

Windows10サポート終了後 どうすれば良いのか悩んでいる人

- ・サポート終了後、何もしないでそのまま続けて使うとどんなリスクがあるのか？
(被害が自分だけでなく、自分が対応していないことによって他の人に被害を与える危険もある。)
- ・費用をかけないで安全な対策はあるのか？ あります。但し、少し面倒です。

挨拶

私は松葉町地域づくり委員会の中村です。5丁目に住んでいます。よろしくお願ひします。

本日はお忙しい中、説明会にご参加いただき誠にありがとうございます。皆さまが長年使い慣れてきたWindows10のサポートが、まもなく終了いたします。これからはセキュリティの更新が行われなくなるため、パソコンをそのまま使い続けるとウイルスや不正アクセスの被害にあうリスクが高まります。

そして実は…自分だけの問題では済まない場合もあるんです！感染したパソコンがウイルスの拡散元になってしまい、知らず知らずのうちにお友達やご家族、時にはネット上の知らない人にまで迷惑をかけてしまうことも…。まるで、風邪をひいてマスクをせずにくしゃみを連発しているようなものですね。

ですが、ご安心ください！今日は費用のかからない対策を中心に、安心・安全にパソコンを使い続ける方法を、できるだけ分かりやすく丁寧にご説明いたします。パソコンが苦手な方でも大丈夫。一緒に確認しながら進めてまいりますので、ぜひリラックスしてお聞きください。

それでは、どうぞ最後までよろしくお願ひいたします。



569437599415557.mp3



569437599415039.mp3

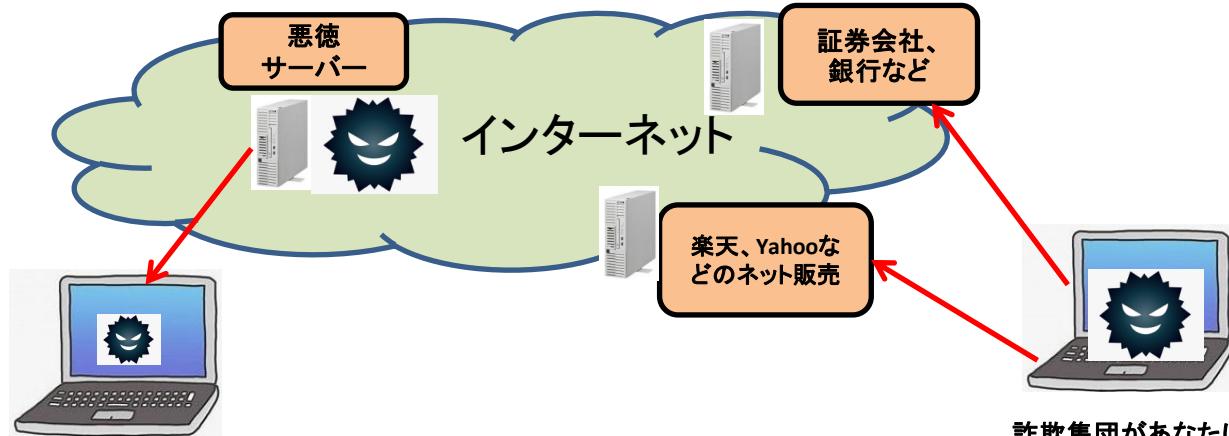
文章作成: Copilot

文章読み上げ: 音読さん

目次

1. Windows 10サポート終了後に何もしない場合のリスク
 - 1.1 そのまま使用するとどんな問題が起きるのか？
 - 1.2 ウィルスがパソコンに入り込み、ウィルスがいろいろな悪いことを行う。(代表例)
 - 1.3 マルウェアはどんな悪さをするのか？
 - 1.4 ウィルスの感染と被害
2. 対応策の種類と流れ
3. Win11にアップグレード
 - 3.1 Windows11のシステム要件
 - 3.2 Windows11システム要件チェック方法
 - 3.3 Windows11へのアップグレード方法
 - 3.4 システム要件を満たしていないPCをWindows11へアップグレードした場合の問題
4. サポート終了後も有料サポートで使用する方法
5. Windows10をちょっと安全に使い続ける対策
6. バックアップ(&リカバリー)手順
 - 6.1 システム修復デスクとシステムイメージの作り方
7. Windows以外のOSを使用する
 - 7.1 UbuntuとWindowsの比較
 - 7.2 Ubuntuが選ばれる3つの理由
 - 7.3 Ubuntuのシステム要件
 - 7.4 Ubuntu環境の構築
 - 7.5 Ubuntuを使おう
 - 7.6 Ubuntuをインストールした後の環境イメージ(デュアルブート)

1. Windows 10サポート終了後に何もしない場合のリスク



◇企業での影響

Windows11へのアップグレードは必須。行わないと最悪、倒産になる可能性あり。

- ・システムの停止:工場、電力、水道などがストップする。
- ・銀行など個人情報を扱っている企業からの漏れ、ブラックマーケットで売られる→信用が落ちる
- ・データにロックがかかり見れなくなる。身代金を請求される。企業活動が停止する

◇個人では具体的には:

- ・個人情報(クッキーなどから、各種ログイン情報(銀行、証券会社、ネットショッピングなどへのログイン情報)が漏れる。
→他人が勝手にログインし悪用して被害に遭う。
- ・データにロックがかかり見れなくなる。身代金を請求される。
他の人に迷惑をかける
- ・メールを通して相手にウィルスを送ってしまいます。
- ・PCが乗っ取られ、迷惑メール送るなど悪用される。

参考)最近話題になっている証券口座乗っ取り被害は2025.5時点で1900件5,000億円以上の被害)

詐欺集団があなたになります
て、証券会社、銀行などにログ
インして取引を行ったり、ネット
ショッピングなどを行う

1. Windows 10サポート終了後に何もしない場合のリスク

Windows10のサポートは2025年10月14日に終了する。

1.1 そのまま使用するとどんな問題が起きるのか？

セキュリティの脆弱性	新しいウイルスやマルウェアに対する防御が弱くなり、個人情報が漏洩する可能性が高まります。
情報漏洩の危険	企業や個人のデータが不正アクセスされる可能性が高まり、重要な情報が流出するリスクがあります。
業務停止の可能性	企業や公的機関で使用されている場合、システムが攻撃を受けることで業務が停止する恐れがあります。
ソフトウェアの互換性問題	新しいアプリや周辺機器がWindows 10をサポートしなくなり、使えなくなる可能性があります。
オンラインバンキングやショッピングの危険性	セキュリティ更新がないため、ネット決済や個人情報入力時に不正アクセスされるリスクが増します。
パフォーマンスの低下	OSの最適化が行われなくなるため、動作が遅くなったり、不具合が増えることがあります。

