

ChromeOS

スタートガイド

目次

ChromeOS スタートガイドをご覧くださいありがとうございます。
Google 管理コンソールの利用が初めてのお客様には、仕事の進め方を変革する方法をご案内します。
このガイドは ChromeOS の基本を説明するものです。既にご利用のお客様は、ご自身に関連するセクションまでスキップしてください。

はじめに.....	2
導入: 方法とベスト プラクティス.....	3
導入方法のチェックリスト.....	3
導入プロジェクトのキックオフ.....	4
ユーザー側の変革から始める.....	4
接続.....	5
ネットワーク プロファイルを管理する.....	6
Wi-Fi を設定する.....	6
デバイス単位の Wi-Fi 設定を追加する.....	6
Wi-Fi のセットアップ.....	8
クライアント証明書.....	8
ウェブ フィルタリング.....	8
デバイスの導入.....	9
ChromeOS の登録方法.....	9
企業の新規のお客様.....	9
教育機関の新規のお客様.....	10
非営利団体の新規のお客様.....	10
Google Workspace などですでにご利用のお客様.....	11
前提条件.....	11
登録.....	12
手動登録.....	13
多数のデバイスを手動登録する際の ベストプラクティス.....	14
ゼロタッチ登録.....	15
一括登録.....	15
導入シナリオ.....	15
クラウド ワーカーと現場スタッフ.....	16
単一の用途に特化したキオスク アプ リケーション.....	16
デジタル サイネージ.....	16

公開セッション デバイス.....	16
学力テスト.....	16
教育者.....	16
ChromeOS Flex の導入.....	17
インストール.....	17
一括導入.....	17
企業登録済みのデバイスを確認する.....	18
管理対象プロビジョニング登録サービス (任意).....	18
管理.....	19
アカウントを設定する.....	19
組織部門とポリシーを定義する.....	20
ポリシーに関する主要な留意事項.....	22
アプリと拡張機能.....	23
推奨設定.....	23
その他の考慮事項.....	25
印刷.....	25
Chrome Management API.....	25
Chrome Management Telemetry API.....	25
Directory API.....	26
Chrome Policy API.....	26
GAM.....	26
Apps Script.....	27
データ損失防止 (DLP).....	27
ChromeOS の導入とチェンジ マネジメント.....	28
ChromeOS 導入のワークストリーム.....	29
変革を通してユーザーをサポートする.....	30
ガバナンス.....	30
準備.....	31
コミュニケーション.....	34
トレーニング.....	36
「ChromeOS への移行」のサポート.....	42
さらにサポートが必要な場合.....	43
サポートを受ける.....	43
セルフサポートのヒント.....	43
補足資料.....	43

はじめに

ChromeOS スタートガイドをご覧くださいありがとうございます。本書は ChromeOS デバイスとデバイス管理を購入されたお客様、またはご購入を検討されているお客様を対象としています。

まずは、用語の定義を紹介します。

- **ChromeOS デバイス**(Chromebook、Chromebook Plus、Chromebase、Chromebox、タブレット、ChromeOS Flex で更新したデバイス)は、クラウドの利用に最適化されたオペレーティング システムである [ChromeOS](#) を実行するコンピューティング デバイスです。これらのデバイスの特徴は、自動的に更新され、パッチのインストールやマシンの定期的な再イメージングも不要であり、起動が速く、いくつかのセキュリティ機能が組み込まれていることです。
- **アップグレード**:
 - Chrome の[アップグレード](#)(デバイス管理のライセンス)は、教育機関向けまたは企業向けのそれぞれの ChromeOS デバイスに対して購入できます。また、ライセンス バンドル型の ChromeOS Enterprise デバイス(Chromebook Enterprise、Chromebase Enterprise、Chromebox Enterprise、Chromebook Plus Enterprise など)は、アップグレードを別途購入する必要はありません(国により Chrome Education Upgrade 付属の Chromebook で利用可能な場合もあります)。
 - Google のデバイス管理ソリューションにより、IT 管理者はクラウドベースの Google 管理コンソールで大規模にデバイスを管理、保護できます。企業データの安全を守る高度なセキュリティ機能があり、ユースケースにかかわらず柔軟にリソースにアクセス可能で、ChromeOS デバイスと他の重要なインフラストラクチャのマネジメントが簡素化されます。さまざまな顧客ニーズに対応できるよう、複数の ChromeOS デバイス管理アップグレード(Chrome Enterprise Upgrade、Chrome Education Upgrade、Kiosk and Signage Upgrade、Chrome Nonprofit Upgrade)が用意されています。
- [Google 管理コンソール](#)は、ChromeOS デバイスの一元管理に使用します。企業または学校の IT 管理者は、さまざまなデバイスを対象に Chrome ユーザー向けのエンタープライズ機能を管理できます。Google 管理コンソールを使用して、ポリシーの適用、ユーザー向けの Chrome 機能の設定、社内 VPN や Wi-Fi ネットワークへのアクセスの提供、アプリや拡張機能の自動インストールなどを行うことが可能です。

このガイドでは、購入方法、アカウントの設定、デバイスを登録する手順、ChromeOS 導入方法の共有、ポリシー設定、チェンジ マネジメント、ベスト プラクティス、プロセスの途中で想定されることについて説明します。

注: ChromeOS デバイスを教育機関や企業に導入する際の推奨事項は、Google がさまざまなお客様やパートナーと現場でやり取りする中で蓄積されたものです。体験談やご意見をお話くださった皆様に感謝申し上げます。

質問がある場合やサポートが必要な場合

[サポートページ](#)をご確認いただくか、一般的な質問については [Chrome Enterprise ヘルプ センター](#)をご覧ください。

導入: 方法とベスト プラクティス

デバイスの登録と展開を開始する前に、適切な展開手法と構成が整っていることを確認することで、パフォーマンスと導入の成功を確実にすることが可能です。

導入方法のチェックリスト

お客様と Google 社内チームがデバイスの導入準備に使用したチェックリストを紹介します。実施する前に、以下のカテゴリごとにデューデリジェンスを必ず行ってください。以下のセクションで、「導入プロジェクトのキックオフ」と「インフラストラクチャの構成」について説明します。「組織部門とポリシーの定義」については「[管理](#)」、「[マネージドプロビジョニングの準備](#)」については「[デバイスの導入](#)」で説明します。

☐ 導入プロジェクトのキックオフ

- ☐ 導入チームの定義
- ☐ 導入の詳細な計画
- ☐ プロジェクト計画の策定

☐ インフラストラクチャの構成

- ☐ ネットワーク接続
- ☐ 帯域幅容量の検証
- ☐ 印刷ソリューション

☐ 組織部門とポリシーの定義

- ☐ コンソール管理
- ☐ 管理者ロールの定義
- ☐ 組織部門階層
- ☐ デバイス ポリシー
- ☐ ユーザー ポリシー

☐ マネージド プロビジョニングの準備

- ☐ ChromeOS の最新ビルドへの更新
- ☐ 企業ドメインへのデバイスの登録
- ☐ 発送の準備
- ☐ デバイス スペックのテストと検証
- ☐ ハードウェア セットアップの検証
- ☐ デバイス ポリシーの構成
- ☐ ユーザー ポリシーの構成
- ☐ 導入チェックリストの作成

導入プロジェクトのキックオフ

新しいワークフローは、一朝一夕で導入できるものではありません。このプロセスは、従業員が仕事の習慣や手順に ChromeOS を組み込めるように、コミュニケーション、トレーニング、エンゲージメントを構成する基本要素に合わせて順次調整されます。成功する ChromeOS 導入の詳細な計画には、ChromeOS 導入プロセスの各段階にチェンジ マネジメントが組み込まれています。

ユーザー側の変革から始める

あらゆる組織変革プロジェクトの中心となるのがユーザーです。ユーザー側の ChromeOS デバイスの受け入れ態勢を整えるための構造的なアプローチを確立することが、最初の目標です。

主な決定事項

1. 導入を成功させるための社内の責任者は？
2. 対象となるユーザーと ChromeOS デバイスの用途は？
3. ChromeOS デバイスへの移行による仕事への影響は？
4. ChromeOS デバイスはユーザーのプライマリ デバイスになるか？
5. 導入の成功を評価する方法は(30 日後にユーザーの 50% が導入済みなど)？
6. ChromeOS デバイスへの移行をユーザーに周知する方法は？
7. ChromeOS デバイスの使用についてユーザーをトレーニングする方法は？

チェンジ マネジメント プランの効果:

- ChromeOS デバイスの使用によって仕事の効率が上がる理由をユーザーが理解する
- ユーザーに合わせてカスタマイズしたコミュニケーションで質問に対応する
- ユーザーがトレーニングを受けて ChromeOS デバイスを使えるようになる
- ChromeOS デバイスの導入をユーザー自身が決定する
- ユーザーと IT 管理者に対して継続的な働きかけとサポートを行う

上記の質問に対する回答をまとめ、「[ChromeOS の導入とチェンジ マネジメント](#)」セクションのガイダンスに沿って対応すると、組織内での ChromeOS の導入を加速させることができます。

接続

組織でワイヤレス接続を設定する際は、建物のどこからでも安定した接続が可能であることと、すべてのデバイスでオンライン作業を行えるだけのインターネット帯域幅が確保されていることを確認してください。ネットワークの管理方法、トラブルシューティング、VPN の設定などについて詳しくは、[接続性に関するヘルプ記事](#)をご覧ください。

主な機能

ChromeOS デバイスでは、一般的な Wi-Fi プロトコル (WEP、WPA、WPA2、WPA3、EAP-TLS、EAP-TTLS、EAP-PEAP、LEAP) がすべてサポートされています。また、一部の ChromeOS デバイスには 3G または 4G / LTE のモバイル インターネット アクセス ハードウェアが搭載されており、モバイル通信圏内にいてモバイルデータ プランを利用していれば動作します。

評価と導入のヒント

組織のネットワーク インフラストラクチャを正しく評価して準備することは、ユーザーに最適な環境を提供するために欠かせない重要な作業です。特に、職場や学校のように限られた空間で複数の ChromeOS デバイスが同時に使用される場所では、IT 管理者が適切な接続と帯域幅を確保する必要があります。

- **Wi-Fi** の通信範囲と密度をテストして、追加のアクセス ポイントが必要かどうかを評価します。このテストは、モバイル デバイスでサードパーティ製の Wi-Fi アナライザー アプリを使って実施できます。
- すべての建物のワイヤレス インフラストラクチャと接続形態について調査します。学校全体または会社全体に導入する前に調べることで、適切なワイヤレス接続を確保できます。通常は、ワイヤレス接続を専門に扱うパートナーに以下を依頼することをおすすめします。
 - 現地調査 - まず、既存の Wi-Fi ネットワークと、デバイスや他の Wi-Fi ネットワークによる周囲の干渉を分析する必要があります。
 - 導入 - 適切なセキュリティ、チャンネル選択、送受信電力を備えたアクセス ポイントを導入または再配置します。
- **ChromeOS** デバイスから必要な URL にアクセスできることを確認します。ChromeOS デバイスが正しく動作し、ポリシーとセキュリティ アップデートを受信するには、Google のネットワークにアクセスする必要があります。お客様の環境でインターネット アクセスを制限している場合でも、導入したデバイスがプロキシ認証や SSL インスペクションを行うことなく Google 固有の [URL](#) にアクセスできるようにする必要があります。

