

Chrome Enterprise Premium のトライアル ガイド

2025 年 12 月



目次

Chrome Enterprise Premium の概要	03
Chrome Enterprise Premium の成功基準を定義する	04
Chrome Enterprise Premium の成功基準の例	05
Chrome Enterprise Premium のアクセスを設定する	06
テスト環境を準備する	07
Cloud Identity と Chrome Enterprise Core を有効にする	08
Chrome Enterprise 管理ロールを作成する	09
組織部門構造を作成する	10
テストブラウザの登録とテストユーザーの作成を行う	11
Chrome Enterprise Premium コネクタの設定を有効にする	12
必要なブラウザ拡張機能をデプロイする	13
(省略可) デバイス トラスト コネクタを設定する	14
Chrome Enterprise Premium の試用を開始する	15
Chrome Enterprise Premium のユースケース - 管理対象ブラウザ	17
Chrome Enterprise Premium のユースケース - 脅威対策とデータ保護	18
Chrome Enterprise Premium のユースケース - アクセス制御	19
Chrome Enterprise Premium のユースケース - 調査とサードパーティ統合	20
トラブルシューティング	21
よくある質問	25
参考情報	26

セキュアな企業向けブラウザ Chrome を使用する

Chrome Enterprise Premium の概要

セキュアな企業向けブラウジングは、ユーザーが場所やデバイスを問わずウェブベースで安全に業務を行えるようにしつつ、企業データを保護するための新しい標準となっています。[Chrome Enterprise Premium](#) には以下の機能が用意されています。

- 設定可能なデータ損失防止 (DLP)
- リアルタイムのフィッシングやマルウェア対策、サンドボックス化による保護
- 最小権限アクセスによる業務に不可欠なアプリケーションへのアクセス管理

このガイドでは、セキュアな企業向けブラウザを設定して、ユーザープロファイルおよびデバイスベースで管理できるようにする手順について説明します。また、試用の設定手順（必要な場合）や、Chrome セキュリティインサイトを有効にして、企業での危険なブラウザ アクティビティに対するセキュリティ審査を無料で行う手順についても説明します。

要件（このガイドで説明）:

- [Chrome ブラウザ](#) がユーザーのデバイスにインストールされている
- [Google 管理コンソール](#) へのアクセス
- [Google Cloud コンソール](#) へのアクセス
- [クラウド管理](#) に登録されているデバイス、および管理対象とするユーザーの Google Cloud Identity ライセンス
- Chrome Enterprise Premium のライセンスまたは 60 日間の試用版



価値実証の範囲を定義する

Chrome Enterprise Premium の成功基準を定義する

Chrome Enterprise Premium には、企業の一般的なユースケースに対応するさまざまな機能があります。Chrome Enterprise Premium を試用する際は、成功基準の範囲を明確にすることが重要です。ガイドの各セクションで、次の場所にある企業データの保護について説明しています。

- SaaS アプリケーション内の企業データ
- Google Cloud Platform の社内向けウェブアプリケーション内のアセット
- 他のクラウドまたはオンプレミスの社内向けウェブ アプリケーションに保存されたデータ

また、次のデータへのアクセスが必要なデバイスとユーザーの種類を定義する必要があります。

- 会社所有デバイスを使用する完全管理対象の企業ユーザー
- 管理対象外デバイスを使用する企業ユーザー、請負業者、パートナー

これらの側面に対応したガイドの各セクションをご確認いただき、Chrome Enterprise Premium の 60 日間試用のメリットを最大限に活用してください。次のセクションでは成功基準の例をご紹介します。



価値実証のユースケースを選択する

Chrome Enterprise Premium の成功基準の例

管理カテゴリ	テスト ユースケース	求められる成果
管理対象ブラウザ / プロファイル	A. 管理対象デバイス(ブラウザ経由) B. 管理対象外デバイス(プロファイル経由) C. レポートと監査 D. パスワードの再利用 E. 拡張機能の制御	A. 管理対象デバイスがアプリアクセスのセキュリティ基準を満たす B. 管理対象外デバイスで管理対象ブラウザのエクスペリエンスを提供する C. 1つのウィンドウで全デバイスのアクティビティレポートを確認する D. 古いパスワードや脆弱なパスワードの再利用を制御する E. 承認されていない拡張機能をユーザーがインストールできないようにする
データ保護	A. アップロードの制限 B. ダウンロードの制限 C. コピー / 貼り付けの制御 D. 印刷の制御 E. ウェブ / URL フィルタリング F. 光学式文字認識(OCR) G. 透かし H. スクリーンショット / 画面共有からの保護 I. データ マスキング	A. 機密データのサイトへのアップロードを防ぐ B. 機密データのデバイスへのダウンロードを防ぐ C. Chrome プロファイル、シークレットモード、他のアプリ間の機密データの転送を防ぐ D. 機密データの印刷を防ぐ E. アクセスできる URL ドメインとカテゴリを制御する F. 画像と PDF の機密データを分析する G. 機密性の高いサイトに透かしをオーバーレイして、データの引き出しを抑制する H. スクリーンショット / 画面共有によるデータのキャプチャを防ぐ I. サイトでデータが見られないように隠す、または削除する
脅威対策	A. フィッシング対策 B. 高度なマルウェア スキャン	A. ユーザーの不審なウェブサイトへのアクセスを防ぐ B. ユーザーによる不審なコンテンツのダウンロードを防ぐ
アクセス制御	A. Workspace アプリの保護 B. GCP アプリの保護 C. オンプレミス アプリの保護 D. サードパーティの SAML / OIDC アプリケーションの保護	A. コンテキストアウェア アクセス ポリシーを適用して、Workspace アプリケーションと管理コンソールへのアクセスを制御する B. GCP でホストされているアプリケーションへのアクセスを制御、監視する C. オンプレミスでホストされているアプリケーションへのアクセスを制御、監視する D. サードパーティの SaaS アプリケーションへのアクセスを制御、監視する
調査	A. Chrome のイベントログ B. エビデンス ロッカー	A. 管理コンソールで Chrome のイベントを調査する B. セキュリティチームが分析できるように、ポリシー違反のファイルの暗号化バージョンを保管する
サードパーティ統合	A. サードパーティの IdP との統合 B. コネクタ	A. デバイストラストコネクタを使用して、サポートされているサードパーティの IdP 内で Chrome Enterprise Premium テレメトリーを利用する B. Chrome のイベントログをセキュリティツール(SIEM / SOAR / XDR)に送信する

アクセスを取得する

Chrome Enterprise Premium のアクセスを設定する

前提条件: Chrome Enterprise Premium の試用を管理するコンソールへのアクセスを取得する

ユースケースを定義した後、このセクションでは、試用を有効にする前に Google 管理コンソールと Google Cloud コンソールへの必要なアクセスを取得する方法について説明します。これらの手順に沿って準備しておくことで、試用開始後すぐに使用できます。