1.2 ウィルスがパソコンに入り込み、ウィルスがいろいろな悪いことを行う。(代表例)

個人情報の漏洩	ウィルスは、パスワード、クレジットカード情報、住所などの個人データを盗み出すことがあります。サイバー犯罪者に悪用される危険性が高い。
PCの動作が遅くなる	バックグラウンドで不正なプログラムが動作し続けるため、PCの速度が大幅に低下することがある。
勝手にファイルを削除・変更される	重要なデータやシステムファイルが改ざんされたり、削除されることで、PCが正常に動作しなくなる可能性がある。
迷惑な広告やポップアップが頻繁に表示される	ウィルスが広告を強制的に表示し、ユーザーの操作を妨げることがある。
別のウイルスをダウンロードさせられる	一度感染すると、新たなマルウェアを次々にダウンロードさせられ、より深刻な被害につながることがある。
遠隔操作される	悪意のある第三者がPCを乗っ取り、犯罪の踏み台として使用する可能性があります。
金銭的な被害	ランサムウェアのようなウイルスに感染すると、PCのデータが暗号化されて開けなくなり、解除するためには金銭を要求されることも。

マルウェアはどんな悪さをするのか？

1.3 マルウェアはどんな悪さをするのか？

マルウェアは、増殖するための仕組みや他のコンピュータに感染するための機能がある。

例えば、コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖します。コンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して、自動的にウイルス付きの電子メールを送信するものや、利用者がホームページを見るだけで感染するものが多く、世界中にマルウェアが蔓延する大きな原因となっています。マルウェアが実施できる主な活動は、以下の通りです。

No.	主な活動	内容
1	自己増殖	ウイルスの中には、インターネットや <u>LAN</u> を使用して、他の多くのコンピュータに感染することを目的としているものがあります。
2	情報漏洩(じょうほうろうえい)	情報漏洩を引き起こすタイプのウイルスには、利用者がキーボードで入力した情報を記録するキーロガーや、コンピュータ内に記録されている情報を外部に送信する <u>スパイウェア</u> と呼ばれるものなどがあります。
3	<u>バックドアの作成</u>	感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でも、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウイルスは、いつでも攻撃者から遠隔操作できてしまう可能性があるため極めて危険です。
4	<u>コンピュータシステムの破壊</u>	ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものでさまざまです。
5	遠隔操作	コンピュータを外部からの踏み台として遠隔操作するためのウイルスをボット(BOT)と呼びます。ボットに感染したコンピュータは、同様にボットに感染した他の多数のコンピュータとともにボットネットを形成し、その一員として動作するようになります。そして、インターネットを通じて、悪意のある攻撃者が、ボットに感染したコンピュータを遠隔操作し攻撃の踏み台として利用することができます。
6	<u>ランサムウェア</u>	ランサムウェアとは、感染したPC上に保存しているファイル(PCからアクセス可能なネットワーク上のファイルも含みます。)を暗号化して使用ができない状態にするマルウェアです。攻撃者は、復旧させることと引き換えに身代金を要求するため、ランサム(身代金:ransom)ウェアと呼ばれています。 ただし、身代金を支払っても復旧されない可能性があることや、金銭を支払うことで犯罪者に利益供与を行ったと見なされてしまうこともあるため、支払いに応じることは推奨されません。 また、これまで暗号化して身代金を要求するケースが多かったものの、攻撃者が「より手軽に」身代金を得るため、「暗号化」を行わず、盗み取ったデータの公開を対価に身代金を要求する「ノーウェアランサム」攻撃による被害も増加しています。

ウィルスの感染と被害

1.4 代表的なウィルスの感染と被害

1) 迷惑メール(なりすましメール)に反応した。

メールを開いただけでは通常ウィルスに感染しない。(キチンをサポートされているOSを使用している場合)

メール内にあるURLをクリックしたり、添付ファイルを開いたときに感染する。(最新のOSを使用していても感染する)

しかし、**サポートされていないOS(例:サポート終了後のWin10を使用している場合)**は開いただけで感染する場合がある。

参考) 感染している人からのメールは注意。知人からのメールなので信用して添付ファイルを開くと知人がサポート切れのWin10を使用していた場合に知人が気が付かないでウィルスを添付してメールする場合がある。

