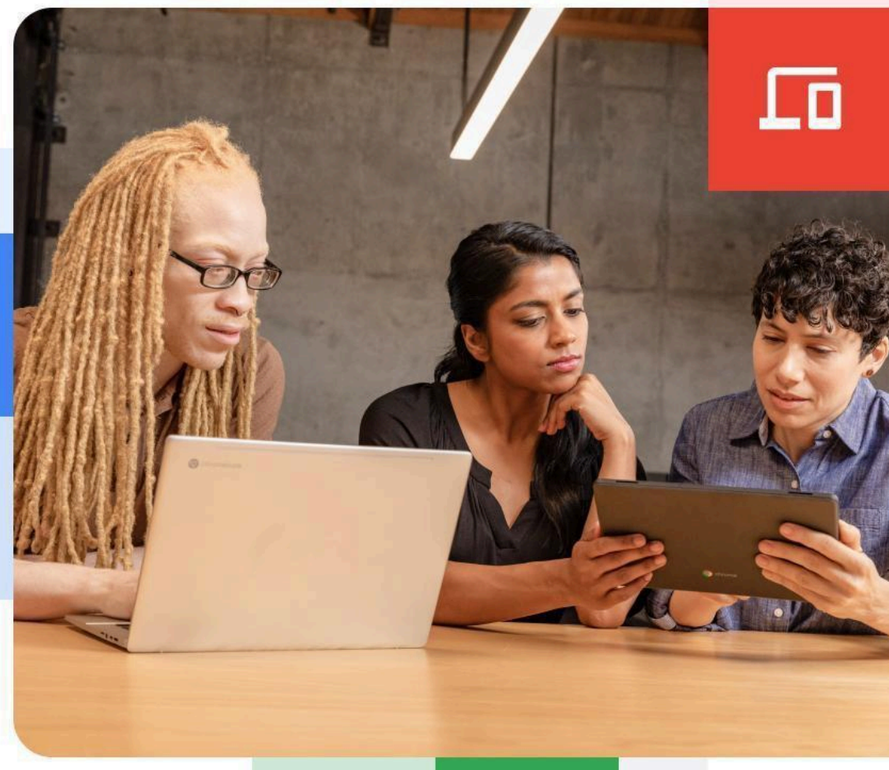
chromeOS

手にしたときから最も安全な OS[1]



ChromeOS が競合製品より優れている 8 つの理由

ChromeOS は Windows 11 や macOS と比べ、手にしたときから非常に安全なオペレーティング システムです。これは、セキュリティ調査会社 Atredis Partners の最近の競合分析レポートによる公式な情報です。

ChromeOS はゼロトラストの理念に基づいて構築されており、ユーザーやデバイスを自動的に信頼することはありません。ログインの試行からファイルのダウンロードまで、すべての操作やデータのやり取りの安全性をその都度チェックします。ChromeOS でユーザー、データ、デバイスがあらゆるレベルで保護される仕組みについて、調査レポートで検証された 8 つの主な特徴を紹介します[2]。