シナリオ 1: 組織ですでに Google サービスを使用している場合

会社で Google Workspace または Google Cloud を使用している場合は、次の手順を行います。

- 1 既存のアクセスを確認する : 組織で次のサービスを使用している場合、必要なコンソールはすでに設定されています。
 - Google Workspace (Gmail、Google ドライブ、Google ドキュメント)、もしくは ChromeOS デバイス、Google Identity、Chrome Enterprise Core などのマネージド サービス。
 - Google Cloud (本番環境のサービスやプロジェクトで使用)。
- 2 管理者に問い合わせる : 多くの場合、Google Workspace の特権管理者または Google Cloud 管理者の協力が必要になります。このガイドを管理者と共有し、試用を有効にして、権限を委任したカスタムの管理者ロールを作成する方法をお伝えください。
- 3 管理者との権限分割に関する注意事項 : 権限の分割について管理者に不安を与えないように配慮してください。Google 管理コンソールで作成するカスタムロールは、Chrome ブラウザのポリシー管理専用です。このロールに付与される権限では、Google Cloud コンソールにアクセスすることはできず、Google Cloud で運用されている組織のリソースは完全に独立した状態のままとなります。
 - 高度なユースケースに関する注意事項 : Google Cloud 内のサービスを保護する目的で(たとえば [Google のセキュア ゲートウェイ](#)などを介して) Chrome Enterprise Premium を設定する必要がある場合は、追加の権限が必要になりますが、これについてはこのガイドでは取り上げません。

シナリオ 2: 組織で Google サービスを初めて使用する場合

組織で Google Workspace サービスと Google Cloud サービスのいずれも使用していない場合は、新しいアカウントを作成する必要があります。

- 1 プロセスを理解する : Google 管理コンソールの作成は簡単で、同時に Chrome Enterprise Premium の試用を有効にするための Google Cloud コンソールも自動的に設定されます。両方とも同じログインを使用します。
 - これらのコンソールを作成するには、Google のエンドユーザー使用許諾契約に同意する必要があります。
- 2 アカウントを作成する :
 - [Google Chrome Enterprise の登録](#) ページにアクセスします。
 - 会社のメールアドレスを入力し、画面上の手順に沿って操作します。

テスト環境を準備する

試用準備を行う

Chrome Enterprise Premium の試用準備を行う

60 日間の評価期間を最大限に活用できるように、試用を有効にする前に以下の段階を追ったチェックリストを使用して試用環境を準備してください。これにより、基本的な設定に貴重な時間を費すことなく、初日から高度な機能をテストできます。

試用前の設定チェックリスト：

- ☐ **Cloud Identity と Chrome Enterprise Core を有効にする**
 - 重要な理由：追加料金なしで登録して、プレミアム機能の動作に必要なユーザーとブラウザの管理フレームワークの基盤を構築できます。
- ☐ **Chrome Enterprise 管理ロールを作成する**
 - 重要な理由：評価チームが最初から適切な権限のもとで、ロールに関連する機能に遅滞なくただちにアクセスしてテストできます。
- ☐ **組織部門構造を作成する**
 - 重要な理由：実際のポリシーの適用をシミュレートし、デバイスベースの制御とユーザーベースの制御の違いをテストするうえで不可欠な設定です。
- ☐ **テストブラウザの登録とテストユーザーの作成を行う**
 - 重要な理由：ポリシーを適用するには、ブラウザが管理対象となっている必要があります。テストデバイスを登録し、テストユーザー アカウントを作成することで、管理対象デバイスと管理対象外デバイスの両方で強力なセキュリティ機能と管理機能を試して評価する準備ができます。
- ☐ **Chrome Enterprise Premium コネクタの設定を有効にする**
 - 重要な理由：特定のテストグループに対してソリューションの高度なセキュリティ機能を有効にできます。Chrome Enterprise Premium を機能させるには、この設定が必要です。
- ☐ **必要なブラウザ拡張機能をデプロイする**
 - 重要な理由：デバイスの状態とセキュリティ ポスチャーに関する重要なデータを収集する拡張機能です。事前にデプロイしておくことで、試用開始直後から、強力なコンテキストアウェアおよびゼロトラストのアクセス ポリシーをテストできます。
- ☐ **(省略可) デバイス トラスト コネクタを設定する**
 - 重要な理由：Okta、Ping、Cisco Duo などのプロバイダを使用している場合は、この手順により Chrome のセキュリティ シグナルを既存の ID およびアクセス ポリシーに直接統合して、強化されたシームレスなセキュリティ ポスチャーをテストできます。
- ☐ **Chrome Enterprise Premium の試用を開始する**
 - すべての設定が整った 環境で、自信を持って 60 日間の試用を開始し、あらゆる高度な機能をすぐに試すことができます。

Cloud Identity と Chrome Enterprise Core を有効にする

無料のサブスクリプションを有効にする方法

基本のサブスクリプションを有効にする(特権管理者が必要)

ユーザーとブラウザの管理の基本となるこのプロセスは、特権管理者が行う必要があります。Google 管理コンソールの [お支払い] セクションから 2 つのサービスを追加します。このプロセスは無料で、お支払い情報は必要ありません。

1 ログインする

- admin.google.com にアクセスして、特権管理者アカウントでログインします。

2 サブスクリプション カタログに移動する

- メインメニューから [お支払い] > [サブスクリプション] に移動します。
- [購入またはアップグレード] ボタンをクリックします。

3 Cloud Identity Free を追加する

1. カタログの [カテゴリ] セクションで [Cloud Identity] を選択します。
2. [Cloud Identity Free] の下にある [開始] をクリックし、プロンプトに沿って「購入手続き」を行います。
3. プランを確定します。合計額は 0.00 ドルになります。
 - 目的: 有料の Google Workspace ライセンスを持っていないテストユーザーに Google Identity アカウントを発行して管理できるようになります。これは、ユーザーベースのポリシーを適用するために不可欠です。

4 Chrome Enterprise Core を追加する

1. [購入またはアップグレード] ページに戻ります。
2. [Chrome Enterprise Core] を検索して選択します。
3. [開始] をクリックして、同じように無料の「購入手続き」を行います。
 - 目的: ブラウザの登録、デバイスレベルでのポリシーの適用、ブラウザ フリートの可視化など、一元的なクラウド管理が可能になります。

5 サブスクリプションを確認する

- [お支払い] > [サブスクリプション] に戻ります。
- [Cloud Identity Free] と [Chrome Enterprise Core] の両方がアクティブなサブスクリプションとして表示されていることを確認します。

これで、基本のサブスクリプションが有効になり、次のステップに進む準備が整いました。

Chrome Enterprise 管理ロールを作成する

Google 管理コンソールで管理者ロールを設定する

次に、特権管理者は Chrome Enterprise Premium の試用に必要なカスタムロールを Google 管理コンソールで作成する必要があります。Google 管理コンソールの権限は、Google Cloud コンソールとは完全に無関係であることに注意してください。このロールでは、クラウドリソースへのアクセスは付与されません。

権限が不明な場合は、[権限を選択] ページで、[管理コンソールの権限] と [管理 API の権限] の両方のセクションを確認します。重複する権限は統合されるため、「組織部門 > 読み取り」などの権限が API のセクションに表示される場合がありますが、機能は同じです。カスタムロールを作成する手順は次のとおりです。

- 1 [アカウント] > [管理者ロール] に移動します。
- 2 [新しいロールを作成] ボタンをクリックし、「Chrome Enterprise Premium 管理者」などの名前を付けたら、[続行] ボタンをクリックします。
- 3 次の管理コンソール権限を選択します。