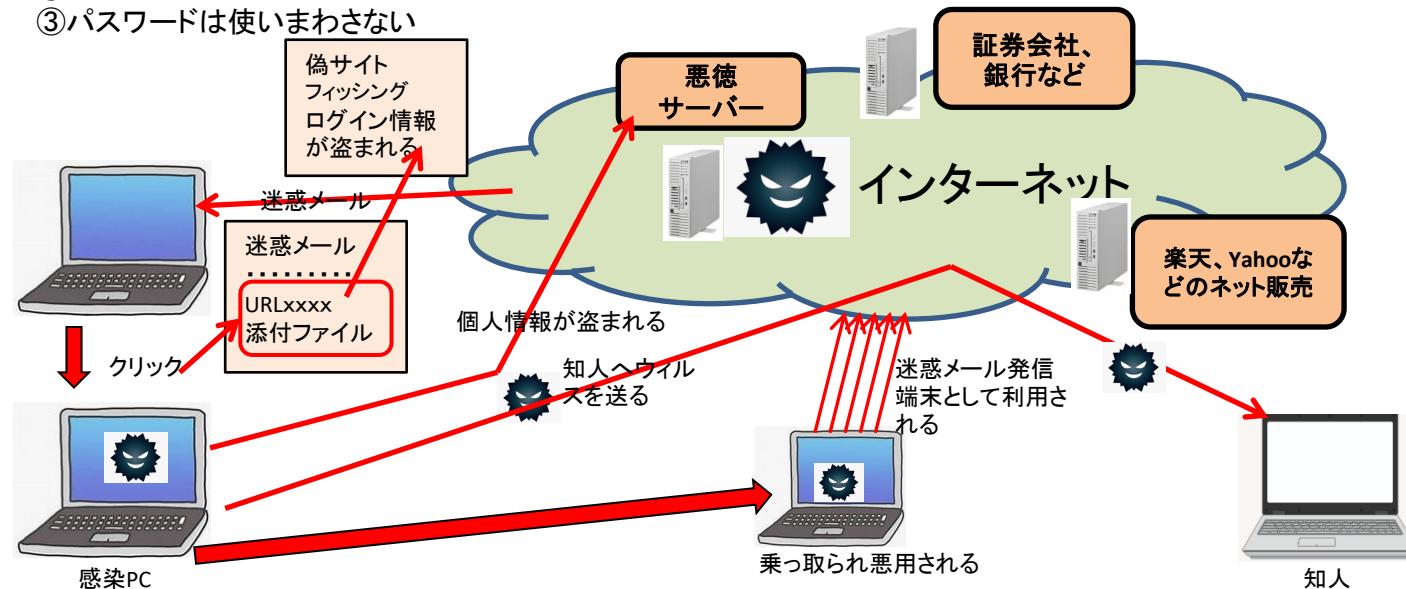
2) インフォスティーラ (マルウェア)の感染

迷惑メール(+感染している知人からのメール)から感染する。

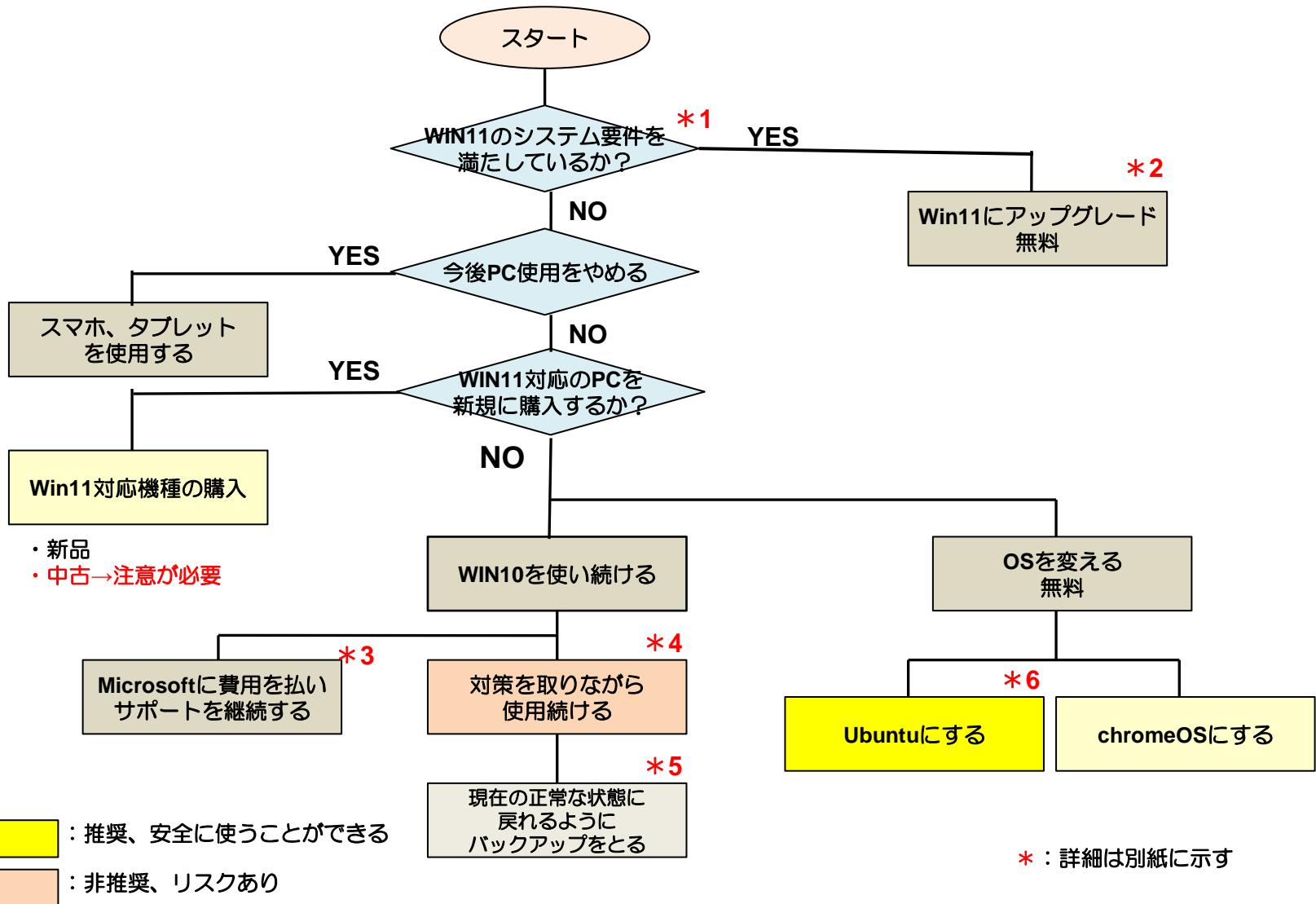
悪徳サーバーからインフォスティーラに指示が出て、PC内にある個人情報が盗まれる。(各種ログイン情報等)

3) 対策

- ①電子メールやSMSのリンクは開かない
- ②Webサイトのアクセスはブックマークから
- ③パスワードは使いまわさない



2. 対応策の種類と流れ



3. Windows11にアップグレードする

3.1 Windows11のシステム要件(Microsoftの公式ページ)

プロセッサ	1GHz以上で2コア以上の64ビット互換プロセッサまたはSystem on a Chip (SoC)
メモリ	4GB
ストレージ	64 GB 以上の記憶装置
システムファームウェア	UEFI・セキュアブート対応
TPM (Trusted Platform Module)	TPMバージョン2.0
グラフィックスカード	DirectX 12以上 (WDDM2.0ドライバー)
ディスプレイ	対角サイズ9インチ以上で8ビットカラーの高解像度(720dpi)ディスプレイ

参考)

TPM 2.0 の搭載 (Trusted Platform Module)

TPM(Trusted Platform Module)は、デバイス上で様々なセキュリティ機能を提供するためのモジュール

暗号化用アルゴリズムエンジン、ハッシュエンジン、鍵生成器、乱数生成器、不揮発性メモリ(鍵などを保管)などを備えたモジュールで、TPM内への暗号キーの作成や使用制限をするために利用される。

簡単に言えば、暗号化で利用する鍵を安全な場所で管理するための仕組み。

例えば、金庫に鍵をかける場合、金庫と鍵を同じ場所に置いておくと開けられてしまう可能性が高いが、鍵を金庫とは別の場所(つまりTPM)に保管し、鍵を取り出せる人を厳密に管理することで、金庫の中身を保護することができる。

2016年以降に出荷されたほとんどのPCには、トラステッド プラットフォーム モジュール バージョン 2.0 (TPM 2.0) を実行する機能がある。しかし有効になっていない場合があるのでチェックが必要。