アクセス ポイントと帯域幅の考慮事項について詳しくは、[ChromeOS デバイス向けの企業ネットワークに関する記事](#)をご覧ください。

ネットワーク プロファイルを管理する

いつでも手動で ChromeOS デバイスに Wi-Fi ネットワークを追加できますが、[Google 管理コンソールを使用してネットワーク プロファイルを適用する](#)ことをおすすめします。これらのプロファイルは、登録プロセス中に ChromeOS デバイスにダウンロードされて適用されます。また、Wi-Fi ネットワーク プロファイルの更新は、ChromeOS デバイスでのポリシーの自動更新時に適用されます。Google 管理コンソールを使ってこれらの設定を適用するメリットの一つは、十分に複雑な事前共有キー (PSK) を使用でき、このキーをエンドユーザーと共有する必要がないことです。

Wi-Fi を設定する

ChromeOS デバイスを利用するお客様の多くは設定の簡単な WPA2-PSK を使用していますが、ChromeOS デバイスはさまざまな教育機関や企業の環境で利用可能です。クライアント証明書やシングル サインオン (SSO) を要し、ウェブ フィルタリング ソリューションが導入される、複雑な Wi-Fi 導入シナリオにも対応します。以下では、Wi-Fi やその他のネットワーク設定を準備するためのヒントを紹介します。

デバイス単位の Wi-Fi 設定を追加する

一部のユーザーまたは ChromeOS デバイスに異なる設定を適用するには、目的のユーザーまたはデバイスを配置した固有の組織部門を最上位組織または親組織の下に作り、各組織部門に対して設定を適用します。組織部門の詳細については、「[管理](#)」セクションをご覧ください。

カスタマイズする組織部門を選択して手動で継承を解除しない限り、子[組織部門](#)は親組織から Wi-Fi ネットワーク プロファイルを継承します。

- [組織構造の仕組み](#)、[Chrome ポリシー管理の概要](#)、別の組織部門に [ChromeOS デバイスを移動する手順](#)をご確認ください。

プロファイルを設定するには、SSID やセキュリティ タイプなどのネットワーク情報を提供する必要があります。サービスセット 識別子 (SSID) とパスフレーズでは大文字と小文字が区別される点に注意してください。

新しい Wi-Fi ネットワーク プロファイルを定義する際は、[自動的に接続する] チェックボックスと、[プラットフォームへのアクセス] セクションの [Chromebooks (ユーザー別)] でチェックボックスをオンにします。ネットワークの設定に関する技術的な詳細情報については、[こちら](#)をご覧ください。

プラットフォームへのアクセス

Android

Google のデフォルトに設定

☐ Android で有効

Chromebooks (ユーザー別)

Google のデフォルトに設定

☐ Chromebooks (ユーザー別) で有効

Chromebook (デバイス別)

JR Chrome に適用しました

☒ Chromebook (デバイス別) で有効

Google Meet ハードウェア

Google のデフォルトに設定

☐ Google Meet ハードウェア で有効

iOS

Google のデフォルトに設定

☐ iOS で有効

 Android と iOS の設定を適用するには、モバイルの詳細管理を有効にする必要があります。 [高度な管理を有効にする](#)

 Google Meet ハードウェアの設定を適用するには、Google Meet ハードウェアのライセンスをご購入いただく必要があります。

詳細

Google のデフォルトに設定

名前 * 

SSID * 

☐ 自動的に接続する

非公開ネットワーク

☐ これは非公開ネットワークです 

セキュリティ設定

セキュリティの種類

なし ▼

IP 設定

☐ デバイスで IP アドレスを設定できるようにする (Chrome OS のみ)

プロキシ設定

プロキシの種類

インターネットへの直接接続 ▼

DNS 設定

ネームサーバー

☐ ユーザーにこれらの値の変更を許可する

☒ 自動ネームサーバー

☐ Google ネームサーバー [詳細](#)

☐ カスタム ネームサーバー

静的 DNS サーバー

IP アドレスを 1 行に 1 つずつ入力してください。

カスタム検索用のドメイン

ドメインの値

ドメインを 1 行に 1 つずつ入力してください。DHCP の値を使用するには空欄のままにします。

保存

Wi-Fi のセットアップ

多くの場合は、オープンなネットワーク、または制限がかかっていないネットワークを使って ChromeOS デバイスを登録し、最初の管理ポリシーの同期を行うのが一番簡単です。このセットアップにより、IT 管理者が定義したネットワークプロファイルを ChromeOS デバイスで受信できるようになります。デバイスを設定したら、優先ネットワークのリストから、登録で一時的に利用した上記のネットワークを削除します。詳しくは、[ネットワークの情報を削除する](#)をご覧ください。

クライアント証明書

ChromeOS デバイスは 802.1x 認証に対応しており、IT 管理者が [ChromeOS デバイスでクライアント証明書をデプロイする](#) には、[Google Cloud 証明書コネクタ](#)、[Google 証明書登録拡張機能](#)、サードパーティ製拡張機能など、いくつかの方法があります。

組織で Simple Certificate Enrollment Protocol (SCEP) を使用して証明書をデプロイすることを検討されている場合は、[SCEP を使用して ChromeOS 用の証明書登録を設定する詳しい手順](#)をご覧ください。

ウェブフィルタリング

組織でネットワークフィルタリング デバイスを使ってセキュア ソケット レイヤ (SSL) インスペクションを行っている場合は、通常、chrome://settings/certificates の [認証局] タブにカスタムのルート証明書を追加する必要があります。ユーザーからのウェブ リクエストのほとんどにはこれに対応できますが、一部のシステムレベルのリクエストではこの証明書を使用しないため、ユーザーをあらゆるセキュリティリスクから保護するわけではありません。ChromeOS デバイスを TLS インスペクション、または外部トラフィックを制限するネットワークで適切に動作させるには、[こちらのリストのホスト名](#)を許可する必要があります。

SSL インスペクションを行うネットワークで ChromeOS デバイスを使用するには、[ネットワークへの SSL コンテンツ フィルタの設定](#)に関するページをご覧ください。組織に登録済みの ChromeOS デバイスにログインするすべてのドメイン ユーザーを対象に、カスタムのルート証明書をインストールする方法を説明しています。

再登録用の Wi-Fi

安全なネットワークを使用してユーザーが独自のネットワークに接続しないようにしている場合は、デバイスの再登録を可能にする 2 つ目の SSID を設定することをおすすめします。トラブルシューティング時には、デバイスを出荷時設定にリセットする、またはハードリセットすることが一般的です。この操作を行うと、設定済みのポリシーがすべて消去されます。デバイスを再登録してデバイス ポリシーを取得するには、インターネット接続を構築する必要があります。ポリシーを取得するために必要な Google サーバーへのアクセスのみに制限された 2 つ目の SSID により、簡単なプロセスでデバイスを出荷時設定にリセットできます。このプロセスには、モバイル アクセス ポイントやイーサネットのインターネット接続を使用することもできます。

デバイスの導入

導入するデバイスの数が少ない場合は、[クイックスタートガイド](#)のオンライン版をご利用ください。複数のオフィスがある場合など、ChromeOS デバイスを大規模なグループに導入したり、[デバイスを一括登録](#)したりする場合は、以下の手順をご覧ください。

ChromeOS の登録方法

ChromeOS Enterprise デバイス(ライセンス バンドル型)を使用していない場合

[Google 管理コンソール](#)を使って管理するには、[ChromeOS デバイス管理を購入](#)していただく必要があります。学校または企業向けの ChromeOS デバイス管理をご購入いただけます。詳しくは、[注文オプション](#)をご確認ください。

- [Google 管理コンソール](#)で、[保有しているライセンスの数と年間アップグレードの管理および更新方法](#)を確認します。
- 詳細については、Google ChromeOS デバイスの販売パートナーにお問い合わせください。認定パートナーとの取り引きがない場合は、[お近くの Google Cloud パートナー](#)を検索できます。

企業の新規のお客様

スタンドアロンの ChromeOS デバイス管理

1. ChromeOS デバイス管理(Chrome Enterprise Upgrade または Kiosk and Signage Upgrade)を購入する
2. [販売パートナー](#)が Google を通じて Google 管理コンソール アカウントの注文を処理する
3. Google 管理コンソールのログインに関するウェルカム レターが Google から届く
4. [ドメインの所有権を証明](#)する
5. ChromeOS デバイスを[登録する](#)

デバイス管理が付属された ChromeOS デバイス

1. デバイス管理が付属された ChromeOS デバイスを購入する
2. <https://chromeenterprise.google/os/upgrade> にアクセスして Google 管理コンソール アカウントを作成する
3. Google 管理コンソールにログインして設定を行う
4. [ドメインの所有権を証明](#)する
5. ChromeOS デバイスを[登録する](#)

教育機関の新規のお客様

スタンドアロンの ChromeOS デバイス管理

1. [Google Workspace for Education の承認をリクエストしてドメインの所有権を証明する](#)
2. ChromeOS デバイス管理 (Chrome Education Upgrade) を購入する
3. [販売パートナー](#) が Google を通じて注文を処理する
4. Google からウェルカム レターが届く
5. ChromeOS デバイスを[登録する](#)

デバイス管理が付属された ChromeOS デバイス

1. [Google Workspace for Education の承認をリクエストしてドメインの所有権を証明する](#)
2. デバイス管理が付属された ChromeOS デバイスを購入する
3. ChromeOS デバイスを[登録する](#)

非営利団体の新規のお客様

スタンドアロンの ChromeOS デバイス管理

1. [Google for Nonprofits | 非営利団体向けプログラム アカウントをリクエストし、審査の完了を待つ](#)
2. [Google Workspace for Nonprofits を有効化してドメインの所有権を証明する](#)
3. ChromeOS デバイス管理 (Chrome Nonprofit Upgrade) を購入する
4. [販売パートナー](#) が Google を通じて注文を処理する
5. Google からウェルカム レターが届く
6. ChromeOS デバイスを[登録する](#)

デバイス管理が付属された ChromeOS デバイス

1. [Google for Nonprofits | 非営利団体向けプログラム アカウントをリクエストし、審査の完了を待つ](#)
2. [Google Workspace for Nonprofits を有効化してドメインの所有権を証明する](#)
3. ChromeOS デバイスを[登録する](#)

Google Workspace などですでにご利用のお客様

スタンドアロンの ChromeOS デバイス管理

1. ChromeOS デバイス管理(Chrome Enterprise Upgrade、Chrome Education Upgrade、Chrome Nonprofit Upgrade、または Kiosk and Signage Upgrade)を購入する
2. [販売パートナー](#)が注文処理時にお客様の Google 管理コンソール アカウント情報を Google に送信する
3. Google からウェルカム レターが届く
4. ChromeOS デバイスを[登録する](#)

デバイス管理が付属された ChromeOS デバイス

1. デバイス管理が付属された ChromeOS デバイスを購入する
2. ChromeOS デバイスを[登録する](#)

Google 管理コンソールの次の 2 か所でアップグレードの合計数を確認できます。

- [お支払い] > [サブスクリプション] - Chrome、Android、Google Workspace のサブスクリプションが表示される
- [デバイス] > [Chrome] > [デバイス] > [アップグレード] をクリック - アップグレードの合計数が表示される

ドメインの所有権の証明、Google 管理コンソール、企業の登録などのトピックに関する詳細ガイドについては、「[ハウツー](#)」デモ動画の再生リストをご確認ください。