Google 管理コンソールの権限

組織部門 [読み取り] のチェックボックスをオンにする ([作成]、[更新]、[削除] は任意ですが、テスト用にオンにしておく役立ちます)

ユーザー [読み取り] のチェックボックスをオンにする ([作成]、[更新]、[削除] は任意ですが、テスト用にオンにしておく役立ちます)

グループ [読み取り] のチェックボックスをオンにする ([作成]、[更新]、[削除] は任意ですが、テスト用にオンにしておく役立ちます)

セキュリティ センター [アクティビティ ルール] と [このユーザーにセキュリティ センターの完全な管理者権限を付与します] のチェックボックスをオンにする

データ セキュリティ [ルールの管理] と [アクセスレベルの管理] のチェックボックスをオンにする

Chrome 管理 [設定] のチェックボックスをオンにする

Chrome DLP [Chrome DLP アプリケーション インサイトの設定の管理]、[Chrome DLP アプリケーションの OCR 設定の表示と管理]、[Chrome DLP アプリケーション インサイトの設定の表示] のチェックボックスをオンにする

モバイル デバイス管理 [デバイスと設定の管理] のチェックボックスをオンにする

Chrome Enterprise セキュリティ サービス [Chrome Enterprise セキュリティ サービスの設定] のチェックボックスをオンにする

DLP [DLP ルールの管理] と [DLP ルールの表示] のチェックボックスをオンにする

アラート センター [フルアクセス] のチェックボックスをオンにする

レポート チェックボックスをオンにする

Google 管理 API の権限

グループ [読み取り] のチェックボックスをオンにする

組織部門 [読み取り] のチェックボックスをオンにする

- 4 選択したら、[続行] ボタンをクリックします。
- 5 [ロールを作成] ボタンをクリックします。
- 6 前のステップで作成したカスタムロールを選択し、[ロールを割り当て] ボタンをクリックして、選択した管理者に割り当てます。

組織部門構造を作成する

ユースケースに合わせてデバイスとユーザー アカウントを分ける

さまざまなセキュリティ シナリオを効果的にテストできるように、2 つの子組織部門 (OU) を含む親組織部門を作成します。この構造は、会社所有デバイスと個人所有デバイスの両方でポリシーの適用をシミュレートするために不可欠で、これにより試用全体を簡単に管理できます。管理コンソールではグループもサポートされているため、組織部門の代わりにグループを使用することもできます。[グループへのポリシーの適用について詳しくは、こちらのリンク](#)をご覧ください。

次の設定を使用して、3 つのレベルでポリシーの適用をテストできます。

- 親組織部門：共通のベースライン ポリシーを両方の子組織部門に同時に適用できるため、管理が簡素化されます。
- 管理対象デバイスの組織部門：信頼できる企業所有のブラウザでデバイスレベルのポリシーをテストする場合。
- 管理対象ユーザーの組織部門：デバイスを問わずアカウントを監視するユーザーレベルのポリシーをテストして、個人所有デバイス (BYOD) のシナリオをシミュレートする場合。

組織部門を作成する手順：

- 1 【組織部門】に移動する
 - Google 管理コンソール (admin.google.com) にログインします。
 - メニューから、【ディレクトリ】>【組織部門】に移動します。
- 2 親組織部門を作成する
 - 最上位の組織部門を選択し、プラス ボタンをクリックして新しい組織部門を作成します。
 - 名前: CEP 試用
 - (省略可) 説明: Chrome Enterprise Premium の試用で使用する親組織部門。
 - [作成] をクリックします。
- 3 子組織部門を作成する
 - 作成した [CEP 試用] 組織部門にカーソルを合わせて、表示された + 記号をクリックします。
 - デバイスの組織部門を作成する：
 - 名前: CEP 試用 - 管理対象デバイス
 - (省略可) 説明: CEP の試用で使用する会社支給のデバイス用。
 - 親が「CEP 試用」であることを確認します。
 - [作成] をクリックします。
 - ユーザーの組織部門を作成する：
 - [CEP 試用] 組織部門にもう一度カーソルを合わせて、+ 記号をクリックします。
 - 名前: CEP 試用 - 管理対象ユーザー
 - (省略可) 説明: Cloud Identity で作成したテストユーザー アカウント用。
 - 親が「CEP 試用」であることを確認します。
 - [作成] をクリックします。

これで、ポリシーを適用するための専用の構造を作成できました。今後、登録するすべてのブラウザを「CEP 試用 - 管理対象デバイス」組織部門に配置し、すべてのテストユーザー アカウントを「CEP 試用 - 管理対象ユーザー」組織部門に配置します。

テストブラウザの登録とテストユーザーの作成を行う

ユースケースに合わせてデバイスとユーザー アカウントを登録する

組織部門を設定したら、次に Chrome Enterprise Premium の評価に使用するテストユーザーとデバイスを組織部門に追加します。

テストユーザー アカウントを作成する

- 1 ユーザーの管理画面に移動する : 管理コンソールで、[ディレクトリ] > [ユーザー] に移動します。
- 2 新しいユーザーを追加する : [新しいユーザーの追加] をクリックします。識別しやすいように、姓: cep、名: テスト のように名前を付けます。
- 3 正しい組織部門に割り当てる : [ユーザーのパスワード、組織部門、プロフィール写真を管理する] でプルダウンをクリックして [CEP 試用 - 管理対象ユーザー] 組織部門を選択します。この手順は極めて重要です。
- 4 確定する: [新しいユーザーの追加] をクリックして、次のページでパスワードをコピーします。

テストブラウザを登録する (Windows)

- 1 デバイスの組織部門に移動して選択する :
 - 管理コンソールで、[Chrome ブラウザ] > [管理対象ブラウザ] に移動します。
 - [管理対象ブラウザ] ペインで、[CEP 試用 - 管理対象デバイス] 組織部門を選択します。これにより、ブラウザが正しく割り当てられます。
- 2 登録ファイルを生成する :
 - 正しい組織部門を選択したら、登録ボタン をクリックします。
 - [ダウンロード] セクションで [.reg ファイル] をクリックします。ファイルを保存します。
- 3 テストデバイスに適用する :
 - ダウンロードした .reg ファイルをテスト用パソコンに転送します。
 - .reg ファイルを右クリックして、[管理者として実行] を選択します。
 - セキュリティ プロンプトに同意して、レジストリを変更します。
- 4 登録を確認する :
 - テストデバイスで Chrome ブラウザをいったん閉じて再び開きます。登録が自動的に行われます。
 - 登録は、管理コンソールの [管理対象ブラウザ] (正しい組織部門内) で、またはテストデバイスでブラウザのアドレスバーに「chrome://policy」と入力して確認できます。
 - または、[クラウド管理型の Chrome ブラウザを登録する](#) の手順に沿って、他の OS (Mac OS など) を登録し、デバイスレベルでブラウザを管理することもできます。