セキュアブートの対応

Intel 第8世代 / AMD Ryzen 2000以降のCPU

これらはマルウェア対策やパフォーマンス、安定性を考慮して設けられたもので、旧型PCの多くはこの要件を満たしておらず、非対応と判断される。

3. Windows11にアップグレードする(1)

参考) TPM を有効にする方法

TPM を有効にする必要がある場合、これらの設定は UEFI BIOS (PC のファームウェア) で管理されており、デバイスによって異なります。これらの設定にアクセスするには、[設定] > [更新とセキュリティ] > [回復] > [今すぐ再起動] を選択します。次の画面から、[トラブルシューティング] > [詳細オプション] > [UEFI フームウェアの設定] > [再起動] を選択して変更を加えます。これらの設定は、UEFI BIOS の [Advanced]、[Security]、[Trusted Computing] というサブメニューに含まれていることがあります。TPM を有効にするオプションには、[Security Device]、[Security Device Support]、[TPM State]、[AMD fTPM switch]、[AMD PSP fTPM]、[Intel PTT]、[Intel Platform Trust Technology] などのラベルが付いている場合があります。TPM の設定をどのように変更すればよいかわからない場合は、お使いの PC メーカーのサポート情報を確認するか、メーカーのサポート組織に問い合わせることをお勧めします。参考までに、一部の PC メーカーについて情報が掲載されているリンクを紹介します。

[Asus](#)

[Dell](#)

[HP](#)

[Lenovo](#)

[Microsoft Surface](#)

Windows11システム要件チェック方法 *1

3.2 Windows11システム要件チェック方法

- 1.生成AIに調べさせる。Copilotに“XXX(機種名)はWindows11に対応しているか調べて？”
2. PCメーカーの公開ページで調べる。 例:XXXX(機種名) Windows11 対応か?などで検索
3. Microsoftが公開しているツールでチェックする。

4.自分で調べる

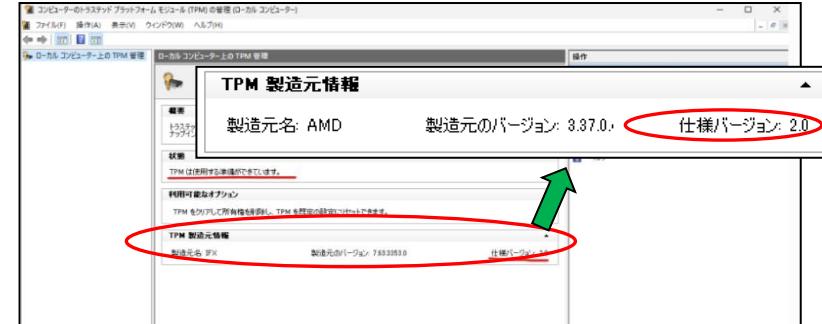
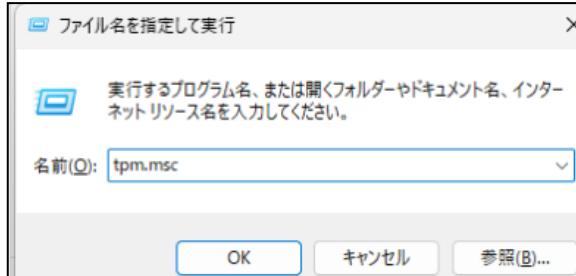
- 1)CPU 下記のネットに載っているCPUか調べる。

[Windows プロセッサ要件 - Windows 11 でサポートされている Intel プロセッサ | Microsoft Learn](#)

[Windows プロセッサ要件 - Windows 11 でサポートされている AMD プロセッサ | Microsoft Learn](#)

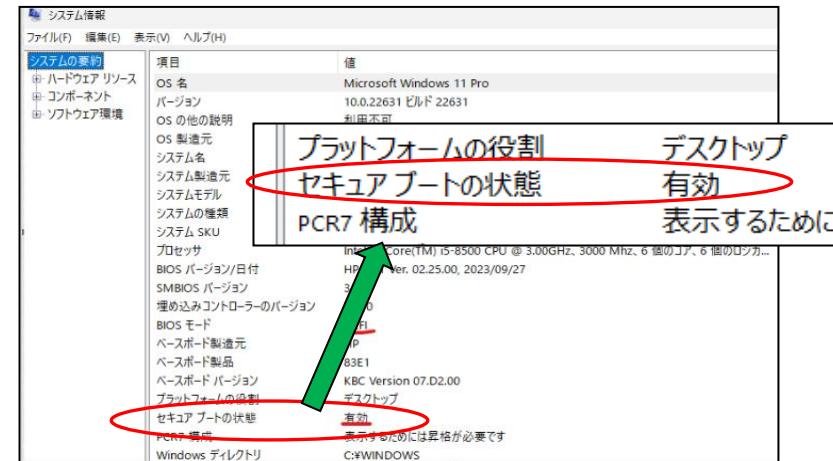
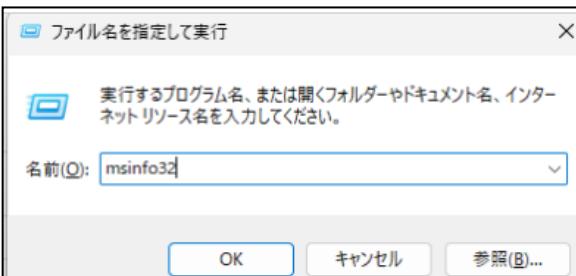
2)TPM