前提条件

ChromeOS デバイスを導入して一元管理するには、以下の準備ができていない必要があります。

IT 管理者

1. プライマリドメインに対する管理者権限

[Google 管理コンソール](#)で ChromeOS デバイス管理のポリシーを有効化し、[Google Cloud サポート ポータル](#)にアクセスできるようにするには、ドメインの所有権を Google に証明する必要があります。プライマリドメインに対する管理者権限が必要です。

- 管理者を確認するには、[こちらをクリック](#)します。
- 記事の手順に沿って[ドメインの所有権を証明](#)します。

2. Google 管理コンソールへのアクセス

ユーザー ポリシーとデバイス ポリシーを設定してデバイスの登録を有効にするために必要です。[こちら](#)からログインしてください。

- Google 管理コンソールの[特権管理者権限](#)を持っていない場合は、アカウントを作成するか、特権管理者から[アクセス権を委任](#)してもらう必要があります。
 - 組織の特権管理者に連絡して、Google 管理コンソールへのアクセス権を取得してください。特権管理者は、ChromeOS デバイス管理と Google サポート アクセスに関するロールと権限をユーザー アカウントに割り当てる必要があります。

3. 電話サポート、ヘルプ アシスタント、Google Cloud サポート センターへのアクセス

特権管理者は[サポート アクセス権限をドメイン ユーザーに委任](#)して、アカウント復元とサポート チケットのログイン用にチケットを管理できるようにすることが可能です。特権管理者はサポート ポータルで、委任されたユーザーをサポート権限が付与されたロールに追加する必要があります。サポート ポータルへのユーザーのアクセス権が付与されていることを検証するには、[こちら](#)でログイン アクセスを確認してください。

エンドユーザー

ChromeOS デバイスを使用するのに Google Workspace アカウントは必須ではありませんが、ユーザーが Google サービスを利用できるように Google アカウントを準備しておくことをおすすめします。詳細については、[ドメインにユーザーを追加する方法](#)をご覧ください。

ChromeOS デバイスの数が多い、または Google Workspace と同時に導入する場合

多数の ChromeOS デバイスを導入したり、Google Workspace と同時に初めて導入したりする場合は、[Google Cloud パートナー](#)と連携することをおすすめします。

登録

ChromeOS デバイスをエンドユーザーに配布する前に、ユーザーが快適に使用できる状態にする必要があります。最小要件は、ChromeOS デバイスをドメインに登録し、管理できるようにしておくことです。これにより、以降のデバイス ポリシーの更新が ChromeOS デバイ스에適用されるようになります。

Google 管理コンソールのセットアップ ガイドを見ましょう

Google 管理コンソールの [\[デバイス\]](#) > [\[Chrome\]](#) > [\[セットアップ ガイド\]](#) で、ユーザーと組織部門の作成、デバイスの登録、ポリシーの設定などの一般的なタスクについて説明した実践的なセットアップ ガイドを確認できます。

ChromeOS デバイスを最新バージョンに更新する

ChromeOS 搭載デバイスは、Wi-Fi またはイーサネットに接続すると自動的に更新を確認してダウンロードします。管理者が [デバイスの更新設定](#) で制限を設定していない限り、デバイスは最新バージョンに更新されます。ただし、多くのデバイスを更新する必要があり、ネットワーク帯域幅を節約したい場合は、キャッシュ サーバーで更新をローカルにキャッシュ保存できます。[Squid キャッシュ](#) は、キャッシュ保存に対応するために使用できるオープンソース ソフトウェアです。USB を使用して手動でデバイスを更新することもできます。

ChromeOS イメージを作成する

USB スティックを使って手動で ChromeOS デバイスを最新バージョンの ChromeOS に更新するには、以下が必要です。

1. 更新する ChromeOS デバイスのメーカーとモデルに関する情報
2. 8 GB 以上の容量を備えた、USB 2.0 以降のフラッシュドライブ
3. ChromeOS、Microsoft Windows、または macOS で稼働する Chrome ブラウザ
4. [Chromebook リカバリ ユーティリティ](#) をインストールし、デバイスのメーカーとモデルを正しく指定して USB リカバリ ディスクを作成する

デバイスの更新、復元、ワイプについて詳しくは、[こちら](#)をご覧ください。

注: 安定版リリースがイメージ書き込みツールで利用できるようになるまで 1 週間程度かかることがあります。

手動登録

デバイスを企業登録する手順

デバイスを企業登録するには(詳しい手順については[こちらの動画](#)をご覧ください):

1. [USB リカバリ デバイスを作成するか、無線\(OTA\)でデバイスを更新します](#)。デバイスが 10 台を超える場合は、USB の使用をおすすめします。
2. 再起動したら、使用言語、キーボードの種類、Wi-Fi ネットワークを選択します。
3. 利用規約に同意します。
4. ChromeOS デバイスにログインする前に、**Ctrl+Alt+E** キーを押して [企業の登録] ダイアログ ウィンドウを開きます。ログイン時に [企業の登録] をクリックして企業の登録を選択することもできます。

デバイスの企業登録を促すプロンプトが自動的に表示されることがあります

Chrome の[アップグレード](#)(デバイス管理のライセンス)がバンドルされた ChromeOS Enterprise デバイス(Chromebook Enterprise、Chromebase Enterprise、Chromebox Enterprise、Chromebook Plus Enterprise など)では、ユーザーがエンドユーザー使用許諾契約に同意した後、ログインする前に Google の管理対象アカウントでデバイスを登録するよう促すプロンプトが自動的に表示されます。表示されない場合は、Ctrl+Alt+E キーを押して登録できます。

5. ユーザー名とパスワード(ドメインの管理者または登録ユーザー)を入力し、[デバイスを登録] をクリックします。
デバイスが正しく登録されると、[このデバイスは組織の管理対象として登録されました] というメッセージが表示されます。
6. [完了] をクリックして最初のログインページに戻ります。ページ下部に [このデバイスは [ドメイン名].com によって管理されています] というメッセージが表示されます。

組織内のすべての ChromeOS デバイスに対してこの手順を繰り返します。デバイスの登録について詳しくは、[ChromeOS デバイスを登録する](#)をご覧ください。

多数のデバイスを手動登録する際のベストプラクティス

- 特権管理者アカウントを使用してデバイスを登録するのではなく、デバイスの登録のみを目的とした、管理者権限が不要なアカウントを作成できます。複数のアカウントを作成し、関連付けられているサービス(Google Workspace など)を削減できるので、アカウントの全体的なアクセスが減ります。「登録の権限」というポリシーで、これを可能にする設定がデフォルトで [許可] に設定されています。
- デバイスを配置する組織部門に登録用アカウントを直接割り当てると、デフォルトの動作でデバイスをルート組織部門(最上位の組織部門)に配置する代わりに、その組織部門にデバイスが登録されます。この変更を行うには、対象となる組織部門の [ユーザーとブラウザの設定] に移動して、[デバイスの登録] のポリシー値を [ChromeOS デバイスをユーザーの組織内に配置する] に変更します。たとえば、デバイスを「キオスク デバイス」組織部門に登録するには、上記の設定を変更した上で、この組織部門で登録用アカウントを作成し、このアカウントを使ってキオスク デバイスを組織部門に直接登録します。
- 1 つのアカウントを使って多数のデバイスを手動で登録する場合、アカウントへのログイン時の本人確認が行われる可能性が高くなります。本人確認に成功してスムーズに登録を進めるために、次の対策を実施できます。
 - 登録用アカウントには管理者権限も関連付けられているサービスもないことを踏まえて、2 要素認証を無効にする。
 - 確認方法として従業員 ID を使用する。
 - i. ユーザーの詳細に移動してユーザー情報を編集し、登録用アカウントに従業員 ID を追加します。
 - ii. [セキュリティ] > [認証] > [ログイン時の本人確認] に移動し、登録用アカウントの組織部門で [ユーザーのセキュリティ強化のために従業員の ID を使用します] チェックボックスをオンにします。

- iii. デバイスを登録する技術者または担当者にこの従業員 ID を共有すれば、ログイン時の本人確認でこの従業員 ID を使用して、登録プロセスを正常に完了できます。

重要: デバイスの登録を行わないと、デバイスをワイプして登録をやり直す必要が生じます。詳しくは、[ChromeOS デバイスのデータをワイプする](#)手順をご覧ください。

ゼロタッチ登録

手動登録の代わりに、ゼロタッチ登録 (ZTE) で事前プロビジョニング パートナーを通じたデバイスの自動登録が可能です。ゼロタッチ登録を使用すると、コンソールに予めデバイスが「事前プロビジョニング済み」ステータスで表示されます。事前プロビジョニング済みのデバイスをインターネットに接続するとすぐに自動登録が行われ、ステータスが「プロビジョニング済み」に変わります。ゼロタッチ登録は、ChromeOS デバイスが自宅に直接届くハイブリッド ワーカーやリモート ワーカー、現地の IT サポートがない遠隔地のデバイスに最適な方法です。

利用するには、[ゼロタッチ登録のヘルプ記事](#)を参照し、[デバイスがゼロタッチ登録に対応していることを確認して、事前プロビジョニングの認定パートナー](#)のサポートを受ける必要があります。この作業には、[事前プロビジョニング トークン](#)とお客様 ID を事前プロビジョニング パートナーに提供する必要があります。また、組織部門 (OU) ごとに一意のトークンを作成できます。これにより、デバイスを登録する場所を選択できるので、後から手動で移動する必要がなくなります。

一括登録

特に多数のデバイスを処理する場合は、手動登録に代わる方法として Chromebook の登録に使用するキー入力をエミュレートするサードパーティ製デバイスを使用した一括登録があります。デバイスの登録に必要な手順を自律的に実施できるので、1 人が一定期間に登録できる ChromeOS デバイスの数が大幅に増加します。

利用するには、ヘルプ記事の [Chromebook を一括登録する](#)をご覧ください。

導入シナリオ

ChromeOS デバイスは高いセキュリティとリモート管理を備え、メンテナンスをほとんど必要としないことから、[ビジネス](#)や[教育](#)の現場で多く採用されるようになってきました。ここからは、一般的な用途をご紹介します。

クラウド ワーカーと現場スタッフ

ChromeOS デバイスは企業の従業員に最適です。ウェブ アプリケーションへのアクセス、生産性向上ツールの使用、コラボレーションを可能にする[フルタイムのデバイス](#)として、ChromeOS デバイスをユーザーに割り当てることができます。[コンタクトセンター](#)のエージェント デバイスとして、[医療機関の臨床医向けデバイスや共有デバイス](#)として、製造業などのさまざまな場面でも使用できます。[詳細](#)

ChromeOS によってクラウド ワーカーを支援する方法について詳しくは、[Cloud Worker Live](#) の動画をご覧ください。

単一の用途に特化したキオスク アプリケーション

単一の用途に特化したキオスクアプリを作成できます。たとえば、顧客がカード申し込み情報を入力するためのアプリ、顧客が店内アンケートに記入するためのアプリ、学生情報を登録するためのアプリなどが考えられます。[詳細](#)

デジタル サイネージ

Chromebox をデジタル サイネージ ディスプレイとして使用し、学校行事の日程、デジタル看板、レストランのメニュー、インタラクティブ ゲームなどを表示できます。ホスト型アプリやパッケージ化アプリを作成し、シングルアプリ キオスクモードで画面全体に表示することが可能です。[詳細](#)