1

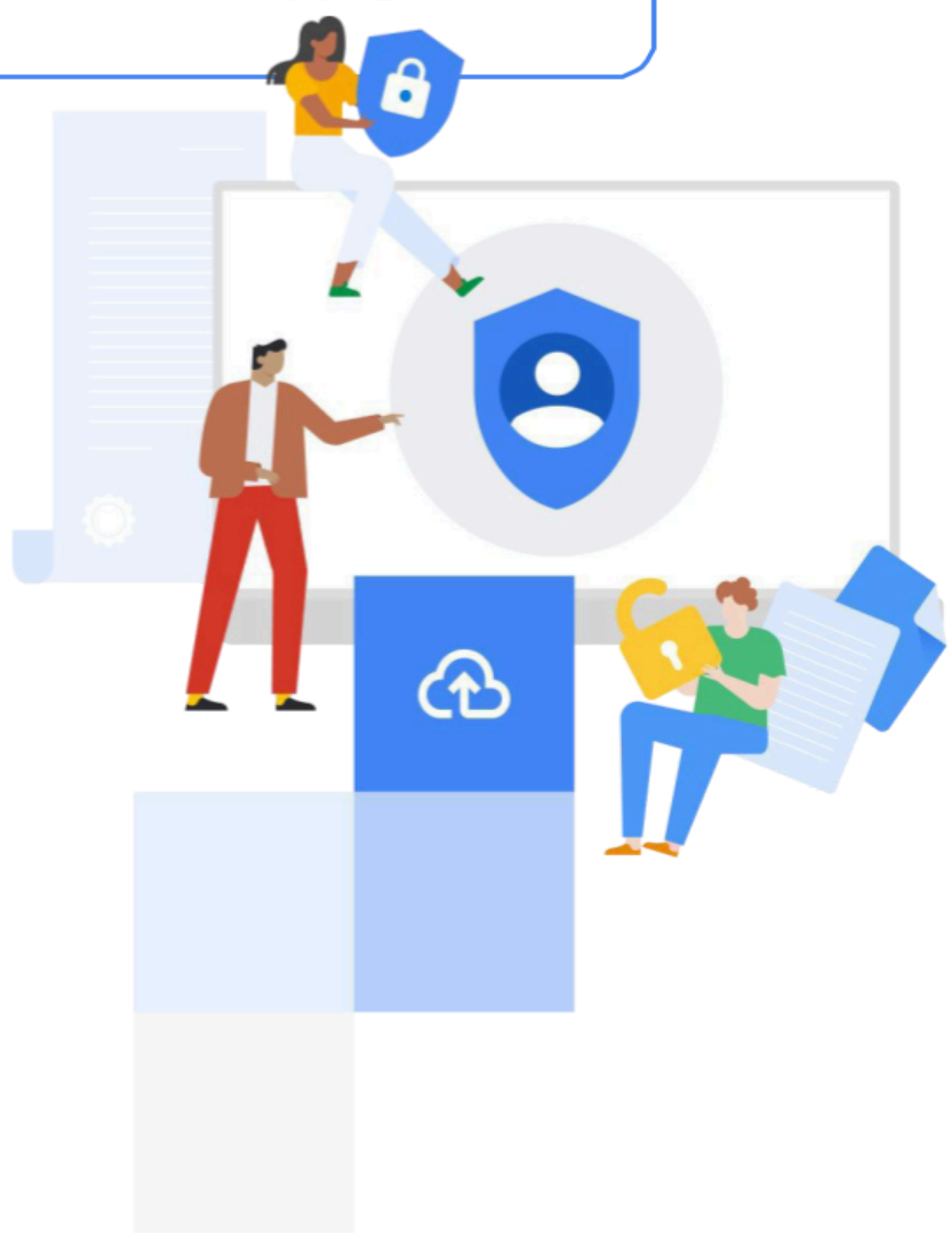
「ChromeOS デバイスは毎回安全に起動」

ChromeOS ではウイルス攻撃やランサムウェア攻撃が 1 件も報告されていません[3]。

ChromeOS には、デバイスの電源を入れるたびにファームウェアに変更が加えられていないかチェックする「確認付きブート」という機能があり、デフォルトの安全基準が macOS や Windows 11 より高くなっています。不明なコードが検出された場合、ChromeOS は以前のバージョンに自動的に戻され、デバイスの安全が確保されます[2]。

