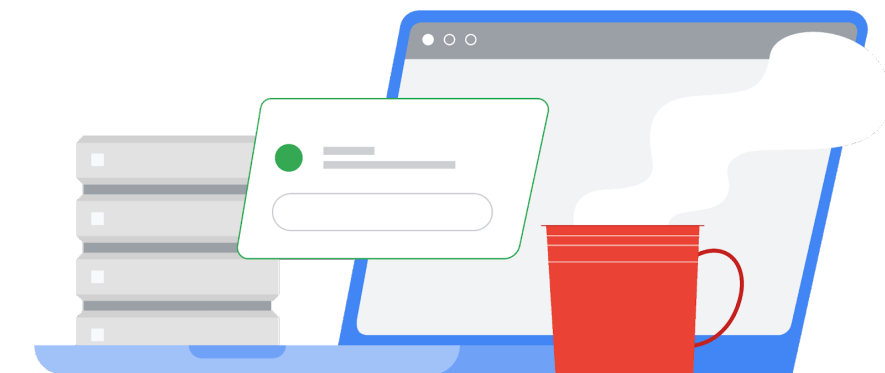


Google for Education

ChromeOS

フリート モニタリング のベスト プラクティス ガイド

2023 年 2 月

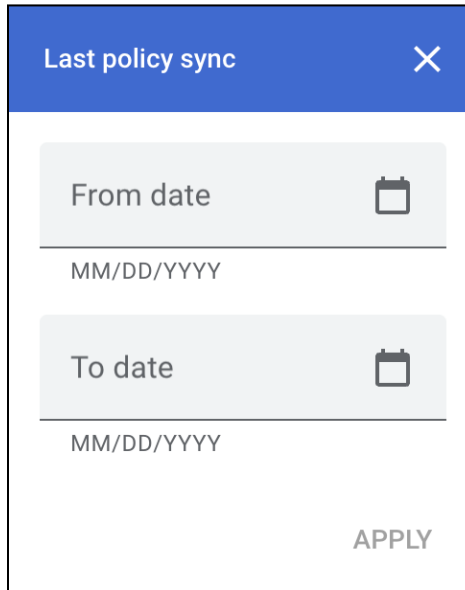


目次


ポリシーを最近同期していないデバイスの特定	2
ユーザーによってデバイスの再登録が繰り返された場合に検出する	4
Workspace for Education Plus または Standard をご利用の場合	4
デバイスの調査	4
再登録用のアクティビティ ルールの作成	5
Workspace for Education Fundamentals をご利用の場合	5
監査ログのフィルタ	5
ユーザーが未認可のデバイスを登録できないようにする	6
未登録のデバイスでログインしているユーザーのモニタリング	6
管理されていない状態で管理対象ネットワークに接続したデバイスの検出	7
推奨設定	8

ポリシーを最近同期していないデバイスの特定


管理コンソールで [デバイス] > [Chrome] > [デバイス] に移動し、最終同期日時の順で [すべてのデバイスのレポート](#) を表示します。フィルタをリストに追加して、特定の期間中に同期したデバイスを表示できます。たとえば、管理者は [ポリシーの最終同期] で [開始日] を 2022 年 1 月 1 日、[終了日] を 2023 年 1 月 13 日に設定して、2023 年 1 月 13 日以降、つまり今年に入ってからポリシーを同期していないデバイスのみを表示できます。



Last policy sync

From date 



MM/DD/YYYY

To date 

MM/DD/YYYY

APPLY

このデバイスリストの列を編集して、[最新のユーザー] (デバイスを最後に使用したユーザー) を追加できます。[ユーザー] 欄に表示されるのはデバイスを登録したユーザーであって、デバイスのメインユーザーではない可能性があります。表示される列を編集するには、歯車アイコンをクリックし、下部にある [新しい列を追加] をクリックして [最新のユーザー] を選択します。[X] をクリックして列を削除することもできます。完了したら、[保存] をクリックします。

Manage columns	
Device list	
Serial number	
Status	×
Asset ID	×
Organizational unit (not currently visible)	×
Online status (not currently visible)	×
Enrollment time	×
Last policy sync	×
Location	×
Most recent user	×
 Last user activity	×
<i>Add new column</i>	▼
CANCEL SAVE	

管理者は、同期が過去 30 日間行われず、[使われていない会社所有デバイスに関するレポートを自動で受け取る](#)ことも可能です。

ユーザーによってデバイスの再登録が繰り返された場合に検出する

ユーザーがデバイスの登録解除と再登録を繰り返した場合に、監査ログでこの情報をキャプチャして管理者に表示できます。Google Workspace for Education Plus または Google Workspace for Education Standard では、こうしたデバイスの再登録によって自動アラートや自動アクションをトリガーできます。