Chrome Enterprise Premium コネクタの設定を有効にする

Chrome Enterprise Connectors とセーフ ブラウジング

セキュリティ機能を有効にするには、親の「CEP 試用」組織部門でコネクタとレポートの設定を有効にします。これらの設定は、ネストされた組織部門に継承されます。教育機関のお客様の場合は、ポリシーを機能させるために必要となる [Chrome Enterprise セキュリティサービス](#) ([アプリ] > [その他の Google サービス] にあります) も有効にする必要があります。

Chrome ブラウザの設定を行う

1. 管理コンソールで、[\[Chrome ブラウザ\]](#) > [\[設定\]](#) に移動します。
2. 左側で、テスト用の親組織部門の[\[CEP 試用\]](#)を選択します。

ブラウザのレポート

- 管理対象ブラウザのクラウド レポート: [\[管理対象ブラウザのクラウドレポートを有効にする\]](#) に設定する。
- イベントレポート: [\[イベントレポートを有効にする\]](#) に設定する。
- 管理対象プロファイルのレポート: [\[管理対象ユーザーの管理対象プロファイルレポートを有効にする\]](#) に設定する。
- 管理対象ブラウザのレポートのアップロード頻度: [\[3 時間\]](#) に設定する。
- デバイストークンの管理: [\[トークンを削除する\]](#) に設定する(推奨)。

コンテンツ コネクタと URL チェック ポリシー

1. 設定の検索バーで、カテゴリに以下を含む:「コネクタ」でフィルタします。
2. 次のポリシーのメインのプルダウンを[\[Chrome Enterprise Premium\]](#)に設定します。
 - アップロードコンテンツの分析
 - ダウンロードコンテンツの分析
 - 一括テキストコンテンツの分析(コピー/貼り付け)
 - 印刷コンテンツの分析
 - リアルタイムでの URL のチェック
 - ファイル転送コンテンツの分析 (ChromeOS 向け)
3. 各設定の [\[追加の設定\]](#) で、以下のとおり設定します。
 - 分析が完了するまで遅らせる: ボタンをオンにする。
 - 失敗時にブロック: (推奨)有効にする。
 - 機密データとマルウェアをチェック: オンに設定する。
 - パスワードで保護されたファイルと **50 MB** を超えるファイルをブロック: 必要に応じて設定する。
 - ユーザーが示した警告無視の理由: 必要に応じて設定する。マルウェア対策のため、無効にしておくことをおすすめします。
 - 最小文字数(一括テキストの場合): **1**に設定する。

セーフ ブラウジングの設定

1. 設定の検索バーで、カテゴリ:「セーフ ブラウジング」でフィルタします。
2. 次のポリシーを設定します。
 - セーフ ブラウジングの保護レベル: [強化モード](#)
 - セーフ ブラウジングの警告の無視: [警告の無視をユーザーに許可しない](#)
 - ダウンロードの詳細スキャン: [有効](#)
 - ダウンロードの制限: [不正なファイルのダウンロードをブロックする](#)

高度なデータ保護機能を有効にする

1. 管理コンソールで、[\[セキュリティ\]](#) > [\[アクセスとデータ管理\]](#) > [\[データの保護\]](#) に移動します。
2. [\[データ保護の設定\]](#) カードで、次の機能をオンにします。
 - 光学式文字認識 (OCR): 画像内の機密コンテンツのスキャンが可能になります。
 - 機密コンテンツの保存: 調査のために DLP ルールをトリガーする機密コンテンツのコピーをログファイル(および設定されている場合はエビデンスロッカー)に保存します。

必要なブラウザ拡張機能をデプロイする

コンテキストウェア アクセス / DLP に必要なデバイス属性を収集する

エンドポイントの確認とセキュアな企業向けブラウザは、デバイスデータの収集と高度なセキュリティ ポリシーの適用に不可欠な拡張機能です。次の手順で、両方の拡張機能をインストールします。

重要: 以下の手順は、テスト用の親組織部門の「**CEP 試用**」で完了する必要があります。ポリシーは、テストデバイスとユーザーを含むネストされた組織部門に継承されます。

ステップ 1 エンドポイントの確認サービスを有効にする

デバイスから情報を収集するには、エンドポイントの確認サービスが有効になっている必要があります。通常はデフォルトで有効になっていますが、確認することをおすすめします。

1. 管理コンソールのホームページから [デバイス] に移動します。
2. ナビゲーション メニューで、[モバイルとエンドポイント] > [設定] > [一般] の順にクリックします。
3. [データアクセス] カードで、エンドポイントの確認が有効になっていることを確認します。

ステップ 2 必要なブラウザ拡張機能をデプロイする

この手順により、指定したテスト組織部門内のすべてのユーザーとデバイスに、必要なブラウザ拡張機能が両方とも自動的にインストールされます。

1. [アプリと拡張機能] に移動する:
 - 管理コンソールで、[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] に移動します。
 - 左側で、テスト用の親組織部門の [CEP 試用] が選択されていることを確認します。
2. エンドポイントの確認の拡張機能を ID で追加する:
 - 黄色の + アイコンをクリックし、[Chrome アプリや拡張機能を ID で追加] を選択します。
 - エンドポイントの確認の ID 「callobklhcbilhphincmkomhkgigmfocg」を入力します。
 - [保存] をクリックします。
 - 表示されたペインで、[インストール ポリシー] を [自動インストールしてブラウザのツールバーに固定する] に設定します。
 - [保存] をクリックします。そのままページから移動しないでください。
3. セキュアな企業向けブラウザの拡張機能を ID で追加する:
 - 黄色の + アイコンをもう一度クリックし、[Chrome アプリや拡張機能を ID で追加] を選択します。
 - セキュアな企業向けブラウザの ID 「ekajlcmdfcigmdbphhifahdfjbkciflj」を入力します。
 - [保存] をクリックします。
 - 表示されたペインで、[インストール ポリシー] を [自動インストールする] に設定します。
 - [保存] をクリックします。
4. 必要に応じて、管理対象デバイスにネイティブ ヘルパー アプリをデプロイできます。詳しい手順については、[エンドポイントの確認ヘルパーアプリのデプロイ](#) に関する公式ドキュメントをご覧ください。

(省略可) デバイス トラスト コネクタを設定する

既存の IdP をリンクして、Chrome からデバイス トラスト シグナルを受け取る

このセクションでは、Chrome Enterprise デバイス トラスト コネクタの設定について説明します。なお、この設定は任意です。

目標: Chrome から ID プロバイダ (IdP) にデバイスベースのシグナルを送信して、組織の認証フローに組み込むようにします。これにより、ユーザーが管理対象ブラウザまたは Chrome ブラウザの管理対象プロフィールからアクセスしていることをウェブ アプリケーションが確認できるようになり、管理対象外ブラウザからのアクセスを効果的にブロックして、コンテキストアウェア セキュリティの価値を証明できます。

ステップ 1 Google 管理コンソールでデバイス トラスト コネクタを作成する

1. [Google 管理コンソール](#) にログインします。
2. メニュー > [デバイス] > [Chrome] > [コネクタ] に移動します。
3. [+ 新しいプロバイダの設定] をクリックします。
4. ID プロバイダ (IdP) を探して選択し、[設定] をクリックします。
5. IdP から提供された必要な設定情報を入力します。
6. (Chrome ブラウザでは省略可) この設定の適用先を選択します。
 - 管理対象ブラウザのみ
 - 管理対象プロフィールのみ
 - 管理対象ブラウザと管理対象プロフィールの両方(注: ChromeOS には適用されず、常に有効になります)。
7. [設定を追加] をクリックします。