公開セッション デバイス

公開セッション デバイスを、従業員の休憩室や店舗のディスプレイなどに置いたり、図書館内の共有デバイスとして設置したりできます。この場合、ユーザーはログインしなくても ChromeOS デバイスを管理対象ゲスト セッションとして使用できます。[詳細](#)

学力テスト

Chromebook は、学力テストの管理に適した安全なプラットフォームです。適切に設定すれば、幼稚園から高校までのテスト規格に対応することができます。Chromebook では、試験中のウェブの閲覧や、外部ストレージ、スクリーンショット、印刷機能の利用を無効にできます。

試験の性質に応じて、シングルアプリ キオスクとして設定する、テスト実施者が指定するドメインに設定する、公開セッション キオスクを使用するなど、さまざまな方法で Chromebook を学力テスト用に設定できます。詳しくは、[Chromebook を学力テストに使用する](#)をご覧ください。

教育者

生徒の Chromebook と同じ環境で管理される Chromebook を教職員に提供することで、同じインターフェースを使い、ChromeOS のセキュリティで保護された状態で、教師向けの機能や[スクリーンキャスト](#)などのツールも活用できます。[教育機関向け Chromebook Plus の詳細](#)

ChromeOS Flex の導入

[ChromeOS Flex](#) では、IntelまたはAMDプロセッサを搭載した Microsoft Windows または macOS が搭載されたほとんどのデバイスに ChromeOS をインストールして、既存のハードウェアを活用しながら、ChromeOS のあらゆるメリットを得られます (ChromeOS FlexはARMアーキテクチャをサポートしていません)。ChromeOS Flex の利用を開始する前に、以下のことを行う必要があります。

1. お使いのデバイスが[認定モデル](#)の[リストに含まれている](#)かどうかを確認する。
2. [ChromeOS Flex と ChromeOS の違い](#)を理解する。
3. [ChromeOS Flex に関するよくある質問](#)を確認する。

ChromeOS Flex をデバイスにインストールしたら、[ChromeOS デバイス管理](#) (Chrome Enterprise Upgrade、Kiosk and Signage Upgrade、Chrome Nonprofit Upgrade、Chrome Education Upgrade などのソリューション) を使用してデバイスをドメインに登録し、他の ChromeOS デバイスと同様に管理できます。

インストール

ChromeOS Flex をインストールするには、以下が必要です。

1. 8 GB 以上の容量を備えた、USB 2.0 以降のフラッシュドライブ
2. ChromeOS、Microsoft Windows、または macOS で稼働する Chrome ブラウザ
3. [Chromebook リカバリ ユーティリティ](#)のインストール

準備ができれば、[ChromeOS Flex インストール ガイド](#)に記載されている手順に沿って、起動可能な USB の作成、USB からデバイスの起動、インストール、登録を行います。

デバイスのセキュリティを強化するために、[ChromeOS Flex 導入のベストプラクティス](#)も確認することをおすすめします。

一括導入

多数のデバイス(100 以上)に ChromeOS Flex をインストールする必要がある場合は、次のような[一括導入](#)ツールを利用して迅速に導入できます。

- [Microsoft Windows 展開サービス\(WDS\)](#)
- [Microsoft Windows System Center Configuration Manager\(SCCM\)](#)
- [Clonezilla](#)

各ツールに関する手順と要件は、上記のリンク先で確認できます。導入後は、必ず[デバイスを登録](#)してください。

企業登録済みのデバイスを確認する

[Google 管理コンソール](#)で、[登録済みの ChromeOS デバイス](#)を検索して表示し、デバイスの情報(シリアル番号、登録のユーザー名とステータス、アセット ID、ポリシー同期データ、サポート終了日、設置場所などを手入力したメモ)をデバイスリストで確認できます。シリアル番号をクリックして、各デバイスの詳細情報(デバイスにインストールされている OS のバージョン、MAC アドレス、最後にログインしたユーザーなど)を確認することもできます。役立つ情報をいくつかご紹介します。

- 歯車アイコン(リストの右上)をクリックして表示される列を管理する。
- デバイスをクリックして以下の操作を行う。
 - 移動、再起動、リモート デスクトップ、ログの取得、リセット、無効化、デバイスのデプロビジョニング、アップグレードの種類の変更
 - ハードウェア情報と OS 情報、カスタム フィールド、システム アクティビティ、トラブルシューティング用データ(ボリューム レベル、メモリ使用量、CPU 使用率、ディスク容量、Wi-Fi 電波強度)の表示
- 上部の [アップグレード] をクリックして、ChromeOS デバイス管理の利用可能なアップグレードを確認する。
- リスト表示にフィルタを追加する(一般的なフィルタとして、アップグレードのタイプ、Chrome のバージョン、OS バージョンのコンプライアンス、機種などがある)

企業登録が完了すると、管理者は次の操作を行えるようになります。

- [ChromeOS デバイスのデータをワイプする](#)
- [ワイプした ChromeOS デバイスを自動的に再登録する](#)

- [ChromeOS デバイスの修理、用途変更、廃棄](#)

Managed Provisioning Enrollment サービス (任意)

サービス パートナーより提供される Managed Provisioning Enrollment サービス (管理対象プロビジョニング サービス) は、ChromeOS デバイスを「ゼロ IT タッチ」で導入できるように設計されています。サービス パートナーに管理対象プロビジョニングを委託すると、納品された ChromeOS デバイスをすぐに使用できるというメリットがあります。ユーザーは ChromeOS デバイスを箱から出してすぐ、特に設定を行わなくても作業を開始できます。エンドユーザーのコンピューティング デバイスと同様に、管理コンソールで ChromeOS デバイスを適切な管理ポリシーに関連付けるための設定は必要です。販売パートナーの多くが、このサービスを提供しています。

出荷前に ChromeOS デバイスの管理対象プロビジョニングを行う販売パートナーなどの組織には、Google 管理コンソールのドメインの管理者以外のユーザー アカウントを登録用に提供できます。つまり、このアカウントはすべてのサービスを無効にした組織部門に追加します。

サービス パートナーが管理対象プロビジョニング サービスで行うのは次のようなことです。

- ChromeOS バージョンの更新
- ChromeOS デバイス管理への登録
- ポリシーの検証 (事前設定の Wi-Fi ネットワークなど)
- アセットのタグ付け
- レーザー刻印
- 周辺機器の同梱

詳しくは、担当の Google ChromeOS デバイス販売パートナー、または[お住まいの地域の Google Cloud パートナー](#)にお問い合わせください。

管理

企業や学校の IT 管理者は、クラウドベースの [Google 管理コンソール](#) で ChromeOS デバイスを管理できます。Google 管理コンソールで、[Wi-Fi 設定](#)、[プリインストールするアプリ](#)の選択、最新バージョンの ChromeOS への[デバイスの自動更新](#)など、[600 を超えるポリシー](#)を設定できます。

[こちらの動画](#)で Google 管理コンソールについて簡単に説明しています。

アカウントを設定する

管理アカウント

Google 管理コンソールを使用するには、組織内に少なくとも 1 人の特権管理者が必要です。このアカウントでは Google 管理コンソールと [Admin API](#) のすべての機能にアクセスでき、組織のアカウントのあらゆる設定を管理できます。アカウントのロックアウトを回避するため、特権管理者は 2 人以上にすることをおすすめします。

また、Google 管理コンソールの一部にアクセスできる管理者用の[カスタムロールを作成し、特定の組織部門に割り当て](#)て、管理者がその組織部門に登録されたデバイスとユーザーのみを管理できるようにすることも可能です。

登録用アカウント(任意)

管理者以外のアカウントを使用して ChromeOS デバイスを登録し、さらに登録ユーザーが所属する組織部門にデバイスを配置できます。

デフォルトでは、デバイスを登録すると最上位の組織部門に配置されます。これを変更するには、[デバイス] > [Chrome] > [設定] > [ユーザーとブラウザ] に移動して、「デバイスの登録」ポリシーを探します。

ユーザー アカウント

ユーザーがデバイスにログインできるようにするには、ユーザー アカウントが必要です。[ユーザーは 1 人ずつ、またはまとめて追加](#)できます。さらに、ユーザーに対して[シングル サインオン](#)を設定する、[Entra ID \(旧 Azure AD\) からのユーザーの自動プロビジョニングを設定する](#)、[データを LDAP サーバーと同期する](#)、[パスワードを Active Directory と同期する](#)こともできます。

キオスクモードと管理対象ゲスト セッションでは、ユーザー アカウントを使用する必要はありません。

組織部門とポリシーを定義する

[Google 管理コンソール](#)を使用してユーザーを管理すると、Google 管理コンソールの Chrome 管理セクションで、デバイスポリシーとユーザー ポリシーを組織部門ごとに設定できるようになります。

- [デバイス] > [Chrome] で Chrome 管理にアクセスする

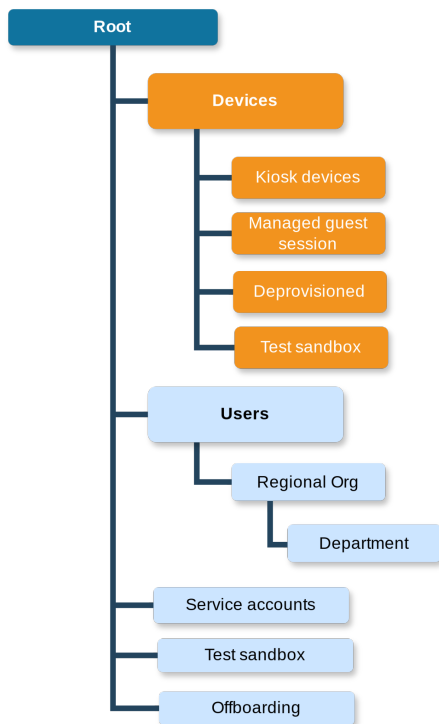
ユーザーやデバイス別にサービスのアクセスまたは設定をカスタマイズする必要がある場合は、組織構造を定義します。[各種ポリシーの違いを理解](#)すれば、より動的な組織部門構造を作成できます。[ユーザーとデバイスのポリシーについて](#)をご覧ください。

[デバイスレベルの設定はデバイスを使用するすべてのユーザーに適用されます](#)。ゲストとしてログインしている場合や、個人の Gmail アカウントでログインしている場合も対象です。これらのポリシーは、管理対象ゲスト セッション モードとキオスクモードのデバイスにも適用できます。自動更新ポリシー、自動的に再登録、ログイン画面のポリシー、キオスクの電源設定、電源とシャットダウンなどの設定が用意されています。