Workspace for Education Plus または Standard をご利用の場合

デバイスの調査

調査ツールの使用方法について詳しくは、[セキュリティ調査ツール](#)をご覧ください。

- [レポート] → [調査] → [管理ログイベント] に移動
- [条件作成ツール] をクリック
- [イベント]、[次に一致]、[デバイスのステータスの変更] という条件を追加
- [新しい値]、[次の文字を含む]、「ACTIVE」という条件を追加
- [結果をグループ化] をクリックして [リソース ID] を選択

The screenshot shows the 'Condition builder' interface in the Google Workspace Security Investigation tool. At the top, there is a search bar with 'Search 1' and options to 'Create activity rule', 'Create custom chart', and 'Discard search'. Below this, the 'Admin log events' dropdown is selected, and the 'Filter' section is active. The 'Condition builder' section shows two conditions: 'Event' is 'Is' 'Change Device State' and 'New value' 'Contains' 'ACTIVE'. The 'Group results by' section is set to 'Resource ID(s)'. A 'SEARCH' button is at the bottom.

- [検索] をクリック

特定のデバイスの再登録が頻繁に行われている場合は、ユーザーが意図的にデバイスの登録を解除して再登録している可能性があります。

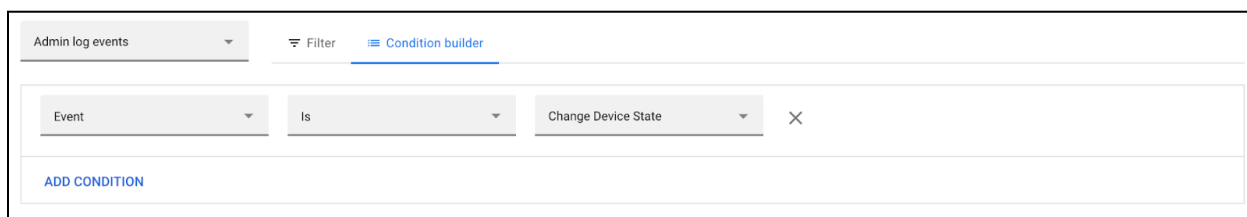
再登録用のアクティビティ ルールの作成

省略可: 上部にある [アクティビティ ルールを作成] をクリックし、この検索をルールとして保存して自動通知を送信します。デバイスを再登録するユーザーを自動的に停止すると誤検出が発生する可能性があるため、現在は推奨されていません。アクティビティ ルールの作成について詳しくは、[アクティビティ ルールの作成と管理](#)をご覧ください。

Workspace for Education Fundamentals をご利用の場合

監査ログのフィルタ

- [レポート] → [調査] → [\[管理ログイベント\]](#) に移動
- [条件作成ツール] をクリック
- [イベント]、[次に一致]、[デバイスのステータスの変更] という条件を追加



- [検索] をクリック

[リソース ID] と [説明] の列がデフォルトで表示されます。

[すべてエクスポート] をクリックして、結果を Google スプレッドシートに書き出します。エクスポートの名前を入力して [エクスポート] をクリックします。

書き出しが完了したら、[「エクスポート」操作の結果] までスクロールし、エクスポート名をクリックして Google スプレッドシートを開きます。

列を追加して説明でテキスト「ACTIVE to ACTIVE」をテストし、デバイスの再登録を特定します。以下の数式の例では、C が [説明] 欄です。この数式をシートのセル E1 として設定します。

```
=Arrayformula(if(row(C:C)=1, "Reenrolled", REGEXMATCH(C:C, "ACTIVE to ACTIVE")))
```

列ヘッダー「リソース ID」を行、列ヘッダー「再登録」を列、他の項目 (列ヘッダー「アクター」など) のカウントを値として使用して、[ピボットテーブルを挿入](#)します。

ユーザーが未認可のデバイスを登録できないようにする

組織によっては、エンドユーザーがデバイスを登録または再登録できます。この権限があると、ユーザーは学校や職場でデバイスを再登録し、ネットワークに接続していないときは登録解除することが可能です。管理者は、ユーザー自身が簡単にデバイスを再登録できないようにしたい場合は、この権限をユーザーに対して無効にすることを検討してください。ユーザーが再登録できるようにする場合は有効にします。