- 1)WinキーとRを同時に押し、“tpm.msc”を入力



3)セキュアブート

- 1)WinキーとRを同時に押し、“msinfo32”を入力



Windows11へのアップグレード方法 *2

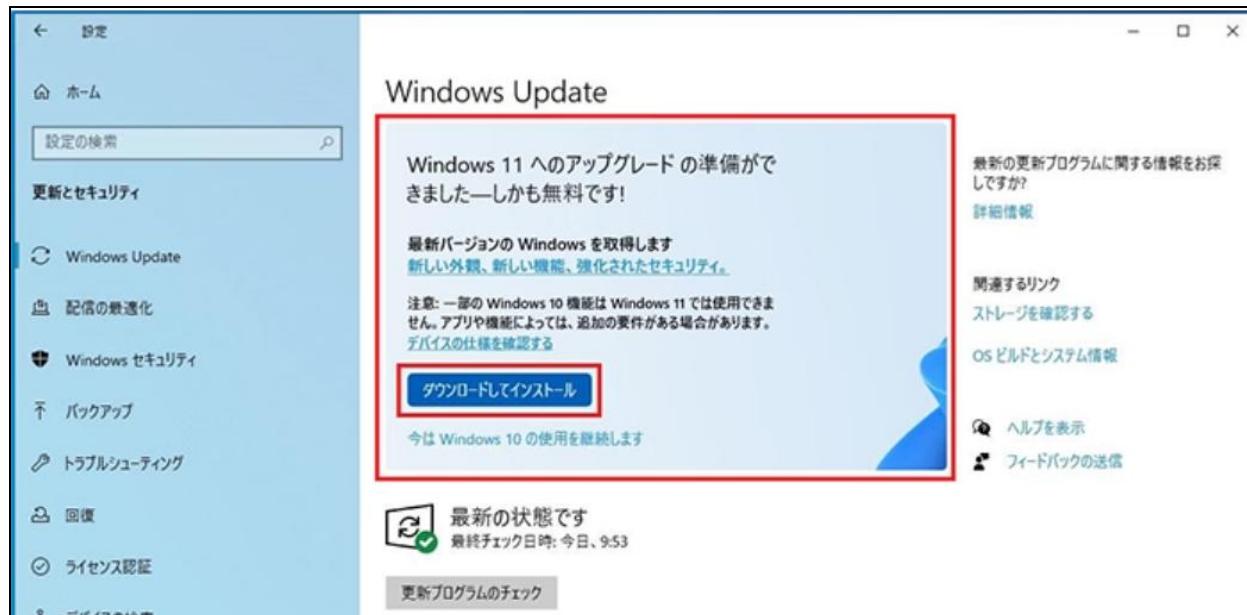
3.3 Windows11へのアップグレード方法

1.事前準備

- システム要件を満たしているか確認する。
- 利用しているソフトウェアやデバイスの互換性を確認する。 →使っているソフトがWin11に対応していない場合がある
- Windows 10を最新のバージョンにアップデートしておく
- 重要なデータをバックアップしておく →万が一失敗したときの安全策

2.「設定」→「更新とセキュリティ」でWindows Update画面を開く。

“Windows11へのアップグレードの準備ができました—しかも無料です”が表示されることを確認する
“ダウンロードしてインストール”をクリックしてアップグレードを開始。



システム要件を満たしていないPCをWindows11へアップグレードした場合の問題

3.4 システム要件を満たしていないPCをWindows11へアップグレードした場合の問題

Windows 11のシステム要件を満たしていないパソコンを無理やりアップグレードすると、いくつかの重要なリスクや制限がある。

Microsoftのサポート対象外	公式にはサポートされないため、トラブルが起きても修正パッチや技術サポートが受けられません。
アップデートの保証なし	セキュリティ更新プログラムや機能アップデートが配信されない可能性があります。
互換性の問題	ドライバーやアプリが正常に動作しない、またはシステムが不安定になることがあります。
保証対象外	ハードウェアの損傷が発生しても、製造元の保証が無効になる場合があります。
警告表示	デスクトップに「このPCはWindows 11の要件を満たしていません」といった透かしが表示されることがあります。

Microsoftは、こうしたリスクを避けるために、要件を満たしていないPCには対応PCへの買い替えを推奨しています。

4. サポート終了後も有料サポートで使用する方法 *3

Microsoftが提供する「Windows 10の拡張セキュリティUpdatesプログラム(ESU)」を利用する。

Microsoftは有料で、引き続き「重要なセキュリティ更新プログラム」を提供する予定。

これを利用することで、2025年10月14日にサポートが終了した後もWindows 10を引き続き使用できる。

◇Windows 10の最終バージョン「22H2」であること。

◇ESUは有料のサブスクリプション

- ・組織や企業向けには、1デバイスあたり1年61ドル(USドル)
- ・個人またはWindows 10 Homeは1デバイス当たり1年30ドル。

・**最大3年間、料金は1年ごとに前年の2倍となる(例えば、個人の場合、翌年は60ドル、翌々年は120ドル、という計算)。**

◇サブスクで提供されるのは「重要なセキュリティ更新」のみで、終了までに通常受け取っていた機能やドライバーのアップデート、通常レベルのセキュリティアップデート、さらには電話やメールなどのテクニカルサポートは含まれていない。

◇Microsoftは「ESUに関連する課題に遭遇したユーザーに対してのみサポートを提供」と述べており、最低限のセキュリティのみの確保であることは明らか。結論からすると、重要なセキュリティ以外のアップデートは提供されないこと、年々コストが増加するシステム、などから推測すると、これはあくまで「一時的な延命措置」といえる。

5. Windows10をちょっと安全に使い続ける対策 *4

Windows 10を安全に？使い続けるための対策

(Windows 10のサポート終了後も費用をかけずに少しでも安全に使い続けるための対策。

こんなケチなことを考えてはいけない！)

★リスクは残ります。推奨しません。

最新のセキュリティソフトを導入	Windows Defenderの更新が止まるため、無料のウイルス対策ソフトを導入する。又定期的にスキャンを実施する。
定期的なバックアップ	重要なデータを外付けHDDやクラウドに保存し、万が一のトラブルに備える。Windowsのバックアップ機能を活用し、万が一に備える。
不要なソフトウェアの削除	古いソフトウェアは脆弱性の原因になるため、使わないものはアンインストールすると良い。
安全なブラウジングの習慣	怪しいサイトやリンクを避け(フィッシング詐欺に注意)、信頼できるサイトのみを利用することでリスクを減らす。
オフライン利用を増やす	インターネット接続を減らすことで、外部からの攻撃リスクを抑える。

6. バックアップ（&リカバリー）手順 *5

バックアップはハード障害、操作ミスなどで重要なデータが消えた、パソコンが使用できなくなつた（例：起動しなくなつた）などの場合に備えて行う基本的なことである。

又Windows 10を使い続ける場合は、定期的なバックアップが重要になってきます。サポート終了後にトラブルが発生しても、バックアップからデータを復元できれば、被害を最小限に抑えられる。

ここでは基本的な2つのバックアップについて説明する。（Windowsの機能）

種類	内容
回復ドライブ	パソコンを初期状態に戻す。 アプリやその他の個人データはバックアップされない。
システムイメージ (+修復ディスク)	全ての状態を、正常に使用していた状態に戻す。 システムイメージの作成とは、コンピューターの全内容を含む完全なバックアップを作成する方法です。オペレーティングシステム、アプリケーション、設定、ユーザーデータなどをイメージファイル化し、外付けHDDなどにコピーします。システムクラッシュやハードウェア障害が発生した場合でも、完全な状態でコンピューターを復元可能です。

準備するもの

- ・回復ドライブ：8GのUSBメモリー
- ・システムイメージ：実際に使っているHDD（又はSDD）のサイズのHDD（又はSDD）
- ・修復ディスク：DVD

参考情報

◇回復ディスクの作り方

[Windows10/11の回復ドライブ（リカバリーディスク）を作成する方法 | 名古屋市パソコン修理専門店「かおるや」のブログ](#)