chromeOS

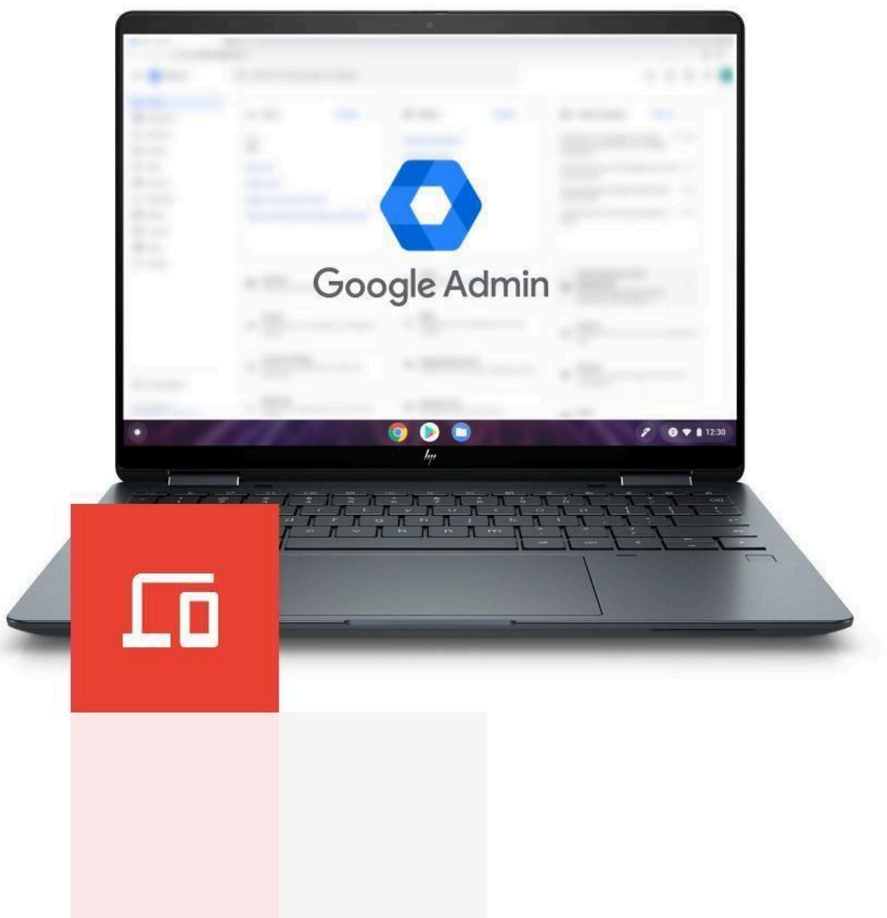
2 「ユーザーデータをデフォルトで暗号化」



ChromeOS は、デフォルトでユーザーが他のユーザーのデータにアクセスできないように設計されている唯一のオペレーティング システムです。

ディスクに保存されるデータはすべて、ユーザーごとに一意の認証情報セットで暗号化されます。ゲストユーザーのデータは、ログアウト後に直ちに削除されます。このため、ChromeOS は共有デバイスに最適なオペレーティングシステムとなっています。一方の Windows 11 や macOS などのオペレーティングシステムは、暗号化に対応するための特別な設定が必要で、その場合でも管理者は他のユーザーのデータにアクセスできます[2]。

3 「ChromeOS に管理者ユーザーは存在しない」



macOS や Windows 11 では、管理者ユーザーがソフトウェアをインストールしたり、ユーザーを作成したり、データを侵害する恐れのあるその他の変更を加えたりできますが、ChromeOS ではより安全なアプローチを採用しています。

ChromeOS にはルートや管理者といったユーザー権限が存在しないため、システムに侵入されるリスクを軽減できます。ユーザーはデベロッパー モードで限定的なシステム変更を行うことができますが、管理者ユーザーと同じ権限が付与されることはなく、ChromeOS の攻撃対象領域は他のシステムより小さくなります[2]。