管理コンソールでこの設定を切り替えるには、[デバイス] > [Chrome] > [設定] > [\[ユーザーとブラウザ\]](#) に移動します。左側の列で関連する組織部門(「生徒」など)を選択します。[登録の管理] の [登録の権限] で、[この組織内のユーザーに、新しいデバイスの登録や既存のデバイスの再登録を許可しない] を選択してユーザーがデバイスを登録できないようにするか、[この組織内のユーザーに、既存のデバイスの再登録のみを許可する(新しいデバイスやプロビジョニング解除済みデバイスは登録できない)] を選択してユーザーが既存のデバイスを再登録できるようにします。

未登録のデバイスでログインしているユーザーのモニタリング

教師や職員が管理対象外デバイスを見つけやすいように、デバイス ポリシーの表示設定を変更できます。この変更は、現在管理対象となっているデバイスにのみ適用されます。管理対象外デバイスに変更は表示されません。

管理者は、ログイン画面に[常にシステム情報を表示する](#)ようにデバイスを設定できます。管理対象外デバイスには、[管理元] またはシステム情報は表示されません。さらに、[ログイン画面の壁紙](#)を保護されている画像に変更することもできます。

管理者は[管理コンソールのデバイスリスト](#)で、最近ログインしたユーザーに関連するポリシー同期を監視できます。想定されるユーザーのリストとポリシーを最近同期したユーザーを相互参照することで、同期が行われていないデバイスを使用している可能性があるユーザーのリストを作成できます。残っているこれらのデバイスをさらに監視して、登録状態を物理的に調査することも可能です。

管理されていない状態で管理対象ネットワークに接続したデバイスの検出

管理されていない Chromebook が Wi-Fi ネットワークに接続するときに、管理する必要があることを迅速に判断できる場合があります。管理者は [DeviceHostnameTemplate](#) ポリシーを使用して、シリアル番号とアセットタグ ID(またはいずれか)を含むホスト名の形式を指定でき

ます。このホスト名は、ネットワークの DHCP テーブルに表示されます。既知の MAC アドレスを持つデバイスが適切なホスト名なしで管理対象ネットワークに接続している場合は、未登録のデバイスである可能性が高いと考えられます。

例: 管理コンソールで、[デバイス] > [Chrome] > [設定] > [デバイス] に移動し、[その他の設定] の [デバイスのネットワーク ホスト名テンプレート] までスクロールします。ネットワーク ホスト名テンプレート ポリシーとして「ManagedChromebook- $\{SERIAL_NUM\}$ 」を管理対象 Chromebook に適用します。これらの Chromebook は、簡単に特定できるように設定されたホスト名で学校のネットワークの DHCP プールに表示されます。その SSID / ネットワーク上にある他のすべてのリースは、一般的または未定義のホスト名で表示されます。そうした一般的または未定義のホスト名の MAC アドレスを書き出して、Workspace テナントの既知の MAC アドレスと比較すると、登録されていないデバイスの特定に役立ちます。

Wi-Fi MAC アドレスを持つデバイスのリストを書き出すには、管理コンソールで [デバイス] > [Chrome] > [デバイス] に移動し、目的の組織部門を選択してからリストの上にある [エクスポート] をクリックします。右上の砂時計アイコンをクリックすると、書き出し処理がタスクリストに表示されます。完了したら、CSV をダウンロードして結果を確認できます。「macAddress」列には Wi-Fi MAC アドレス(コロン文字なし)が含まれています。

その後、管理者は特定したデバイスに対していくつかの操作を行うことができます。たとえば、当該デバイスやユーザーを追跡する、それらの MAC アドレスによるネットワークへの接続を完全にブロックする、デバイスを制限付きアクセス VLAN に分けるといった操作が可能です。ネットワーク管理者はコンテンツ フィルタまたはキャプティブ ポータル システムを使用すれば、IT サポートへの問い合わせ方法やデバイスの再登録方法(管理者が許可している場合)が記載されたページに、特定したこれらのデバイスをリダイレクトできます。

推奨設定

- [自動的に再登録](#) - [ワイプ後にデバイスを自動再登録] に設定する。[「自動的に再登録」に関するサポート記事](#)
- [Powerwash](#) - [Powerwash のトリガーを許可しない](選択したユーザーを除く全員が対象)に設定する。[Powerwash に関するサポート記事](#)
- [確認済みモード](#) - [認証アクセスで確認付きブートを求める] に設定する。[確認済みモードに関するサポート記事](#)
- [確認済みアクセス](#) - [コンテンツ保護で有効にする] に設定する。[確認済みアクセスに関するサポート記事](#)
- [デバイスの再登録の権限](#) - ユーザーに再登録を許可する特定の組織部門を選択する。[登録の権限に関するサポート記事](#)
- 次の内部 URL への[アクセスをブロックする](#)。

chrome://policy
chrome://net-export
chrome://prefs-internals
chrome://version
chrome://kill
chrome://hang