◇システム修復ディスクの作り方

[【【Windows10】システム修復ディスクの作成方法！PCが起動しない時はどうする？](#)

◇システムイメージの作り方

[【Windows11】システムイメージのバックアップを取る方法](#)

[【Windows 11】無料で簡単バックアップ！起動できないトラブルも復元可能。標準ツールでシステムイメージバックアップ](#)

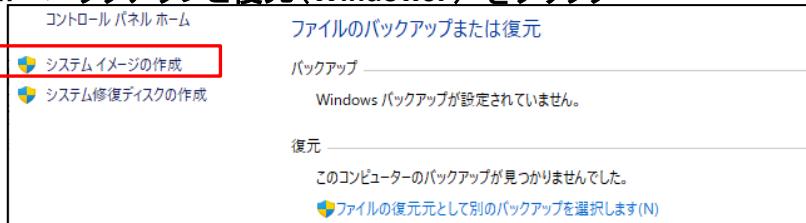
6.1 システム修復デスクとシステムイメージの作り方

0. 準備 バックアップを作るHDDを接続する。

1. コントロールパネルを開く。(ファイル名を指定して実行で“control”を入力)
(又はWindowsツールから開く)



2. “バックアップと復元(Windows7)”をクリック



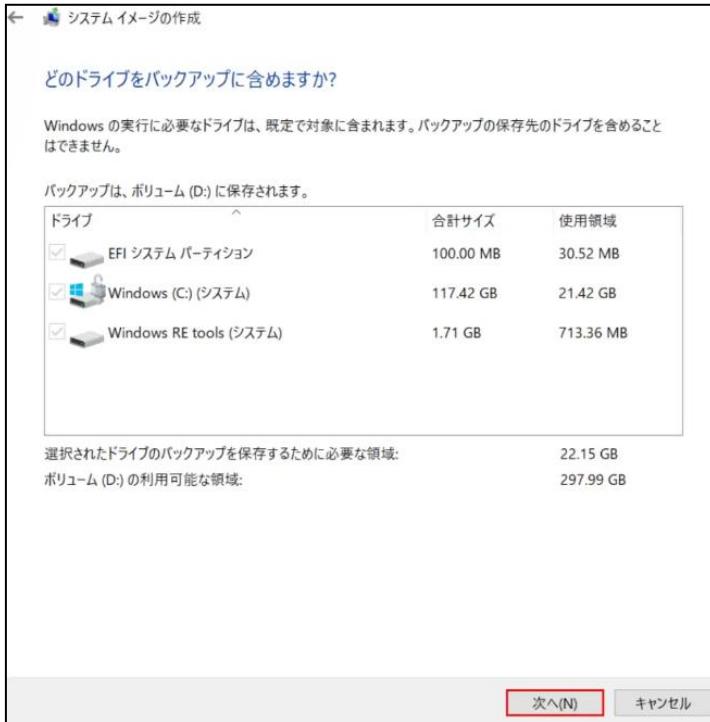
3. “システムイメージの作成”をクリック



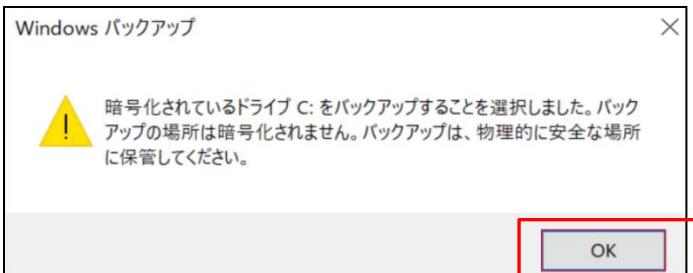
4. “次へ(N)”をクリック

6.1 システム修復デスクとシステムイメージの作り方(1)

5. バックアップするドライブを確認。通常表示された内容で良い。
“次へ(N)”をクリック



6. “OK”をクリック



7. 確認画面の内容が間違いない事を確認して
“バックアップの開始(S)”をクリック



7. Windows以外のOSを使用する *6

Windows以外のOSを使う。

代表的な代替えOSは

1. Ubuntu(Linux)
2. chromeOS (小学校低学年に支給されているパソコンのOS)

2つともLinux系OSである。

ここではUbuntuについて説明する。

Linux: 無料のオプションオープンソースであるOSである。

これをベースにいろいろなOSが開発されている。

代表例: Android, ChromeOS(chromebook) 開発はGoogle

7.1 UbuntuとWindowsの比較

項目	Ubuntu	Windows
開発元	Canonical	Microsoft
ライセンス	オープンソース(無料)	商用(有料)
ユーザーインターフェース	GNOME、KDEなど(カスタマイズ可能)	Windows GUI(固定的)
ソフトウェア互換性	オープンソースソフトが豊富	商用ソフトが豊富(MS Officeなど)
ハードウェア互換性	一部ドライバーが必要	幅広いハードウェアに対応
セキュリティ	高い(ウイルスが少ない)	定期的なセキュリティアップデート
コマンドライン	必須(高機能)	ほぼ不要(PowerShellあり)
ゲームサポート	限定的(Steam対応あり)	多くのゲームが対応
サポート	コミュニティ主体	公式の技術サポートあり
アップデート	頻繁で自由(ユーザー管理)	自動更新あり(制御可能)

Ubuntuが選ばれる3つの理由

7.2 Ubuntuが選ばれる3つの理由

Ubuntuは他のOSと比べて、いくつかの優れた特徴を持っている。以下に、特に注目すべき3つのポイントを示す。

無料で利用可能でコストパフォーマンスが高い

Ubuntuはオープンソースのため、個人利用や商業利用でも基本的に無料で提供されており、公式サイトから簡単にダウンロードしてインストールできる。特に、最新技術の研究や教育目的で利用されるケースが多く、コストを抑えつつ実用的な環境を整えられる点が強みです。

安定性とセキュリティが高い

Ubuntuは企業向けに提供されている「LTS(Long Term Support)」バージョンにより、5年間の長期サポートと定期的なセキュリティアップデートが保証されている。このため、企業のサーバー用途としても信頼されており、リスク管理が求められるビジネスシーンでも安心して導入可能です。

日本語環境と豊富なサポート

日本語Remix版には、日本語入力ソフト「Mozc」が標準搭載されており、日本語表示のサポートも充実しています。日本語フォーラムやQ&Aサイトなどのオンラインコミュニティが豊富に存在するため、設定やカスタマイズで困ったときにもすぐにサポート情報を得ることができます。特に、Ubuntu Japanese Teamが提供する日本語リソースが充実していることから、日本語ユーザーも快適に利用できます。