4

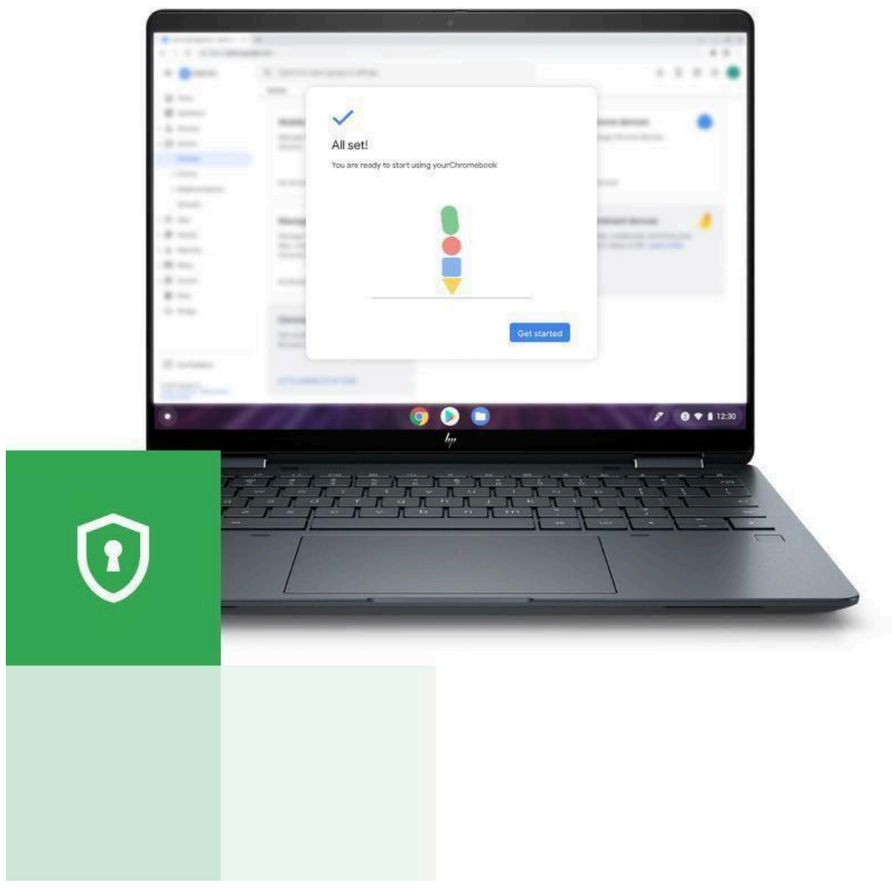
「ChromeOS はオンラインの脅威からユーザーを自動的に保護」

ChromeOS では、システム、アプリケーション、ブラウザの各レベルでサンドボックス化を使用して、データに対する脅威をすばやく封じ込め、無力化します。

Chrome ブラウザでは、組み込みのセーフブラウジング機能により、各ウェブページを分離して、他のタブやアプリ、その他のデバイス要素に影響が生じないようにします。毎日 50 億人を超えるユーザーが、この機能によって自動的に保護されています。macOS や Windows 11 とは異なり、ChromeOS のシステムアーキテクチャはすべてセグメント化され、根幹のシステムファイルは完全に隔離されます。悪意のあるアプリやファイルにアクセスした場合でも、デバイスのファームウェアに侵入されることはありません[2]。