ステップ 2 コネクタをテスト用の組織部門に適用する

1. [コネクタ] ページでテスト用の組織部門 (例: CEP 試用) を選択します。
2. [デバイス トラスト コネクタ] 設定を探します。
3. プルダウン メニューから、作成した IdP 設定を選択します。
4. [保存] をクリックします。

次のステップ: アクセス ポリシーを作成してテストする

コネクタを有効にすると、Chrome から IdP にデバイス シグナルが送信されるようになります。最後のステップでは、これらのシグナルを使用して、IdP の管理コンソール内でコンテキストアウェア アクセスのポリシーを作成します。たとえば、既存の認証フローにデバイス トラスト シグナルを追加すると、管理対象ユーザーまたは管理対象デバイスで Chrome 以外のすべてのブラウザに対して、CRM ツールへのアクセスをブロックできます。

このプロセスはプロバイダごとに異なります。

- [IdP の設定ガイドと確認手順を確認する](#)

Chrome Enterprise Premium の試用を開始する

Google Cloud コンソールで試用を有効にする

Chrome Enterprise Premium の 60 日間の試用を有効にするには、2 つの方法があります。Google 管理コンソールを使用する方法と、Google Cloud コンソールを使用する方法です。

方法 1: Google 管理コンソールを使用する。

この方法は、特権管理者アカウントが必要で、現在は教育機関以外のお客様のみ使用できます。また、お客様の組織で Google Cloud 組織を作成している必要があります。[Google Cloud 組織の作成について詳しくは、こちらのリンク](#)をご覧ください。

- 1 Google 管理コンソールにアクセスする:[Google 管理コンソール](#)に移動し、Google 管理コンソールで作成した管理者アカウントでログインします。
- 2 [Chrome ブラウザ] > [レポート] > [セキュリティ インサイト] に移動します。
- 3 [Chrome Enterprise Premium で組織のデータを今すぐ保護しましょう] というカードの [試用を開始] ボタンをクリックします。
- 4 表示された概要ページで [試用を開始] ボタンをクリックします。完了したら、下の「ライセンスを割り当てる」セクションに進みます。

ライセンスを割り当てる:

ポリシーを有効にするには、**Chrome Enterprise Premium** ライセンスが必要です。

1. [お支払い] > [サブスクリプション] に移動します。
2. [Chrome Enterprise Premium] を選択します。
3. [割り当て済みのライセンス] 列に表示される数字のハイパーリンクをクリックします。
4. テストデバイスまたはテストユーザーを検索して、ライセンスが適用されていることを確認します。
5. ヒント: 特定の組織部門または企業全体に対して、ライセンスの自動割り当てを設定することもできます。

Chrome Enterprise Premium の試用を開始する

Google Cloud コンソールで試用を有効にする

方法 2: Google Cloud コンソールを使用する。

- 1 Google Cloud コンソールにアクセスする: [Google Cloud コンソール](#) に移動し、Google 管理コンソールで作成した管理者アカウントでログインします。
 - CEP 試用専用のプロジェクトは、任意ですが作成することをおすすめします。
- 2 管理者ロールを設定する:
 1. まず、右上の組織(必須)を選択し、メインメニュー > [IAM と管理] > [IAM] に移動します。
 2. Google Cloud Platform コンソールへのログインに使用した管理者アカウントを探して、鉛筆アイコンをクリックし、プリンシパルを編集します。
 3. 表示されたポップアップウィンドウで[別のロールを追加]をクリックし、[Cloud BeyondCorp サブスクリプション管理者]を検索して選択します。
 4. [別のロールを追加]をもう一度クリックし、[閲覧者]を検索して選択したら、[保存]をクリックします。
 5. 注: ポリシーを設定してアプリケーショントンネルを作成するには、Access Context Manager、Compute Engine、ロードバランシングの追加の権限が必要になる場合があります。

ロールが反映されるまで最大 5 分ほど待ってから、次のステップに進んでください。

- 3 試用を有効にする:
 1. 「Chrome Enterprise Premium」を検索します。
 2. [登録] ボタンをクリックし、[無料試用を開始] をクリックして試用を有効にします。
 3. 無料試用を適用するプロジェクトを選択します。
 4. これで 60 日間の試用が有効になります。完了するまで 5 分ほどお待ちください。

- 4 ライセンスを割り当てる:

ポリシーを有効にするには、**Chrome Enterprise Premium** ライセンスが必要です。

1. [お支払い] > [サブスクリプション] に移動します。
2. [Chrome Enterprise Premium] を選択します。
3. [割り当て済みのライセンス] 列に表示される数字のハイパーリンクをクリックします。
4. テストデバイスまたはテストユーザーを検索して、ライセンスが適用されていることを確認します。
5. ヒント: 特定の組織部門または企業全体に対して、ライセンスの自動割り当てを設定することもできます。

Chrome Enterprise Premium のユースケース

ワークフローは、Chrome Enterprise Premium のほとんどのテストユースケースで似通ったものとなります。管理対象デバイスと管理対象外デバイスのユーザーでさまざまなシナリオが考えられるため、Chrome の一部の設定は組織によって異なります。

ユースケースごとに、[このガイドの成功基準の例](#)で概説したテストに適用できる一般的な設定のフレームワークをご紹介します。

管理対象ブラウザ / プロファイル

Chrome ブラウザを登録し、ユーザー ポリシーを適用する

設定手順でおおまかに説明しましたが、Chrome Enterprise Core を使用したブラウザ管理と、Google 管理コンソールを使用した Chrome ブラウザ管理のその他の機能について、追加情報とドキュメントへのリンクを以下にご紹介します。

- [Chrome Enterprise Core - 設定ガイド](#): 企業向け Chrome の管理、最初のブラウザの登録、ブラウザ プロファイルのレポート機能の有効化、ポリシーの優先度、API サポートのチュートリアル
- [ユーザーの関連付けについて](#): 別の会社のドメインに属するログインユーザー向け

管理対象デバイスと管理対象外デバイス

- [管理対象プロファイルと管理対象ブラウザの違いについて](#)
- [MDM を使用してブラウザを登録する](#): 企業で MDM を使用して Chrome を登録する方法を説明した各種ガイド
- [エンドポイントの確認を有効にする](#): テストプロファイルでデバイス属性の収集に必要な拡張機能
- [エンドポイントの確認で収集されるデバイス属性](#): デバイス ポスチャーに使用できる属性
- [管理対象プロファイルのレポートを有効にする](#): アクティブなログインユーザーに関するユーザーとデバイスの詳細を確認

レポートと監査

- [レポートとデータ](#): 各種レポートの確認、エクスポートの設定、その他のサードパーティ統合

パスワードの再利用

- [パスワードの再利用を管理する](#): 不審なサイトでのユーザーのパスワード使用を防ぐ

拡張機能の制御

- [アプリと拡張機能](#): 自動インストール、権限の管理、拡張機能のリクエストなどの方法

Chrome Enterprise Premium のユースケース

データ保護

DLP の管理機能を通じてデータ保護ポリシーを適用する

管理対象外のデバイスも含め、業務に不可欠なアプリケーションへのアクセスを安全に管理し、機密情報の不正な引き出しを防ぎます。これにはまず、最も機密性の高いアセットを保護するルールを設定します。

