



お問い合わせ

ブラウザの効果的な導入方法と運用管理のベスト プラクティスなど、
詳細をご希望の方は下記または QR コードよりお気軽にお問い合わせください。

https://chromeenterprise.google/intl/ja_jp/contact/browser/

© Copyright 2024 Google
Google は、Google LLC の商標です。その他すべての社名および製品名は、それぞれ該当する企業の商標である可能性があります。



Chrome Enterprise ガイドブック

March 2025



はじめに

ビジネスにおけるデジタル化がより加速する昨今では、SaaS を始めとするクラウド サービスが業務で広く用いられ、場所や時間に依存しない働き方が急速に広まっています。

SaaS アプリケーション拡大に伴い、働く人々はより業務でブラウザを操作する時間が増え、さまざまなデジタルデータや情報をブラウザ経由で扱うようになっていきます。言い換えれば、デジタル時代は、日々の業務がなくてはならないほどブラウザに依存するようになった時代とも言えます。

そうした中で、企業・組織における新たな課題となるのがサイバー セキュリティ対策です。登場当初、Web サイト上の情報を閲覧するツールに過ぎなかったブラウザは、いまでは重要な情報をやり取りするためのエンドポイントのツールでもあります。サイバー攻撃被害や情報漏えいによるセキュリティ事故を防ぐために、いまこそ組織的にブラウザのセキュリティ対策を見直す時が来ています。

Google では、これまで全世界数十億人に利用されているブラウザとして「Google Chrome」を開発・提供し、今日まで進化を続けてきました。その上で、ブラウザの管理機能やセキュリティ機能を充実させることで、こうした企業・組織の課題を解消しようとしています。

本書では、企業の Google Chrome ブラウザ利用において、セキュリティやガバナンスを確保する上で欠かせない「Chrome ブラウザ クラウド管理 (Chrome Enterprise Core)」の各機能とその設定方法を紹介しています。次に、より高度なポリシー設定や強固なセキュリティを実現したい方に向けて、有償ソリューション「Chrome Enterprise Premium」での機能と設定を紹介しています。

Chrome Enterprise Core、Chrome Enterprise Premium とも幅広い機能を搭載しているので、設定方法に迷ってしまうことがあるかもしれません。そのようなときにぜひ本書を活用いただき、自社に必要な対策を行いながら、柔軟な働き方とセキュリティを実現する IT 環境を実現していただければと思います。



Contents

Chrome Enterprise Core

基本設定

- Chrome Enterprise Core の導入メリットを得る P5
- まずはこのポリシーから①「CloudReportingEnabled」 P7
- まずはこのポリシーから②「OnSecurityEvent EnterpriseConnector」 P8
- ポリシーの優先順位のおさらい P9
- 従来のポリシーはそのまま運用「CloudPolicyOverrides PlatformPolicy」 P10
- 管理対象とする Chrome ブラウザの登録 P12

セーフ ブラウジング シリーズ

- セーフ ブラウジングの有効化「SafeBrowsingProtectionLevel」 P15
- セーフ ブラウジングの強制「DisableSafeBrowsingProceedAnyway」 P17
- 特定ドメインの保護、セーフ ブラウジングの制御「SafeBrowsingAllowlistDomains」 P18
- ダウンロードの徹底管理「DownloadRestrictions」 P19

セキュリティ シリーズ

- 特定のサイトのアクセスをブロック
 - もしくは社内のポータル サイトのみアクセスを許可「URLBlocklist」 P20
- 広告をコントロール、ビジネスに集中「AdsSettingForIntrusiveAdsSites」 P23
- 必要なポップアップだけを許可
 - またはポップアップをブロック「DefaultPopupsSetting」 P24
- シークレット モードの無効化で、全てを明確に「IncognitoModeAvailability」 P25