5

「教育機関や企業では、ユーザーがアクセスするコンテンツを限定できる」



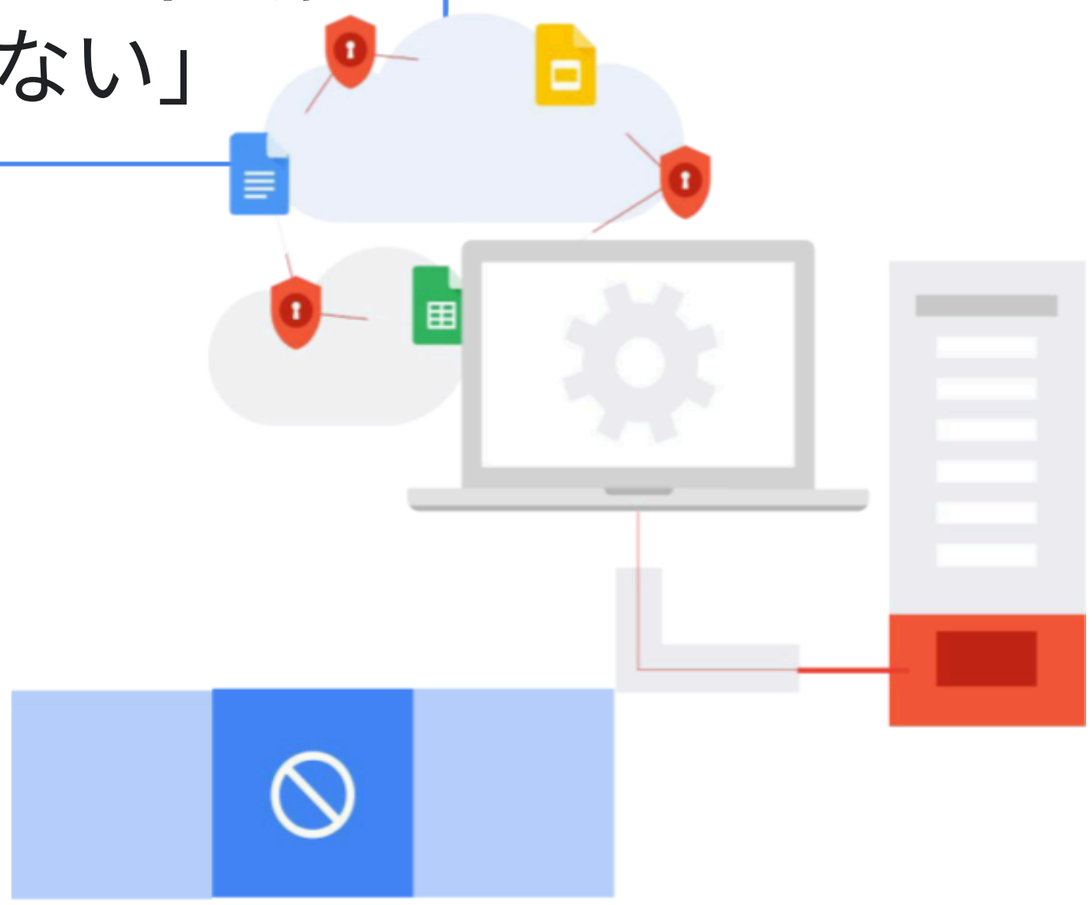
Chromebook は日々 5,000 万人もの生徒と教師に使用されています。アプリやウェブサイトへのアクセスを簡単に制限できる ChromeOS は教育機関のユースケースにも適しています。

Google 管理コンソールを使用すると、ユーザーがアクセスできるウェブ コンテンツや拡張機能についてポリシーを設定したり、JavaScript の実行、Cookie の設定、画像の読み込みなどを許可するサイトを指定したりできます。macOS や Windows 11 では、制限が設定されている場合でも、こうした制御を簡単に回避できます[2]。

chromeOS

6

「攻撃者は ChromeOS デバイスにリモートでアクセスできない」



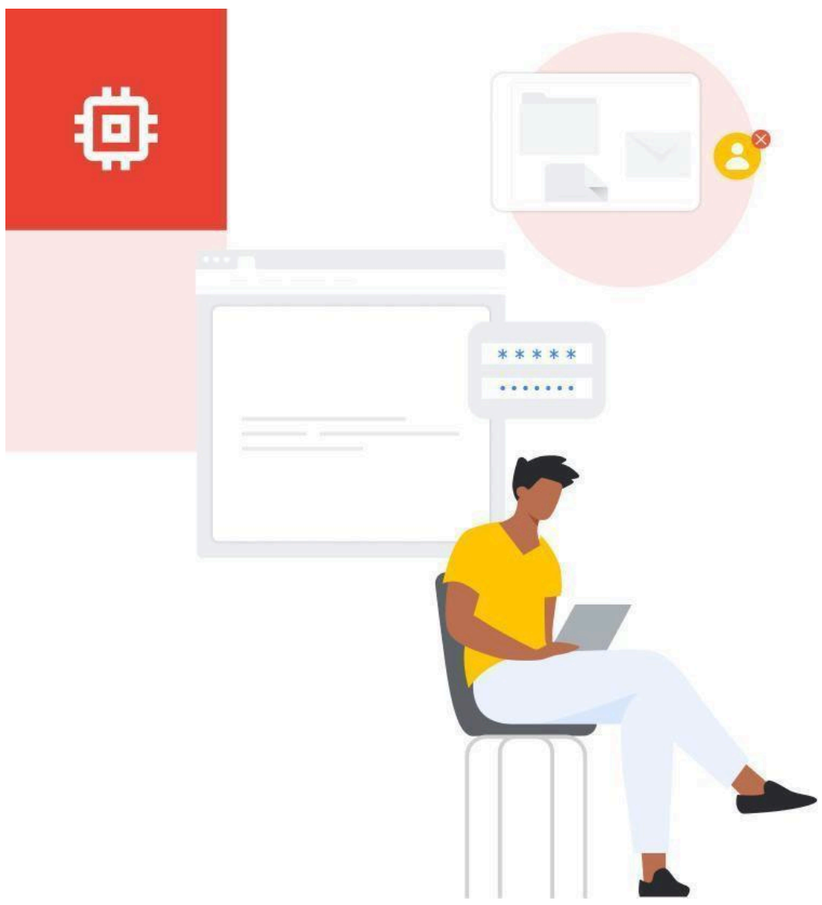
ChromeOS は、リモート アクセスの攻撃対象領域が小さくなるよう設計されています。