始める前に、次の手順を完了していることを確認してください。

- [Chrome Enterprise データ損失防止 \(DLP\)コネクタを管理する](#): コネクタのステータスを確認し、サードパーティの DLP ベンダーと統合 (必要な場合)

アップロード / ダウンロードの制限、印刷の制御、ウェブ / URL フィルタリング、OCR 分析

- [Chrome Enterprise Premium を使用して DLP を Chrome と統合する](#): データ保護ルールの設定方法、アクティビティアラートの設定方法、OCR を有効にする方法、DLP / URL フィルタリングルールの例

コピー / 貼り付けの制御

- [データ管理](#): 不正な共有から保護するコンテンツソース / 送信先

透かし、スクリーンショット / 画面共有からの保護、データ マスキング

- [特定のウェブページに透かしを表示する](#): 特定の URL での不正使用を防止
- [スクリーンショット / 画面共有からの保護を使用する](#): 不正な共有を防止
- [データマスキングを実施する](#): サイトに表示される機密情報を保護

脅威対策

フィッシングやマルウェアの攻撃を防ぐ

Chrome Enterprise Premium は、リアルタイムの URL のチェック、静的分析と動的分析、高度なサンドボックス化によって、ユーザーを包括的にマルウェアから保護します。詳しくは、以下のリンクをご覧ください。

- [Chrome のセーフブラウジングで閲覧データのプライバシーを保護する仕組み](#): 悪意のある行為者、マルウェア、フィッシング攻撃などからユーザーを保護
- [セーフブラウジングの保護レベル](#): 危険なサイト、危険なダウンロード、信頼できない拡張機能についてユーザーに警告する保護強化機能の詳細
- [サイト分離を使用してデータを保護する](#): データの盗難を防ぐため、ウェブサイトを個別のプロセスに分離
- [セーフブラウジングのテストリンク](#): さまざまな脅威シナリオのテストに使用できるリソース

Chrome Enterprise Premium のユースケース

アクセス制御

Chrome Enterprise Premium は、現代の働き方に適したブラウザベースのエージェントレスなセキュリティを提供します。デバイスを問わず業務に不可欠なアプリケーションに安全にアクセスできるようにし、データの不正使用を防ぎます。このガイドでは、アプリの接続と、きめ細かいセキュリティ ポリシーの作成について説明します。

アプリケーションを接続する

Chrome Enterprise Premium のセキュア ゲートウェイを使用して、従来の VPN を使用せずにウェブ アプリケーションにトラフィックをルーティングすることで、一貫したポリシーを適用しながらレイテンシを短縮できます。

- **SaaS アプリケーション**：セキュア ゲートウェイの IP アドレスをアプリの許可リストに追加してアクセスを制御し、セキュリティ チェックを簡素化します。
 - [ガイド: SaaS アプリケーションへのセキュアなアクセス](#)
- **社内向けウェブ アプリケーション**：ゼロトラスト フレームワークを適用し、きめ細かい制御で社内向けアプリが社外に公開されないように保護します。
 - [ガイド: 限定公開ウェブアプリケーションへの安全なアクセス](#)

Chrome Enterprise Premium は、より広範なアプリケーション エコシステムも保護します。

- [Google Workspace アプリを保護する](#)
- [Google Cloud\(GCP\)ウェブアプリケーションを保護する](#)
- [アプリコネクタを使用してGoogle Cloud 以外のアプリを保護する](#)
- [Chrome アプリにSAML SSOを設定する](#)

高度なコンテキストウェア アクセス ポリシーを作成する

アプリを接続したら、ユーザー、デバイス、場所などに基づいて強力なアクセス ポリシーを作成します。

- **セキュリティ パートナーのシグナルを統合する**：CrowdStrike や Microsoft Intune などのツールのデバイス ポスチャール データを使用してポリシーを強化できます。
 - [ガイド: クライアントサイドのパートナー統合を設定する](#)
- **カスタム ポリシーを構築する**：デバイスのコンプライアンスや時間ベースのアクセスなど、一般的なシナリオのテンプレートを使用できます。
 - [ポリシーの例を見る](#)
- **DLP と組み合わせる**：デバイスのセキュリティ ポスチャールに基づいてデータ損失防止(DLP)ルールをカスタマイズし、きめ細かく制御できます。
 - [DLPとCAAを組み合わせる方法を確認する](#)

Chrome Enterprise Premium のユースケース

監査と可視化

セキュリティ イベントを可視化する

ユーザーの危険なアクティビティを可視化することは、セキュリティ プログラムの最も重要な側面の一つです。Chrome Enterprise Premium の脅威対策とデータ保護機能では、ユーザーの危険なアクティビティに関するイベントの詳細なログが取得されます。これにより、管理者はユーザーのアクティビティと行動を監視、確認、分析し、組織内のあらゆるリスクを軽減できます。この情報の表示と監査について詳しくは、以下のリンクをご覧ください。

- [Chrome のログ イベント](#) : さまざまなセキュリティ イベントを分析して監査
- [Chrome のレポートコネクタ](#) : SIEM ツールにセキュリティ イベントを送信
- [セキュリティ ダッシュボード](#) : さまざまなセキュリティ レポートの概要を確認 (最大 180 日間)
- [セキュリティ 調査ツール](#) : セキュリティとプライバシーに関する問題を特定し、優先順位を付けて対処
- [エビデンスロッカー](#) : マルウェアとして報告されたファイルやデータ保護ルールに違反しているファイルを検査

サードパーティ製品との連携

Chrome を IdP やさまざまなアプリケーションと統合する

Chrome デバイストラストコネクタを使用すると、管理対象の Chrome ブラウザデバイスから取得したコンテキストウェアシグナルを、サードパーティの ID プロバイダ (IdP) と共有できます。また、Google をさまざまな企業アプリに統合して、ユーザーが使い慣れた認証情報で安全にログインできるようにすることも可能です。

- [Chrome Enterprise デバイストラストコネクタを管理する](#) : IdP とサードパーティ統合 (SIEM / XDR) で使用
- [サードパーティアプリとカスタムアプリを統合する](#) : Workspace を他の IdP と統合
- [社内向けウェブアプリをデプロイする](#) : GCP、他のクラウド、オンプレミスのデータセンターでホストされているアプリをユーザーに割り当て

問題のトラブルシューティング

Chrome Enterprise Premium のトラブルシューティング

このセクションでは、Chrome Enterprise Premium の初期設定に関する一般的な問題を診断して解決する論理的なワークフローについて説明します。

ステップ 1: 基本事項の確認(「電源は入っているか?」)