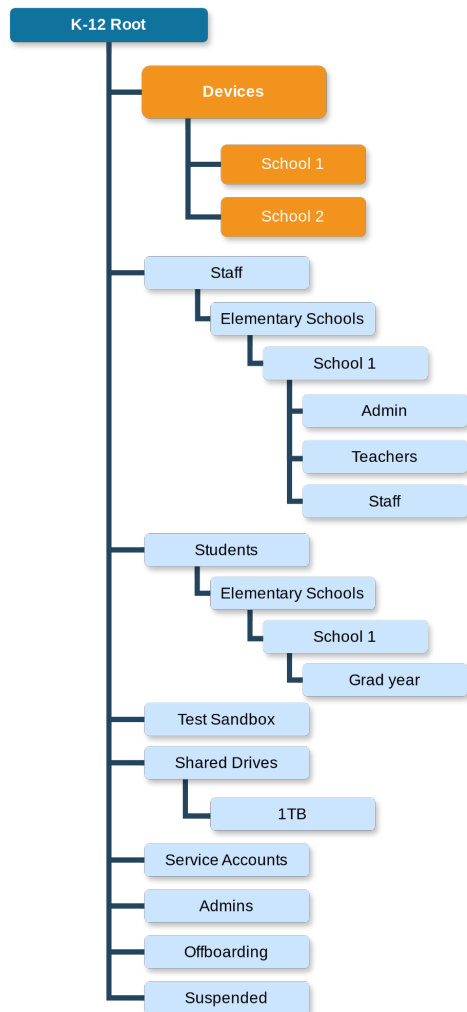
ユーザーとブラウザの設定は、ユーザーがログインするあらゆる場所（登録済みおよび未登録の ChromeOS デバイスを含む）で適用されます。これらの設定を使用して、セキュリティ ポリシーやユーザー エクスペリエンスを設定し、ユーザーによるダウンロードやアクセスの対象などを制御できます。詳しくは、[ユーザーまたはブラウザに Chrome のポリシーを設定する](#)をご覧ください。

ユーザーが利用できるサービスや機能は、そのユーザーが所属する組織部門によって決まります。[組織構造の仕組み](#)を確認して、組織部門の構造を決定してください。おすすめの例を以下でご紹介します。

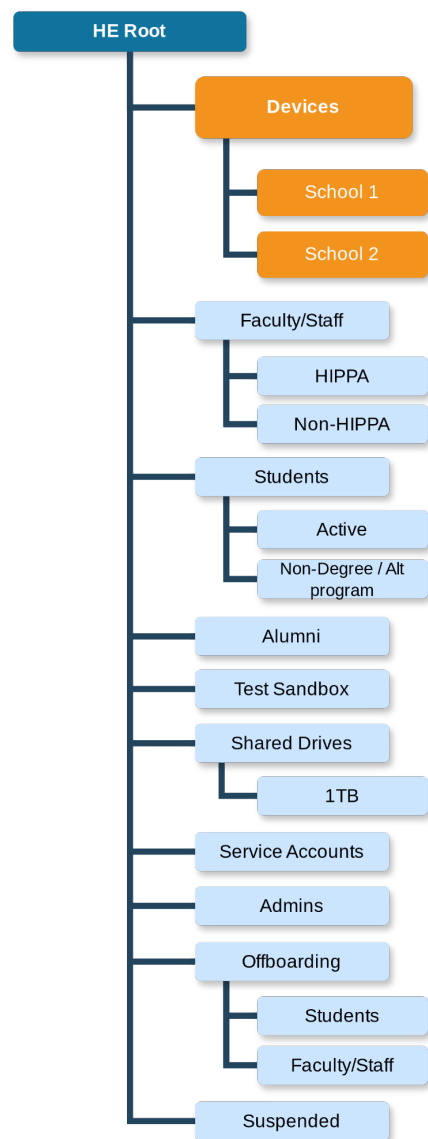
企業の例



K-12 の例



高等教育機関の例



ベストプラクティス: デバイスとユーザーを複数の組織部門に分けることで柔軟性が高まり、ユーザー プロファイルおよびポリシーとは別にデバイス ポリシーを適用できます。

Google 管理コンソールの組織構造によって制御されるのは、ユーザーが利用できるサービスと機能だけです。この構造は LDAP 構造に合わせて作成することもできますが、必ずしもその必要はありません。Google の組織構造は、必要に応じてさまざまな設計に合わせることができます。

Google 管理コンソールの組織構造に Microsoft Active Directory や LDAP 組織構造を複製する場合は、[Google Cloud Directory Sync](#) ツールを使用できます。



ChromeOS ポリシーに加え、[Chrome Enterprise Core](#) と [Chrome Enterprise Premium](#) を使用して、ログイン ユーザー用のブラウザ ポリシーを管理できます。[ブラウザを登録して](#)、Windows や macOS などのデバイスで Chrome を使用しているすべてのユーザーにポリシーを適用する方法をご確認ください。

ポリシーに関する主要な留意事項

ChromeOS デバイスは、ほぼすべての教育機関や企業の環境で機能するように設定できます。ChromeOS デバイスを導入する際、管理者は次の方法で、Wi-Fi ネットワークへのアクセス、ウェブ フィルタリング、プリインストール済みのアプリといったさまざまな要素を制御できます。

- デバイスの設定 - ログインするユーザーに関係なく、組織の管理対象 ChromeOS デバイスに設定やポリシーを適用する場合に使用できます。たとえば、ログインを特定のユーザーに制限したり、ゲストモードをブロックしたり、自動更新を設定したりできます。[詳細](#)
- ユーザーとブラウザの設定 - 使用する ChromeOS デバイスに関係なく、組織のユーザーに設定やポリシーを適用する場合に使用できます。たとえば IT 管理者は、特定のユーザー用にアプリをプリインストールしたり、セーフ ブラウジングを適用したり、シングル サインオン (SSO) を設定したりできます。また、特定のプラグインをブロックしたり、特定の URL をブロックリストに登録したり、ブックマークを管理したりすることも可能です。他にも多くの設定を組織内のユーザーに適用できます。[詳細](#)
- 管理対象ゲスト セッションの設定 - ドメイン内の[共有デバイスの設定](#)を行う場合に使用できます。管理対象ゲスト セッションを使用すると、ログインや認証を行わなくても複数のユーザーが同じ ChromeOS デバイスを共有できます。一定の時間が経過したらユーザーをログアウトさせるなどの設定を適用できます。
- キオスクの設定 - キオスクアプリには、デバイスの IME 機能とネットワーク設定の制限など、デバイス全体の設定を制御する特別な権限が追加されます。キオスクアプリでは 1 つの Chrome アプリが全画面で実行され、他のアプリケーションに切り替えることはできません。一般的なユースケースとして、教育機関用の標準的なテスト アプリケーション、デジタル サイネージ ディスプレイ、小売店で使用する単一の用途に特化したデバイス、コールセンター、VDI シン クライアントなどがあります。

自社に適した設定を選ぶには:

1. ご使用の環境でモデルとなる ChromeOS デバイスをどのように設定したいかをメモします。
2. Google 管理コンソールで、テスト用に 1 つの組織部門を使って、それらの設定をポリシーとして指定します。
3. 設定 (起動時に読み込むデフォルトのページ、プリインストールするウェブアプリ、ブロックリストに登録する URL など) を選択してこの組織部門の ChromeOS デバイスで検証した後、これらの設定をドメイン全体で複製できます。

前述の[登録用アカウント](#)を設定していない場合、ChromeOS デバイスは自動的に最上位組織で登録されます。[組織部門を追加](#)して複数のユーザー コホート(対象となる集団)やデバイス グループにカスタム ポリシーを適用し、[ChromeOS デバイスを異なる組織部門に移動する方法をご確認ください](#)。本ドキュメントで前述した登録方法を利用して、目的の組織部門に直接デバイスを登録することもできます。

アプリと拡張機能

[デバイス] > [Chrome] > [アプリと拡張機能] で、[アプリケーションと拡張機能を表示して設定](#)できます。オフライン Gmail や Google ドライブなど、ユーザーに関連するウェブアプリ、[Android アプリ](#)^{*}、または Chrome アプリを選択し、[アプリを自動的にインストール](#)してタスクバーに固定できます。さらに、[Chrome ウェブストア](#)または [Google Play ストア](#)からユーザーがインストールできるアプリと拡張機能を細かく制御する場合は、[アプリをブロックリストまたは許可リストに登録](#)できます。

プリインストール済みアプリの削除: プリインストール済みのアプリケーションを削除するには、リストにアプリケーションを追加して [ブロック] を選択します。すでにログインしているユーザーがこの変更を確認するには、アカウントを削除してからもう一度デバイスに追加する必要があります。この変更は、デバイスに初めてログインする全ユーザーにすぐに適用されます。

*Android アプリを使用できるのは、ChromeOS デバイスにログインしているユーザーだけです。ChromeOS Flex デバイスや、管理対象ゲストモードまたはキオスクモードのデバイスでは使用できません。

推奨設定

Google 管理コンソールの [デバイス] > [Chrome] > [設定] で、[ユーザーとブラウザ]、[デバイス]、[管理対象ゲスト セッション] 設定の多数のポリシーにアクセスできます。

- [フィルタを追加または検索] にキーワードを入力して、設定をフィルタできます。
- ChromeOS、ブラウザ (Windows、Mac、Linux)、Android デバイスに関する設定を、組織部門ごとにローカルで適用したり、トップドメインから継承したりすることができます。
- このビューの [継承] 列でポリシーの継承を確認することも、検索バーの [継承] フィルタを使用して、ローカルで適用されているポリシーまたは継承されたポリシーを表示することもできます。
- 各設定のアイコンを見れば、ポリシーが適用される対象を把握できます (ChromeOS デバイス、Windows、Mac、Linux 版のブラウザ、Android デバイス、iPhone と iPad)。



- 各ポリシーをクリックして詳細(使用可能な値や効果など)を確認できます。

ほとんどの組織はデフォルトのまま使用しますが、組織によってはカスタマイズすることもあります。カスタマイズがよく行われる項目は次のとおりです。

自動的に再登録

この設定はオンにしておくことをおすすめします。ワイプされたデバイスが自動的にドメインに再登録されます。ChromeOS デバイスがドメインに再登録されないようにするには、デバイスを[デプロビジョニング](#)する必要があります。[自動再登録の詳細](#)

ログイン画面の電源管理	アイドル時またはカバーを閉じた際に画面が自動的にロックされるように設定すると、安全性が強化され、ユーザーが席を離れたときに他のユーザーにパソコンを使用される可能性が低くなります。AC 接続時とバッテリー駆動時に画面がロックされるまでの時間を指定することもできます。
起動時に読み込むページ	通常はイントラネット ポータルまたはホームページに設定します。このページを設定すると、ChromeOS デバイスを再起動したときに前回の閲覧セッションと同じタブが復元されなくなります。
ログインの制限	ログインを *[ドメイン名].com のユーザーのみに制限すると、一般ユーザー向け Gmail アカウントや別ドメインのアカウントを使ってログインすることができなくなります。これにより、管理対象(登録済み)の ChromeOS デバイスにログインできるユーザーを制御できます。
自動更新の設定	自動更新の設定はデフォルトのままにしておきます。ChromeOS デバイスは 4 週間おきに自動的に更新され、新機能、バグの修正、セキュリティの脆弱性の修正が追加されます。また、今後の ChromeOS リリースの動作を組織でテストできるように、組織の 5% のユーザーは Beta チャンネルまたは Dev チャンネルを使用するようにしておくことをおすすめします。ChromeOS デバイスの自動更新の展開と ChromeOS リリースのおすすめの使用方法に関する記事で、推奨事項を確認してください。 注: デバイスを登録して再起動する前に、バックグラウンドでの更新のダウンロードを停止するには、エンドユーザー使用許諾契約の画面で Ctrl+Alt+E キーを押します。これを行わないと、ユーザーがデバイスを再起動したときに、ポリシーでブロックされるべきダウンロード済みの更新が適用される可能性があります。
シングル サインオン	シングル サインオン(SSO)を使用する組織の場合は、組織全体に展開する前に、少数のユーザーで ChromeOS デバイスへのログインをテストします。 ChromeOS デバイスに SAML シングル サインオンを設定する方法、および Microsoft Entra ID と ChromeOS 間の SSO およびユーザー プロビジョニングを設定する方法の完全ガイドをご覧ください。
セキュリティ	Elevating Security 構成ガイドで、デバイスとユーザーのセキュリティを最大限に高める、おすすめのポリシー設定について説明しています。