ChromeOS では、革新的なファイアウォール防御システムにより、犯罪者がサービス ディスカバリ プロトコルを利用してリクエストをポイズニングし、自身が制御するリソースへの接続をシステムに強制するのを防ぎます。macOS や Windows 11 でもファイアウォール防御を使用していますが、最終的な効果はあまり高いものとは言えません。いずれも ChromeOS のファイアウォールでは許可されないようなプロトコルを介したポイズニングに対して脆弱です[2]。

「デフォルトの動作と豊富な設定オプションに加え、アプリケーションで動作を変更できることで、ChromeOS はリモート攻撃対象領域を最も効果的に制限できるソリューションとして注目されています[2]。」

7

「Google セキュリティ チップで攻撃を阻止」



攻撃者がデータにアクセスするには ChromeOS デバイスに物理的にアクセスする必要があり、その場合も簡単には侵入できません。

Google Secure Microcontroller（H1）は、暗号鍵やローカルデータの保護といった ChromeOS のさまざまなセキュリティ機能で使われています。攻撃者が総当たり攻撃で何百万通りもパスワードや PIN コードの組み合わせを試してログインしようとしても、チップによって阻止されます[2]。

8

「自動更新によって常に最新のセキュリティ機能で保護」

定期的な更新はデータ セキュリティにとって不可欠ですが、一部のオペレーティング システムでは更新が不必要に複雑で時間のかかるものとなっています。

macOS では、新しい利用規約への同意やパスワードの再入力が必要になることがあります。また Windows 11 では、手動で設定しないと自動更新されません。ChromeOS では、デフォルトで自動更新がバックグラウンドで行われ、システムの再起動が必要な場合はユーザーに通知されます。高度に統合された設計の ChromeOS では、システムアップデートによりすべてのコンポーネントが一括更新されます[2]。

IT セキュリティに詳しくない従業員でもウェブ上で安全に作業できます。

ChromeOS は、ゼロトラストの原則に沿って設計された、デフォルトで高度に安全なインフラストラクチャです。どのデバイスも手にしたときから安全に使用でき、組織で追加のセキュリティ対策を設定する時間やコストを削減できます。

Atredis Partners による詳細な分析についてはこちらをご覧ください。

ChromeOS が企業の固有のニーズをどのように満たして、最初から競合システムより安全なエクスペリエンスを提供できるか[2]については、ChromeOS のスペシャリストにお問い合わせください。

chromeOS

[1] macOS や Windows 11 と比べて、ChromeOS は最も安全なエクスペリエンスを提供します。
[2] Google の委託により Atredis Partners が実施した調査、「Google ChromeOS Security Competitive Analysis Report」（2024 年 4 月）
[3] 2024 年 5 月現在、ChromeOS がウイルス攻撃またはランサムウェア攻撃の被害を受けたことを示すデータはありません。データは国内および社内の各種データベースの ChromeOS のモニタリングに基づきます。