複雑なルールを調査する前に、簡単なベースライン テストでコアサービスが機能していることを確認します。

1. 管理コンソールで、[セキュリティ]>[アクセスとデータ管理]>[データの保護]>[ルールを管理]>[ルールを追加]>[新しいルール]に移動します。
2. 「Chrome Enterprise Premium テストルール」などの名前を付けて、[スコープ] セクションで Chrome Enterprise Premium テスト用の組織部門を選択します。
3. [アプリ] 設定の [Chrome] セクションで [ファイルがアップロードされました] を選択します。
4. [条件を追加] をクリックし、[すべてのコンテンツにテキスト文字列が含まれる] に設定して、「factorytestkeyword」のような一意のキーワードを入力します。
5. [操作] 設定で、操作を [ブロック] に設定します。必要に応じて、カスタム メッセージを追加できます。[続行] をクリックし、次の画面で [作成] をクリックします。

Security > Data protection > Rules > CEP Test Rule



← Rule List

CEP Test Rule

Active

EDIT RULE

INVESTIGATE RULE

Scope

Organizational units / CEP Trial

Exclude organizational units

Groups

Exclude groups

Apps

Chrome

File uploaded

Conditions

All content

Contains text string "factorytestkeyword"

Actions

Alert Disabled

Chrome Block

Severity Low

6. テストファイルを作成する : ローカル デバイスで、キーワード「factorytestkeyword」のみを含む書式なしテキスト ファイルを作成します (例 : dlp_test.txt)。
7. ルールをテストする : テストユーザーまたは登録済みのブラウザを使用して、Google ドライブなどのサイトにファイルをアップロードしてみます。
 - アップロードがブロックされた場合 : コアシステムは機能しています。問題は、より具体的で複雑なルールにあるため、簡略化して問題の特定を試みます。
 - アップロードが成功した場合 : 問題は根本的なものです。前のセクションの手順を確認し、次のセクションでシステム設定をチェックします。

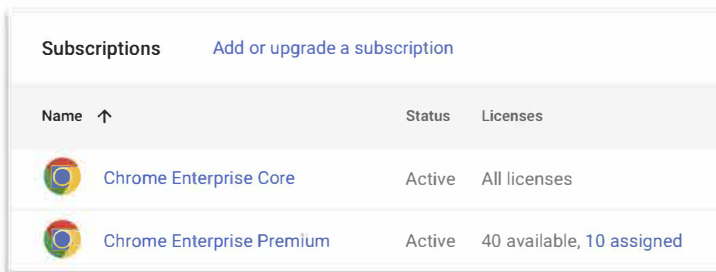
問題のトラブルシューティング

Chrome Enterprise Premium のトラブルシューティング：続き

ステップ 2: 一般的な問題(単純な問題の除外)

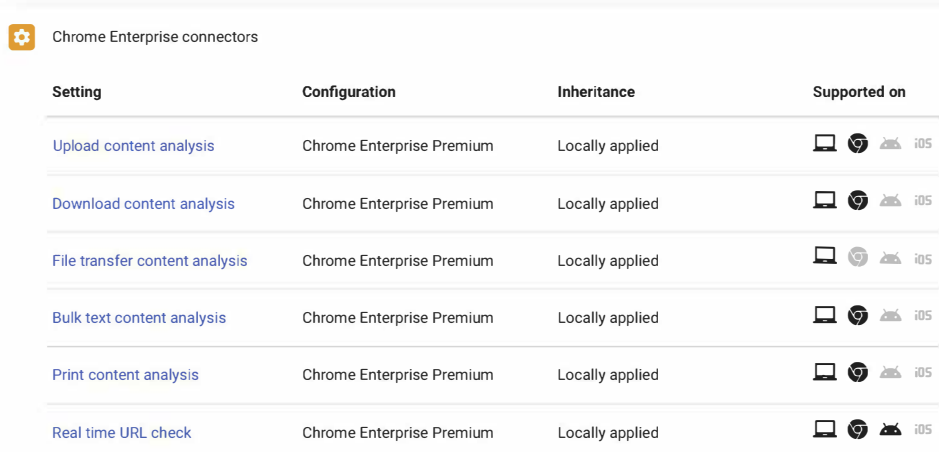
テストした DLP ルールが機能しなかった場合は、Google 管理コンソールで、次のよくある設定エラーを確認します。

- **ライセンスを確認する**：問題が生じているテストユーザーまたはテストデバイスに有効な **Chrome Enterprise Premium** ライセンス が割り当てられているか確認します。【お支払い】>【サブスクリプション】で確認できます。



Subscriptions Add or upgrade a subscription		
Name ↑	Status	Licenses
 Chrome Enterprise Core	Active	All licenses
 Chrome Enterprise Premium	Active	40 available, 10 assigned

- **コネクタの設定を確認する**：DLP が機能するためには、セキュリティ コネクタが **[Chrome Enterprise Premium]** に設定されている必要があります。
 - a. **【追加の設定】の【ファイルのアップロードを遅らせる】が【即時アップロードを許可する】に設定されている場合**、イベントはログに記録されるだけで、ブロックされません。
 - b. **セーフ ブラウジング モードを確認する**：脅威対策のコアエンジンを機能させるには、セーフ ブラウジング保護強化機能を有効にする必要があります。
 - c. **問題が生じているユーザーまたはデバイスが、コネクタがプロビジョニングされ、DLP ルールのターゲットとなっている組織部門に属していることを確認します。**
 - d. 具体的な設定手順については、このガイドの [「Chrome Enterprise Premium コネクタの設定を有効にする」セクション](#) をご覧ください。



Chrome Enterprise connectors			
Setting	Configuration	Inheritance	Supported on
Upload content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Download content analysis	Chrome Enterprise Premium	Locally applied	   iOS
File transfer content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Bulk text content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Print content analysis	Chrome Enterprise Premium	Locally applied	   iOS
Real time URL check	Chrome Enterprise Premium	Locally applied	   iOS

問題のトラブルシューティング

Chrome Enterprise Premium のトラブルシューティング：続き

ステップ 3: 診断ツール(システムログの確認)

Chrome には、ブラウザの動作を正確に確認できるツールが組み込まれています。それらのページを使用して、テストデバイスから詳細な診断情報を直接取得します。右側のペインには、最も詳細な情報が表示されます。

- **DLP とマルウェアのイベント:** `chrome://safe-browsing/#tab-deep-scan`
 - このタブはテストする前に開いてください。セキュリティスキャンのリアルタイムログが表示されます。`triggered_rules` を含む「result」エントリを探して、発動したルールと実際の動作を確認します。イベントが表示されない場合、ブラウザでは動作の評価は行われていません。

```
[10/14/2025, 2:44:45 PM]
{
  "request_token": "35D9CE08556EC4C05A5025A542E8A75830E497DD23A7305
5D6B360431F14F49043A97A5072B67B2890E5B2C04F1ADF8D6C8185B8AE3ED1
BEDD4891187DA1CAEF866EEED19D1B2CD57513DC7193E4060D1A030CB5CE9F2
9EBB19FEA0CF74E94EC54BD48E2641E03E253E0CFE1C227D47BC9B1B0FCC7D6
1AFD1BD11BE52C11DA3B",
  "results": [{
    "status": "SUCCESS",
    "tag": "dip",
    "triggered_rules": [{
      "action": "REPORT_ONLY",
      "rule_id": "685305242",
      "rule_name": "[D&R] Evidence Locker file uploads to non-corp domains"
    }]
  }]
}
```