7.3 Ubuntuのシステム要件

7.3 Ubuntuのシステム要件(古くても、ほとんどのパソコンは問題ない)

プロセッサ	1GHz以上で2コア以上の64ビット互換プロセッサまたはSystem on a Chip (SoC)
メモリ	最低4GB
ストレージ	64 GB 以上の記憶装置
システムファームウェア	UEFI・セキュアブート対応
TPM (Trusted Platform Module)	TPMバージョン2.0
グラフィックスカード	DirectX 12以上 (WDDM2.0ドライバー)
ディスプレイ	対角サイズ9インチ以上で8ビットカラーの高解像度(720dpi)ディスプレイ

7.4 Ubuntu環境の構築

参考) <https://www.linux.digibeatrix.com/ubuntu-basics/ubuntu-download-install-step/>

1. ライブUSBの作成(USBメモリー(8G以上)、又は外付けHDD,SDDを用意)

①Ubuntuのダウンロード

Ubuntuの公式サイト(<https://jp.ubuntu.com/download>)から最新版をダウンロードする。

Ubuntu Desktop 24.04.2 LTS

デスクトップPCおよびノートPC向けUbuntu LTS版の最新バージョンをダウンロードいただけます。LTSはlong-term support (長期サポート) の略称です。2029年4月までの5年間、無料のセキュリティアップデートおよびメンテナンスアップデートが保証されています。

ダウンロード

[Ubuntu 24.04 LTS release notes](#)

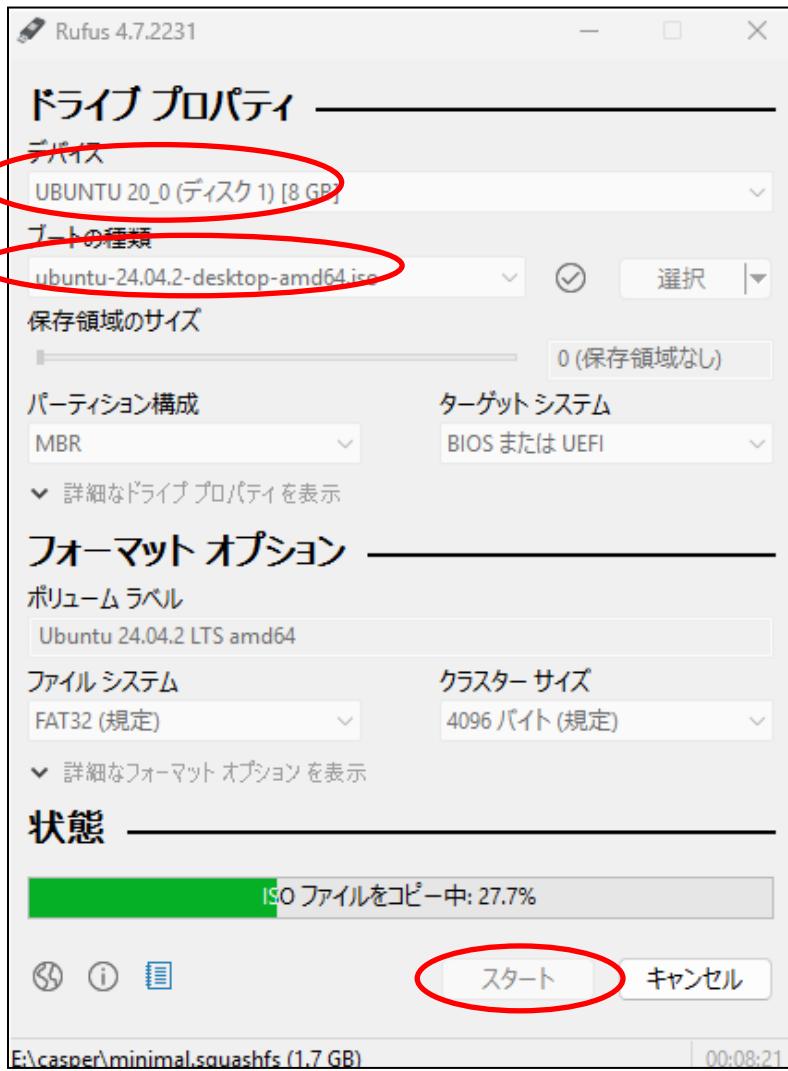
注) Desktop版のLTSを指定する。

② Rufusをダウンロード <https://rufus.ie/ja/>

ダウンロード					
最新リリース:					
リンク	タイプ	プラットフォーム	サイズ	日付	
rufus-4.7.exe	標準	Windows x64	1.6 MB	2025.04.09	
rufus-4.7p.exe	Portable	Windows x64	1.6 MB	2025.04.09	
rufus-4.7_x86.exe	標準	Windows x86	1.6 MB	2025.04.09	
rufus-4.7_arm64.exe	標準	Windows ARM64	5.3 MB	2025.04.09	

7.4 Ubuntu環境の構築(1)

- ③ Rufusを起動して必要事項を設定し、“スタート”をクリックし作成する。



7.4 Ubuntu環境の構築(2)

2. Ubuntuをインストールする。

1)事前準備

- ①失敗してPCが起動できなくなる可能性があります。必ずバックアップ(6.1)を取ってから行うことをお勧めします。
- ②Ubuntu格納場所を確保する。[Windows10 ドライブ\(パーティション\)を縮小する | PCの鎖](#)
 - ・未割当てとして64G以上を確保する。(各PCの状況によって異なる。)
- ③BIOSを変更して。起動順番を“USB”にする。

2)Ubuntuをインストールする。[Ubuntuのセットアップ #環境構築 - Qiita](#)

注) どうやってUbuntuをインストールしますか？

“UbuntuとWindows10を共存させる”を選択すること。“UbuntuとWindows Boot Managerと共に存させる”

注)インストール先のディスク選択

次に、Ubuntuをインストールするドライブを選択します。専用のドライブにインストールする場合は「ディスクを削除してUbuntuをインストール」を選択し、他のOSと共に存させる場合は「パーティションを自分で選択」を選択します。OS共存を選択する際は、既存のデータをバックアップしておくことをおすすめします。

ルートパーティション(/):ここにOSがインストールされます。

サイズ:80GB

Use as:Ext4ジャーナリングファイルシステム

マウントポイント:/

スワップパーティション

サイズ:8GB

Use as:スワップ領域

ホームパーティション(/home)

