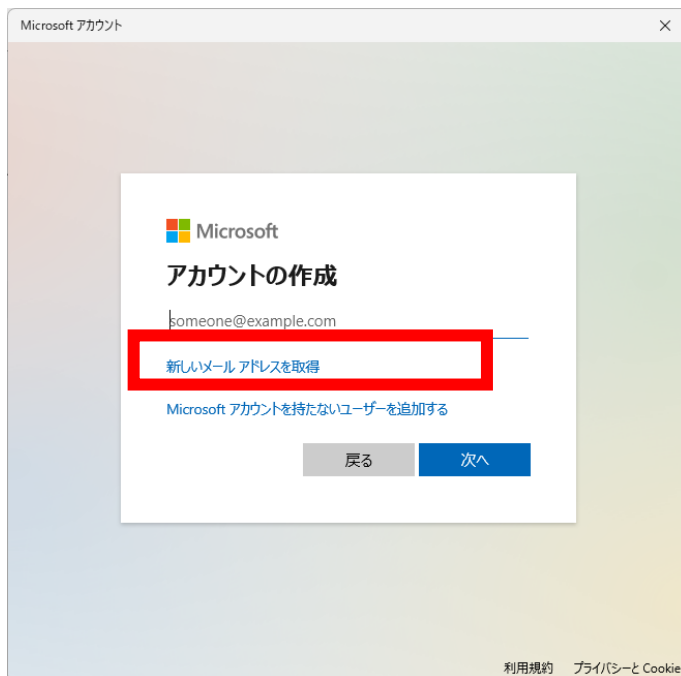
アカウントを追加を選択します。



Microsoft アカウントを持っていないので、このユーザのサインイン情報がありませんを選択します。



Microsoft アカウントを持たないユーザを追加するを選択します。



ユーザ名とパスワードを入力することでアカウントを作成することができます。

Microsoft アカウント ×

この PC のユーザーを作成します

このアカウントが子供または 10 代のユーザー向けのアカウントの場合は、**[戻る]** を選択して Microsoft アカウントを作成することを検討してください。若い家族が Microsoft アカウントでログインすると、年齢に焦点を当てたプライバシー保護が提供されます。

パスワードを使用する場合は、覚えやすく、他人からは推測されにくいパスワードを選んでください。

この PC を使うのはだれですか?

パスワードの安全性を高めてください。

次へ(N) 戻る(B)

2.6. 導入にあたっての留意点

利用環境によって追加の設定が必要になる場合や、すでに有償ツールを利用しており、対応が不要な項目が出てくる場合があります。

例えば、ファイアウォールの設定などはプリンタやファイル共有の設定など利用環境を考慮して行ってください。

3. さらにセキュリティを向上させるには

本ドキュメントは、コストをかけずにできる対策として、様々な項目をマッピングしています。さらにセキュリティを向上させるためには、有償のクラウドサービスの利用や、Intune等の構成管理ツールの利用等が考えられます。これらのツールを利用すればさらに細かい設定を利用することができセキュリティはもちろんのこと PC の管理といった面でも有効です。

4. おわりに

中小企業に対するサイバー攻撃も増えており、中小企業においてもサイバーセキュリティ対策を進めていく必要があります。しかしながら中小企業においてすぐにサイバーセキュリティ対策の費用を捻出することは困難です。本プロジェクトでは、実際の中小企業・団体をモデルケースとして中小企業向けのコストをかけずに行える対策の一助として対策のドキュメントの作成まで行いました。対策の第一歩として少しでも中小企業のセキュリティを向上させるために寄与できれば幸いです。

5. 参考資料

- i. 中小企業の情報セキュリティ対策ガイドライン 第3.1版
URL: <https://www.ipa.go.jp/security/guide/sme/about.html>
- ii. 一般社団法人JPCERT コーディネーションセンター
URL: <https://www.jpCERT.or.jp>
- iii. 独立行政法人情報処理推進機構
URL: <https://www.ipa.go.jp/index.html>
- iv. 7-Zip
URL: <https://7-zip.opensource.jp/>
- v. KeePass
URL: <https://keepass.info/>
- vi. MyJVN バージョンチェッカ for .NET
URL: <https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html>
- vii. Thunderbird
URL: <https://www.thunderbird.net/ja/>
- viii. Check and Send
URL: <https://addons.thunderbird.net/ja/thunderbird/addon/check-and-send/>