- **URL カテゴリの検証:** `chrome://safe-browsing/#tab-urt-lookup`
 - テストする前にこのタブを開いてから、カテゴリを調べるサイトを表示すると、Google がそのウェブサイトをどのように分類しているかを正確に把握できます。URL ベースのルールをトラブルシューティングする場合は、ここに表示される正確なカテゴリ名(例: `/Internet & Technology/Computer Security`)を使用する必要があるため、この手順は不可欠です。

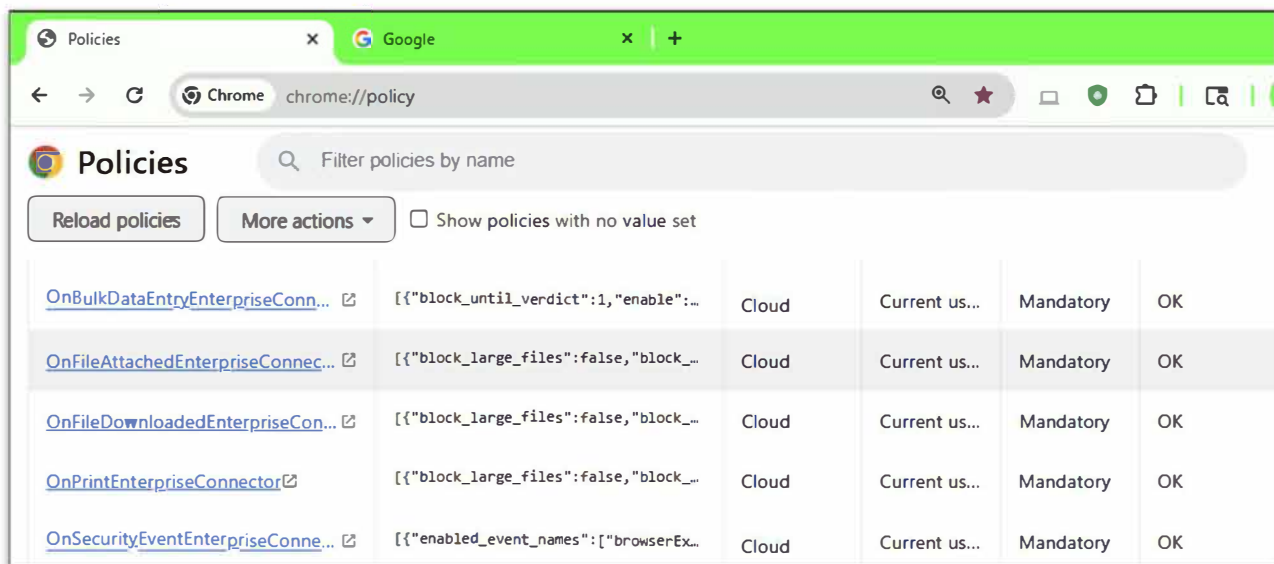
```
{
  "threat_info": [{
    "cache_duration_sec": "90",
    "cache_expression_match_type": "EXACT_MATCH",
    "cache_expression_using_match_type": "cloud.google.com/free",
    "verdict_type": "SAFE"
  }],
  "url_categories": ["/Internet & Technology/Cloud Storage", "/Internet & Technology",
"/Internet & Technology/Enterprise Technology"]
}
```

問題のトラブルシューティング

Chrome Enterprise Premium のトラブルシューティング：続き

ステップ 3: 診断ツール(システムログの確認の続き)

- 適用済みのポリシー : chrome://policy
 - ブラウザで有効になっているポリシーの正式なソースです。[ポリシーを再読み込み]をクリックして強制的に更新します。主要なコネクタポリシー (例: OnFileAttachedEnterpriseConnector) が有効になっていることを確認します。
 - このページは、ポリシーの競合を特定する場合や、デバイスまたはユーザー アカウントがドメインに登録されていることを確認する場合も重要となります。
 - 最近変更を加えた場合は、[ポリシーを再読み込み]をクリックして、Chrome ポリシーが更新されたことを確認します。
 - 注: DLP ルールがデバイスに適用されるまで 5 分以上かかることがあります
 - 次の画像は、[このガイドで前述](#)したように必要なすべてのポリシーが設定された正常なポリシーページです。



- デバイスシグナルに関する問題(CAA): エンドポイントの確認のデバッグログ
 - chrome://extensions で、[エンドポイントの確認とセキュアな企業向けブラウザの拡張機能](#)がインストールされ、有効になっていることを確認します。
 - コンテキストウェア アクセスに関する問題については、エンドポイントの確認の拡張機能アイコンを右クリックし、[オプション]>[ログを表示]を選択します。同期メッセージとエラーを探します(例: 高度なデバイス シグナルに必要な「ネイティブ ヘルパー」への接続の失敗など)。

よくある質問

ユーザーベースの保護を提供するには Google Workspace が必要ですか？

必ずしも必要とは限りません。[Google Cloud Identity Free](#) を管理対象ユーザー アカウントに使用したり、[現在の IdP と Google を同期](#)したりすることで、ユーザーベースの保護を提供できます。

他のブラウザもサポートしていますか？

Chrome Enterprise Premium は Google Chrome ブラウザ内でのみ機能しますが、このソリューションには、他のブラウザでの機密データへのアクセスを防ぐ機能が用意されています。

このソリューションはシークレット ウィンドウをサポートしていますか？

[データ管理](#) ポリシーを活用して、アプリ、ブラウザ、プロファイル間で共有を許可するデータを制限（シークレット モードを含む）できます。また、ユーザーがシークレット モードでブラウジングできるかどうかを制限することもできます。

Chrome ではデータはどのように収集されますか？

収集されるデータは、管理者の設定によって異なります。

- デバイスが Chrome 管理に登録されていてレポートがオンになっている場合は、[収集されるデータについて詳しく説明したこちらのドキュメント](#)をご確認ください。
- Chrome セキュリティ イベント レポートがオンになっている場合は、[収集されるデータについて詳しく説明したこちらのドキュメント](#)をご確認ください。
- [Chrome のログイベントおよび属性に関するその他の情報については、こちらのリンク](#)をご覧ください。

参考情報

Chrome Enterprise Premium

[!\[\]\(7283d9faf9c88ace5d8a560ea0213e53_img.jpg\) Chrome Enterprise Premium の概要](#)

[!\[\]\(72b4cf351241b08691672e806c1604b7_img.jpg\) Chrome Enterprise Premium の購入](#)

Chrome Enterprise Core

[!\[\]\(77e670be72de63f664b9f3cf25895195_img.jpg\) Chrome Enterprise Core の概要](#)

[!\[\]\(784bf2e4d7fa94d6a886b9dc39d8ea88_img.jpg\) Chrome 管理の設定](#)

[!\[\]\(1c70f21f694d12b9fc928edb998ea27b_img.jpg\) Chrome 管理導入ガイド](#)

Chrome ブラウザの統合

[!\[\]\(3a91434fb6b4bec5a2c52d3fbe2b9c14_img.jpg\) Chrome ブラウザ レポートコネクタ](#)

[!\[\]\(0a9d8c730cfe4d693d610f984c906f3a_img.jpg\) Chrome ブラウザ デバイストラストコネクタ](#)