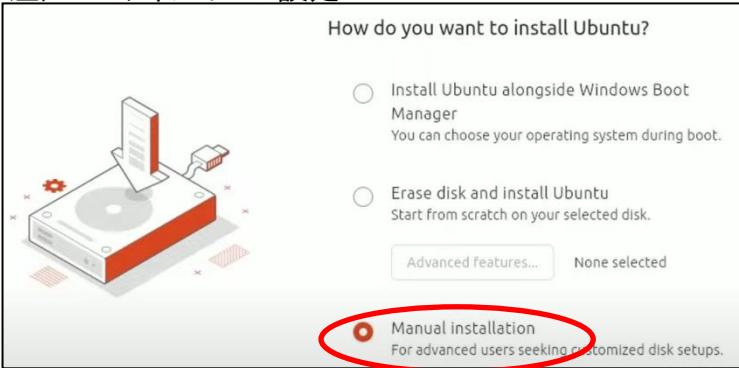
サイズ:残りの空き領域(約40GB)

Use as:Ext4ジャーナリングファイルシステム

マウントポイント:/home

7.4 Ubuntu環境の構築(3)

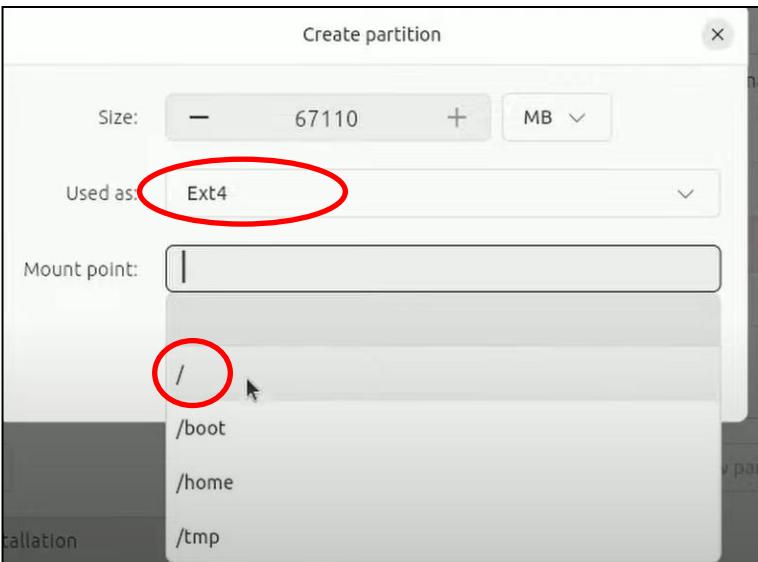
注)パーティションの設定



①“Manual Installation”を指定

Device	Type	Mount point	Size	System	Format
sda			137.44 GB		
sda1	VFAT		104.86 MB	Windows Boot Manager	
sda2			16.78 MB		
sda3	NTFS		69.57 GB		
Free space			67.11 GB		
sda4	NTFS		633.34 MB		
Free space			1.05 MB		

②未割当を指定し、“+”クリック



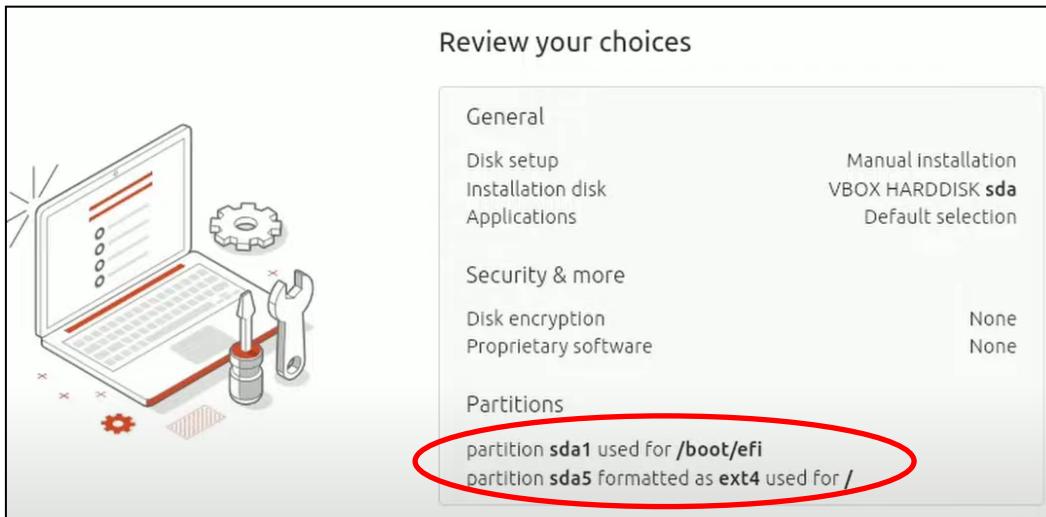
③“+”を指定

Device	Type	Mount point	Size	System	Format
sda			137.44 GB		
sda1	VFAT	/boot/efi	104.86 MB	Windows Boot Manager	
sda2			16.78 MB		
sda3	NTFS		69.57 GB		
sda5	Ext4	/	67.11 GB		
sda4	NTFS		633.34 MB		
Free space			1.05 MB		

④設定した内容を確認

7.4 Ubuntu環境の構築(4)

⑤最終確認



7.5 Ubuntuを使おう

1. 検索(ブラウザー) : Firefox(最初から使用できる。)

Windowsで使用していたブラウザーを使用したい場合

1) Edgeを使えるようにする。<https://lifework-blog.com/ubuntu-microsoft-edge/>

① Microsoftサイトから“Edge(Linux (.deb))”をダウンロードする。

[Microsoft Edgeのダウンロード:Windows, macOS, iOS, Android](#)

② ダウンロードしたファイルを右クリックし、「Open With...」を選択して“アプリセンター”で開く。

③ “インストール”をクリックして終了。

2) Chromeを使えるようにする。[ChromeをダウンロードしてUbuntuにインストールする方法と同期設定 | 旅好きねっとなまら北海道野郎](#)

① Googleが作ったブラウザー “Chromeをダウンロード”をクリックする。

② 64ビット .deb (Debian/Ubuntu 用)を選択し“同意してインストール”をクリックしてダウンロードする。

③ ①②、③(Edgeの場合と同じ。)

2. メール : Thunderbird

3. Office : Microsoft Office Web上で使用

LibreOffice 参考)2025年6月デンマーク政府がMicroOfficeからLibreOfficeに移行すると発表。

EUのデジタル主権のため(アメリカのテクノロジー会社への依存を減らすため(コペンハーゲン市のデジタル赤字は2018年:45億円→2023年:78億円に拡大)

WPS Office

Googleドキュメント

4. プリンター接続

5. ZOOM

7.6 Ubuntuをインストールした後の環境イメージ

デュアルブート(1つのパソコンに2つのOSで使用できるようにする。)