その他の考慮事項

印刷

Google 管理コンソールには、組織内での印刷を管理できる包括的な機能スイートが用意されています。これらの機能によって、管理者は印刷デバイスやプリント サーバーへのアクセス、印刷パートナーの設定を制御できます。

- [プリンタの管理](#): 管理者には、プリンタを追加、削除、設定する(プリンタの名前、場所、アクセス承認の指定など)権限が付与されます。
- [プリント サーバーの管理](#): 管理者は Google 管理コンソールで CUPS プリント サーバーを追加、削除できます。
- [印刷パートナーの設定](#): 管理者は、インターネット印刷プロトコル(IPP)ベースの印刷キューを作成してネットワーク経由で印刷ジョブを送信するか、拡張機能を使用してプリンタを追加することで、印刷パートナーが提供する印刷サービスを設定できます。

Chrome Management API

管理者は [Chrome Management API](#) を活用して、自動化、スケーリング、情報のエクスポートなど、環境をプログラムで操作できます。一般的な API をいくつかご紹介します。

Chrome Management Telemetry API

この API を使用すると、ChromeOS 搭載デバイスの動作と健全性をモニタリングし、デバイスから送信されるテレメトリー イベントだけでなく、バッテリーの状態、CPU、ストレージ、メモリ、ネットワーキング、更新、音声、Wi-Fi 電波強度などの情報も取得できます。詳細、コードサンプル、API のテストについては、[Telemetry API ガイド](#)をご確認ください。

Directory API

この API では、デバイス識別情報を取得して、移動、更新、デプロビジョニング、無効化などの操作を行うことで、ChromeOS デバイスを管理できます。詳細については、[Directory API ガイド](#)をご覧ください。

Chrome Policy API

Chrome 管理者は Chrome Policy API を使用して、Chrome ポリシーをプログラムで表示および管理し、適用されているポリシーを一覧表示して変更、削除できます。詳細、一般的なユースケース、コードサンプルについては、[Chrome policy API ガイド](#)をご覧ください。

GAM

GAM(Google Apps Manager)は、管理者がコマンドラインから ChromeOS や他の Google Workspace サービスを管理できるオープンソースのコマンドライン ツールです。GAM を使用して以下のようなさまざまな作業を行います。

- ユーザー アカウントの管理
- デバイスの管理
- Chrome ポリシーの設定

- レポート
- その他

GAM は ChromeOS や他の Google Workspace サービスの管理を効率化するために使用できる優れたツールです。ChromeOS デバイスやユーザーの数が多い組織では特に役立ちます。

GAM の主な機能

- クロス プラットフォームのサポート: GAM は、Windows、macOS、Linux で利用できます。
- コマンドライン インターフェース: GAM のコマンドライン インターフェースでは、タスクの自動化や他のシステムとの連携を簡単に行えます。
- 詳細な[ドキュメント](#): GAM には詳細なドキュメントが用意されており、ツールの使い方を簡単に確認できます。
- アクティブな[コミュニティ](#): GAM には、他のユーザーを積極的に支援してくれる大規模なユーザー コミュニティがあります。

GAM を使用するメリット

GAM の使用には数多くのメリットがあります。

- 効率性の改善: GAM を使用することで、管理者はより効率的にタスクを自動化して ChromeOS を管理し、スクリプトで実行されるタスクを作成して一括操作できるようになります。
- 無料: オープンソースなので費用はかかりません。

Apps Script

[Apps Script](#) は Google ドライブを活用したクラウドベースの JavaScript プラットフォームで、Google プロダクト全体でタスクの統合と自動化を可能にします。Google スプレッドシートなどの Google エディタと連携してうまく機能します。GAM と同様の方法で Apps Script を使用して、より柔軟に他の API と連携できます。Apps Script は無料で利用できます。

データ損失防止 (DLP)

データ損失防止 (DLP) はシグナルを識別して、クリップボード操作、画面共有、印刷、電子プライバシー画面などのルールを実装します。個々の URL (ウェブアプリ) と種類 (Android、Linux、VDI) 別に DLP 制限を適用できます。ポリシーは、オンラインとオフラインの両方でルールに基づいてデバイスで適用されます。

DLP アクション

DLP で、指定されたルールに基づいて特定のアクションをブロック、許可、報告します。

- ブロック: アクションの実行をブロックする。
- 警告: リスクがあっても続行するかどうかを確認する。
- 報告: アクションの実行をブロックせずに、管理者に報告する。

- 許可: アクションの実行を許可し、管理者への報告を行わない。

DLP 機能

- クリップボード、スクリーン キャプチャ、画面共有、印刷、電子プライバシー画面
- セキュリティ調査ツールとの連携
- 管理対象ユーザー セッションと管理対象ゲスト セッション
- ChromeOS デバイス

注意点

- ソースは URL のみで、パターンに対応している。
- キオスクモードはサポートされない。
- Android、Linux VDI は 1 つの blob として扱われる(たとえば、URL からすべての Android または VDI アプリにコピー / 貼り付けすることはできるが、個々のアプリに行くことはできない)。

DLP を設定するには、[こちらの記事](#)をご覧ください。

ChromeOS の導入とチェンジ マネジメント

新しいテクノロジーを導入して変化を受け入れるのは、難しい場合があります。そこで、チェンジ マネジメント手法を ChromeOS 導入プロジェクトの各段階に組み込むことで、プロジェクトの目標を予定どおりに予算内で達成できるよう後押しします。組織はユーザー グループと各コホート(対象となる集団)のトレーニング ニーズを評価する時間を設ける必要があります。通常、作業環境がどのように変わるかを理解してもらうために、コホートにはユースケースごとに固有のトレーニングが必要です。

ユーザー側の ChromeOS の受け入れ態勢を整えるための構造的なアプローチを確立することが、Google の主な目標です。体系的なチェンジ マネジメント プランにより、従業員は以下のことが可能になります。

- ChromeOS デバイスを使用するメリットを理解する
- ChromeOS デバイスを使用するための知識、スキル、能力を持つ
- ChromeOS デバイスを導入してビジネスの目標を達成する

導入の成功を後押しする詳細な手順を提供するために、[従業員 Chromebook 導入キット](#)を共有してください。

チェンジ マネジメントを行っているチームは、プロジェクトの障害になり得る課題を早いうちに察知して行動し、成功につながるビジョンの設定に集中できます。チェンジ マネジメントの 4 つの段階について考えてみましょう。

刺激

- 関係者を引き込む
- 支持を取り付けて範囲を決め、サポートモデル、コミュニケーション、トレーニングを計画する

有効化

- サービスをデプロイする
- サービスをデプロイし、サポートモデル、トレーニング、コミュニケーションの計画を実施する

展開

- 導入を拡大する
- Google チームを編成し、トランスフォーメーション ワークショップを実施して、サポート オペレーションを管理する

組み込み

- 成功を評価して促進する
- 導入の進捗を評価し、成功事例を紹介して、社内でユーザーをサポートする
- 導入とチェンジ マネジメントのワークストリーム

刺激

有効化

展開

組み込み

ガバナンス

準備

コミュニケーション

トレーニング

リリース サポート

ChromeOS 導入のワークストリーム

技術構成

- 最高のユーザー エクスペリエンスを実現する
- 統合ポイントを特定する
- 技術的課題の早期解決を可能にする

プロジェクト管理

- プロジェクトを予定どおりに進める
- リソースを整理する
- 関係者を連携させる
- 稼働を管理する

チェンジ マネジメント

- 組織の移行コストを削減する
- ユーザーがツールの機能を十分に活用できるようにする
- 適切なトレーニングとサポート資料を提供する
- ポジティブな評価を得る

変革を通してユーザーをサポートする

ガバナンス	- 変革の顔となる変革リーダーを擁立する - 先導役となる「ChromeOS 支持者」を選んでトレーニングする - シニア マネジメントなどが手本となって主導する
準備	- ユーザーとユースケースを適切なコホートに分類する - コホートごとに変革の影響を評価する - コホートごとにチェンジ マネジメントの成果を定義する
コミュニケーション	- コホートごとにコミュニケーション ニーズを特定する - すべてのコホート向けのコミュニケーション プランを作成する - キャンペーンを実施する
トレーニング	- コホートごとにトレーニング ニーズを特定する - コホートごとにカリキュラムを作成してトレーニングを実施する - 印刷可能なユーザーガイドと ChromeOS の社内サイトを作る
リリース サポート	- コホートごとにコミュニケーション ニーズを特定する - すべてのコホート向けのコミュニケーション プランを作成する - キャンペーンを実施する

ガバナンス

このプロジェクトを成功させるための社内の責任者は？

変革の顔となる変革リーダーを擁立します。リーダーシップとエンゲージメントによって変革のビジョンを統一し、従業員が変革を受け入れるきっかけや動機を作ります。アクティブでわかりやすいリーダーシップの存在は、導入を成功させるための第一条件と言えます。

適切な支持者の属性

- 変革の顔となる部門のシニアメンバー(IT 以外)
- 模範となる人
- 組織内で顔が広く、尊敬されている、影響力のある人
- プロジェクト全体を通して積極的にサポートを行う能力がある

役割と責任

- プロジェクトの「エレベーター ピッチ」に承認を与える
- 組織にプロジェクトを発表する
- プロジェクトの目標、取り組み、メッセージに沿ってリーダーシップ チームを調整する
- リーダーや従業員の反発に対処する
- プロジェクトの成功を称える

成功のためのヒント

- 上層部による積極的かつ献身的な目に見える支持は成功に不可欠であり、従業員のエンゲージメントを高めて最大限の賛同を引き出す

導入をサポートする: ChromeOS Champions

ChromeOS Champions は、オンボーディング エクスペリエンスを改善してユーザーの利用を促進することを目的としています。このプログラムでは ChromeOS に移行するユーザーを同僚がサポートすることで、効率的な管理しやすい導入を実現します。

ChromeOS Champions のネットワークを募る

- ChromeOS に興味があり導入に積極的な、技術に精通した従業員
- ロールアウト時に同僚をサポートできる
- 稼働後も導入の状況を確認するためのイノベーション評議会に参加する
- 物理的場所ごとに 1 人以上を目標とする

役割と責任

- ChromeOS デバイスのトレーニングを先行して受け、十分な知識を習得する
- ChromeOS の導入に向けた組織の変革について理解する
- 同僚の関心を喚起し、フィードバックや質問を収集する
- 導入時に同僚をサポートする（見回り、Q & A セッションなど）
- 社内向けのよくある質問、役立つ情報、[ヒントとコツ](#)を維持管理する

準備

対象ユーザーとユースケースは？

プロジェクト開始時に特定した、組織における ChromeOS デバイスのすべての用途を確認します。組織のユースケースを把握することで、コミュニケーションとトレーニングのアセットに必要なコンテンツを作成できます。

例:

- コンピューティング
 - Chrome とウェブ アプリケーションのみ(クラウドベース)
 - デスクトップ仮想化
 - 既存の仮想化インフラストラクチャを活用
 - 新しい仮想化インフラストラクチャを構築
- [デジタル サイネージとキオスク](#)
- e ラーニング
- [管理対象ゲスト セッション](#)

チェンジ マネジメントの対象となるコホートを特定する

ChromeOS に移行する組織内のユーザーを特定して、ユースケースごとにグループ化します。ユーザー グループやそのニーズを把握することで、適切なメッセージやトレーニングを適切なユーザーに届けることができます。ChromeOS 支持者に各コホートをサポートしてもらうことをおすすめします。

例:

ユーザー

- 経営幹部
- 管理職員
- IT 管理者
- 管理者
- 従業員
- エンドユーザー サポート

ユースケース

- コンピューティング
- デスクトップ仮想化
- デジタル サイネージ
- キオスク
- e ラーニング
- 管理対象ゲスト セッション
- デバイス管理
- Chromebox for meetings

コホート

- 管理者、従業員、管理職員
- コンピューティング
- 従業員 - デジタル サイネージ
- IT 管理者 - デバイス管理

コホート(対象となる集団)を作成する



変革による影響の評価

ChromeOS デバイスの使用によって変わる業務について考えましょう。ChromeOS を使用することで変わる、または新たに生じる作業とワークフローをリストアップします。ChromeOS デバイスが作業環境に与える影響を理解することで、コミュニケーションとトレーニングのアセットに必要なコンテンツを作成できます。

変革の影響に関するコホート分析を行う

主要な変革によって作業環境に影響が生じる組織内のコホートを特定します。コホートと変革による影響を把握することで、適切なメッセージやトレーニング カリキュラムを適切なユーザーに届けることができます。

例:

- アプリケーションの互換性(およびギャップがある場合の対応方法)
- 管理ポリシーのマッピング / 代替案
- クラウド ファイル管理(Google ドライブ)
- 印刷
- 周辺機器の互換性
- デバイスの共有
- サポート / ヘルプデスク

導入の成果を評価する方法は？

ベンチマークを設定する

導入中に確認できるように、開始前に ChromeOS の成果を評価する指標を明確に定義しましょう。指標を追跡することで、問題を早期発見し、必要に応じて軌道修正できます。組織がデバイスを購入したそもそもの理由につながる主な指標を特定します。

例:

- トレーニングと教育のデータ
- トレーニング参加者数
- 以前と比較したヘルプデスクのチケット数
- ユーザー アンケートのデータ
- ユーザー準備アンケートのデータ
- 導入満足度アンケートのデータ
- 従業員のビジネスデータ
- 従業員 1 人あたりの平均コストまたはパフォーマンス

コミュニケーション

変革をユーザーに周知する方法は？

コミュニケーションを計画する

変革を前に「コミュニケーションの取りすぎ」ということは決してありません。またメッセージを伝えるために役立つリソースは無数にあります。

適切な相手に適切なメッセージを発する

- コホート別にコミュニケーションをカスタマイズし、疑問に答える必要がある
- ChromeOS に切り替えることで得られる業務上の改善点をユーザーが理解できるように、コミュニケーションは受け手に関連する内容にする必要がある
- ChromeOS を受け入れることでユーザーに生じ得るリスクを減らす
- チェンジ マネジメントのコホート分析を活用し、各コホートに適したコミュニケーション コンテンツを作成する

適切なチャネルで適切なメッセージを発する

組織内のユーザーにリーチするための適切なコミュニケーション チャネルを特定し、各コミュニケーションの有効性を評価します。

例: メール、社内コラボレーション、ユーザーガイド、社内ウェブサイト、グループ、[Chromebook ハウツー動画](#)

変革を組織に伝える方法は？

導入に合わせたコミュニケーション キャンペーンを展開する

最大限の効果を引き出し、望ましい行動に誘導できるように、ロールアウトに合わせたコミュニケーションを計画します。

ユーザーに情報を提供して期待を高める

さまざまな方法でコミュニケーションを図り、ChromeOS の導入を従業員に周知して期待を高めます。

主要なメッセージを補強して導入を継続的に促進する

ユーザーに継続的に働きかけて、最新情報、[ヒントとコツ](#)、導入事例を紹介します。

導入を後押しする方法は？

エレベーター ピッチを作成する

- 会社が ChromeOS に移行する理由をエレベーター ピッチでわかりやすく説明する
- ChromeOS を使用するメリットを明確にして、組織のビジョンや戦略と関連付ける
- ChromeOS への移行における組織のビジョンをエレベーター ピッチに盛り込む
- 説得力があり、ユーザーに関係した内容にする必要がある

すべてにエレベーター ピッチを盛り込む

エレベーター ピッチのメッセージをあらゆるコミュニケーション資料に盛り込んでメッセージを強化します。

キャンペーンをブランディングする

ChromeOS プロジェクトに名前を付けて周知し、コミュニケーションを取りやすくします。

文化を変える

従業員を刺激して変革を後押しします。

- コンテストを実施して、先行導入を奨励する
- 組織内の導入コミュニティを支援する

トレーニング

複数のトレーニング形式を使用すると、プロジェクトは最も成功しやすくなります。

- 経験豊富なパートナーがトレーニングを提供する
- 既存の学習開発チームを活用してスケジュール設定と調整を支援する
- トレーニング クラスの 50% をリリース後の日付にスケジュールする
- 強制参加と任意参加のトレーニングを決める

組織のユーザーに必要なトレーニングは？

トレーニングのニーズを徹底的に検討することで、ユーザーが確実に ChromeOS を使いこなせるようになり、導入を促進して、移行期間に大きな混乱が生じるリスクを軽減します。

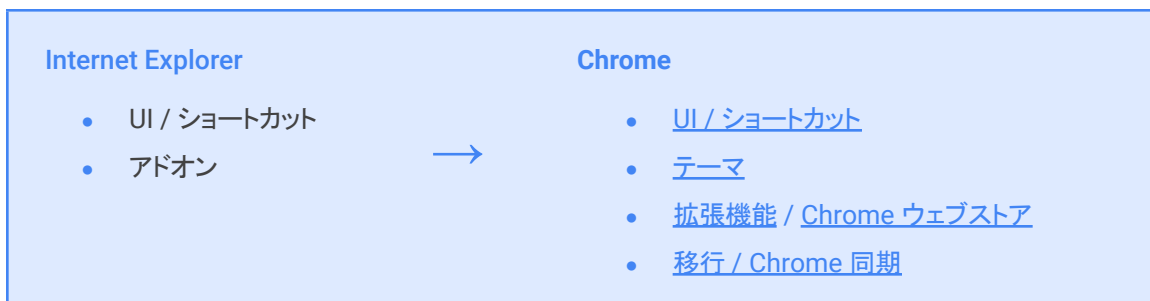
最新のヒントとコツについては、[生産性とコラボレーションに関するブログ](#)と [Chromebook の使い方](#)をご覧ください。

トレーニング ニーズを精査する

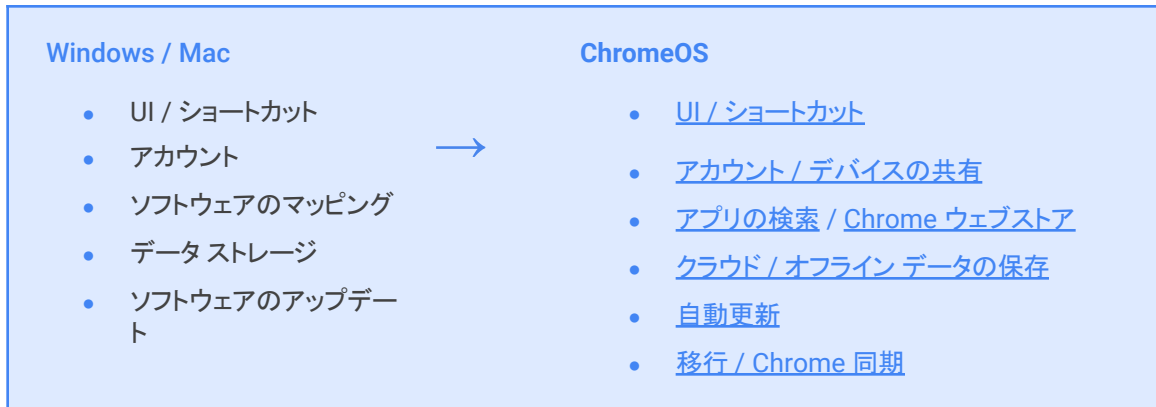
組織の分析を基に各コホートのトレーニング ニーズを文書化します。多くの場合、作業環境がどのように変わるかをユーザーに理解してもらうためには、コホートごとにユースケースに応じた専用のトレーニングが必要になります。トレーニングのニーズを徹底的に検討することで、[ユーザーが確実に ChromeOS を使いこなせるようになり、導入を促進して、移行期間に大きな混乱が生じるリスクを軽減](#)します。

例:

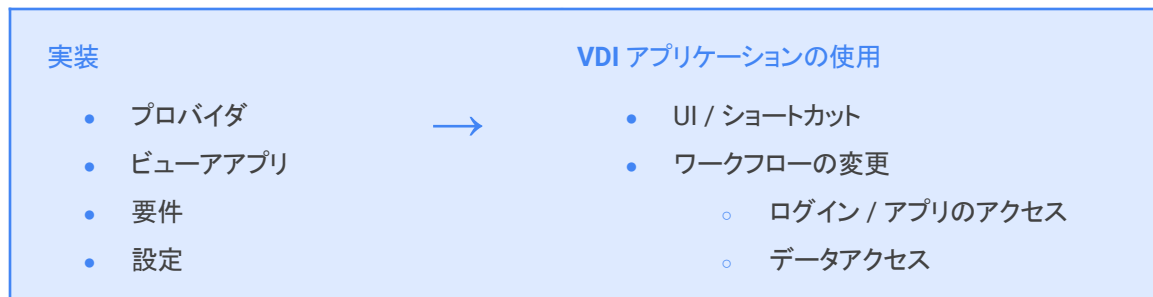
Internet Explorer からの移行 - すべてのユーザー



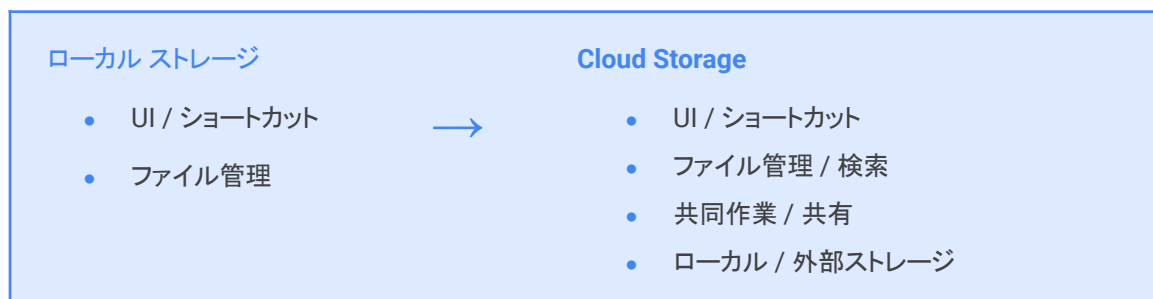
Chromebook の基本 - すべてのユーザー



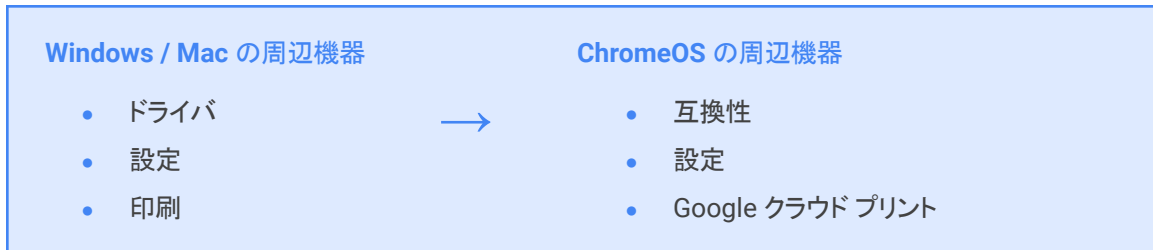
ChromeOS での VDI の使用 - 従来のアプリを必要とするユーザー



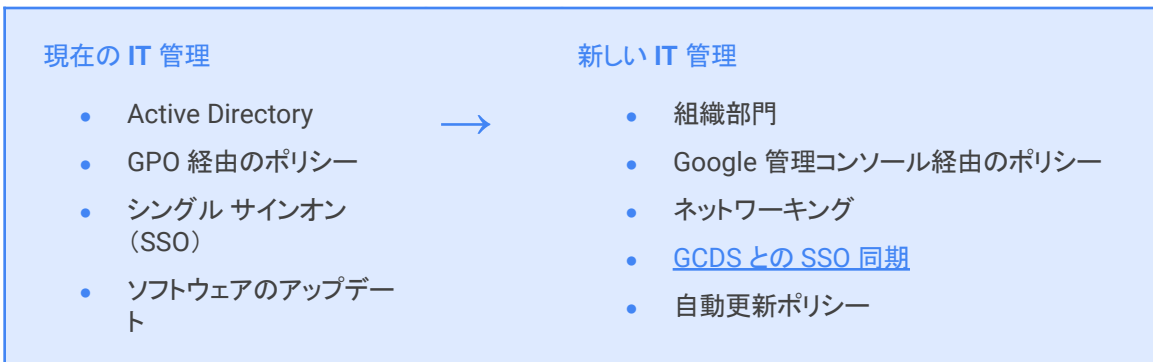
ファイル管理 - すべてのユーザー



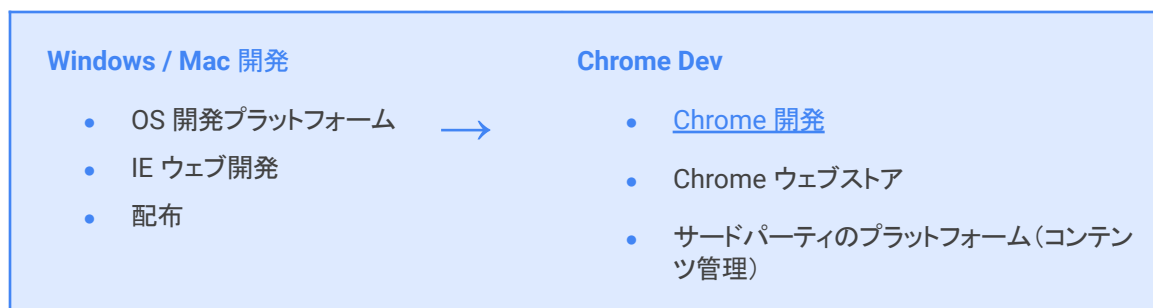
Chromebook と周辺機器 - 周辺機器の使用を必要とするユーザー



Google 管理コンソール - IT 管理者



アプリ開発 - コンテンツ作成者



ChromeOS のトレーニング方法は？

トレーニング カリキュラムを作成する

トレーニング ニーズの精査結果に基づいて、適切なトレーニング方法を特定し、ユーザーがトレーニング リソースに手軽にアクセスできるようにします。

従来のトレーニング方法

セルフペース型の e ラーニング	インストラクター主導のリモートトレーニング	クラスルームトレーニング
• 多人数に対応、画一的なコンテンツ • インストラクター主導トレーニングより低コスト • 最小限の設備要件 • 場所や時間を問わずアクセス可能	• 多人数に対応、カスタマイズ可能なコンテンツ • 通常は低～中程度のコスト • 中程度の設備要件 • 所定の時間に場所を問わずアクセス可能 • パートナーまたは顧客側に進行役のトレーニング リソースが必要	• 少人数に限定、カスタマイズ可能なコンテンツ • 高程度の設備要件 • パートナーまたは顧客側に進行役のトレーニング リソースが必要 • 通常は高い定着率と効果

最新のトレーニング形式

ランチ ミーティング

- 多人数に対応、画一的なコンテンツ
- 高い定着率と効果
- 従業員の士気向上
- 対面またはリモートで実施可能

改善されたデバイス配布プロセス

- 対面またはリモートで実施可能
- 新デバイスの受け取りを待つ間にポイントを絞った即席のトレーニング セッションを提供するなど、シンプルな配布プロセスを構築する
- デバイスを使い始める前に、全員が最低限のトレーニングを受けられるようにする
- 受け取り後にデバイスの設定や登録、動作に問題がないか確認する工程を設けることもできる

ドロップイン型のエキスパート バー

- 必要となきにエキスパートに質問できる窓口を設ける
- 移行の前後だけ一時的に設置することも、既存のサポート体系に組み込んで継続することもできる

成功のためのヒント

- ユーザーに ChromeOS デバイスを受け入れてもらうには、快適に使用できるようにすることが不可欠です。導入前に ChromeOS のライトナイト セッション、トレーニング セッション、セルフペース型トレーニング教材を提供し、ChromeOS

デバイスに慣れてもらうことで、移行時のユーザー エクスペリエンスを向上させます。

導入をサポートする

導入プロセスが楽しいものとなるよう、ChromeOS 支持者に見回り、同僚のサポート、プロジェクト チームとの情報交換、問題のエスカレーションを行ってもらいます。

- 事前に導入プロセスを 1～2 回テストし、必要に応じてチェックリストを見直す
- 対象のユーザー グループがログインできることを確認する
- 全体に導入する際は先行ユーザーに支持者になってもらい、期待感を醸成して、初期サポートモデルの人員を増やす

リリース サポートのチェックリスト

- オンボーディング エクスペリエンスを作り出す
- 1 日目のユーザー チェックリスト
- ChromeOS 支持者に働きかける
- フィードバックを求める
- 影響に対処する

オンボーディング エクスペリエンスを作り出す

- ユーザーが移行する際の楽しくポジティブな体験を計画することで支持者を生み出す
- 旧式のハードウェアを並行して運用するのか、交換するのかを検討する
- 移行を容易にするため、リリース前の一定期間、ユーザーが Chrome ブラウザをテストできるようにする(全ユーザーのクラウド移行に役立つが、別のステップが必要になる)
- 移行に必要とされる、次のような適切なアクセサリを提供する
 - モニター / 互換ドッキング ステーション / モバイル ディスプレイ / USB アダプター
 - 保護ケース、保護カバー
 - 移動するユーザー用のプライバシー フィルタ
 - 設定不要ですぐにデバイスを使用できるようにするマネージド プロビジョニング

ChromeOS 支持者に働きかける

移行中に ChromeOS 支持者が積極的で目立つ存在になるよう、以下のことを促します。

- フロアを歩いて手助けをする
- 統一した目印を付けてわかりやすくする

- エンタープライズ ソーシャル プラットフォームで健全な議論を促進する
- 問題を追跡し、プロジェクト チームにフィードバックする

複数のチャンネルでフィードバックを求める

- ChromeOS 支持者からのフィードバック
- ユーザー アンケート
- エンタープライズ ソーシャル プラットフォームをモニタリングし、構造化された方法でフィードバックに回答する
- 疑問や問題に対処するためのフォーラムを決定し、周知する
- フィードバックに耳を傾けて対応していることを示す

「ChromeOS への移行」のサポート

社内コミュニティによるセルフサポートを奨励する

ChromeOS Champions プログラム

従業員同士のサポートを支援する社内プログラムを奨励します。[Google ガイド](#)を活用して ChromeOS 支持者向けのプログラムを作成します。ChromeOS 支持者は、エンドユーザーをサポートしたり、チームを作ってエンドユーザーから質問を募ったりする有志の従業員です。こうしたプログラムを構築すると、実質的に初期サポートのヘルプデスクを社内に配置することになり、IT サポートチームの負担を軽減できます。

学校では、生徒が参加する同様のプログラムを作成できます。一部の OEM は、生徒の技術教育を支援する [Chromebook 修理プログラム](#)を提供しています。生徒が初期サポートとして Chromebook を修理します。

チケットの処理数や質問の回答数が最も多かった ChromeOS 支持者に対して、今月の従業員に選出する、ギフトカードを進呈する、専門性を認定する (Premium Chromebook を支給する) などの方法でインセンティブを提供することができます。

長期的な導入を促進する

- 変更プロセスの早い段階で導入の成功を宣言する
- 得られたメリットについてユーザーベースに伝え、そのメリットを可能な限り数値化する
- ChromeOS が「通常」の仕事の方法として定着し、オンボーディング研修の初期フェーズを逃した「新規参加者」など、プロセスの更新が含まれていることを確認する
- 旧デバイスに戻せるオプションを用意することで Chromebook との交換を奨励する、切り替えプログラムの作成を検討する

成功のためのヒント

- ユーザー コミュニティに対して積極的かつ継続的に ChromeOS の取り組みの周知を図り、情報に簡単にアクセスして利用できるようにする

さらにサポートが必要な場合

サポートを受ける

- [サポート ページ](#)を確認する
- Chrome Enterprise の[ヘルプセンター](#)と[コミュニティ](#)を参照する
- [Chrome Enterprise の「ハウツーデモ」](#)を確認する
- ChromeOS デバイスの[使い方のヒント](#) (エンドユーザー向け)
- [登録](#)して [Chrome Enterprise リリースノート](#) についてのお知らせメールを受け取る
- Chrome ブラウザのダウンロードと Chrome Enterprise サービスの概要 - [Chrome ブラウザ エンタープライズ](#)
- パートナー向け: [Chrome OnAir ウェブセミナー](#)
- [従業員の Chromebook 導入キット](#)を確認して共有する

セルフサポートのヒント

- Chrome ブラウザで `chrome://settings/help` にアクセスする
- [ChromeOS デバイスのログを収集するには](#)
- [Chromebook の問題を解決する \(エンドユーザー向け\)](#)
- [既知の問題](#) (Chrome Enterprise)
- [Log Analyzer](#) (Google Workspace ツールボックス) - エラーが発生した場合は `/var/log/messages` と `/var/log/chrome/` を分析

補足資料

- Chrome ブラウザ エンタープライズ サポート - [組織で Chrome サポートを利用する方法](#)を確認する
- [Chromebook ヘルプセンター](#)と[コミュニティ](#)
- お知らせ: [Google Chrome ブログ](#)、[Chrome リリースのブログ](#)、[Chromium ブログ](#)をフォローする
- [ChromeOS 更新トラッカー](#)、[Chrome プラットフォーム ステータス](#)、[Chromium データ](#) (リリース、スケジュール)
- デベロッパー: [ウェブ プラットフォームの変更点](#)を確認して [Chrome for Developers YouTube チャンネル](#)をフォローする