Contents

Chrome Enterprise Core

パスワード マネージャー シリーズ

- パスワードは自動で管理、安全性と利便性の両立「 PasswordManagerEnabled 」 P26
- 不正利用を未然に防ぐ、パスワード警告システム！「 PasswordProtectionWarningTrigger 」 P27
- パスワード変更の URL を指定「 PasswordProtectionChange PasswordURL 」 P30
- 企業のログインページの保護を強化「 PasswordProtectionLoginURLs 」 P31

更新管理シリーズ

- 更新管理もお手の物「 Chrome ブラウザのバージョンの固定 」 P32
- ブラウザの更新は計画的に自動化「 AutoUpdateCheckPeriodMinutes 」 P34
- 再起動を通知、アップデートのスムーズな実施「 RelaunchNotification 」 P36
- 帯域幅の削減、アップデートの効率化「 Cacheable URLs 」 P38

拡張機能シリーズ

- 徹底的な拡張機能の管理「 ExtensionInstallAllowlist 」 & 「 ExtensionInstallForcelist 」 & 「 ExtensionInstallBlocklist 」 P39
- 外部拡張機能のインストールをブロック「 BlockExternalExtensions 」 P41

作業効率シリーズ

- ワンクリックでホームへ、作業の効率化！「 ShowHomeButton 」 P42
- ホームは社内ページから、効率化の極！「 HomepageLocation 」 P43
- 起動時に最重要ページへ、生産性の向上！「 RestoreOnStartupURLs 」 P44
- Chrome を既定に、ブラウジングを最適化！「 DefaultBrowserSettingEnabled 」 P45
- 閲覧データの自動消去、セキュリティを確保！「 BrowsingDataLifetime 」 P46
- アイドル状態の対応、企業のルールで決定！「 IdleTimeout 」 & 「 IdleTimeoutActions 」 P47

Chrome Enterprise Premium

基本設定

- ポリシーの優先順位のおさらい P50
- Chrome Enterprise Premium ライセンスの有効化 P51
- Chrome Enterprise Premium をフルに活用する為に P52
- まずはこのポリシーから「 エンタープライズ コネクタを許可する 」 P53

シナリオ1

- 「 個人情報が入ったファイルのダウンロードとアップロードの禁止 」 P54

シナリオ2

- 「 URL のカテゴリによるフィルタリング 」 P56

シナリオ3

- 「 生成 AI サイトへのコードの貼り付けの禁止 」 P58

シナリオ4

- 「 管理されていないブラウザからの生成 AI サイトへのアクセス管理 」 P60

シナリオ5

- 「 オンライン ストレージからの大量ダウンロードの検知 」 P63

シナリオ6

- 「 BYOD 上のブラウザからのデータのダウンロード禁止 」 P65

シナリオ7

- 「 オンライン ストレージへの透かしの追加 」 P67

シナリオ8

- 「 DLP ルールをトリガーしたアクションを調査する 」 P69

Chrome Enterprise Core

各ユーザーのブラウザをクラウドから一元管理

自社において各従業員が Chrome ブラウザを利用している場合、IT 管理者は「Chrome ブラウザ クラウド管理（Chrome Enterprise Core）」を利用することで、各ユーザーのブラウザに関する設定やポリシーを一元管理し、組織全体のセキュリティ強化や統制確保を実現することができます。

Chrome Enterprise Core 上で設定できるポリシーは 300 近くに及び、各企業のブラウザ運用のニーズに沿った設定を行うことが可能です。中でも本章では、ブラウザの基本設定から、安全な Web ブラウジング機能や、アクセス制御、パスワード管理、ブラウザの更新管理などのいくつかの観点から、セキュリティ強化に向けてぜひ設定しておくべき重要なポイントを解説しています。

基本設定

Chrome Enterprise Core の導入メリットを得る

Chrome Enterprise Core を業務に導入し、Chrome ブラウザの組織内の利用制御を実現するには、以下の作業が必要です。

- ✓ 管理対象とする Chrome ブラウザの登録
- ✓ Chrome ブラウザの使用状況の可視化
- ✓ Chrome ブラウザでのイベントログの可視化

これらの作業を終えたのち、必要に応じて以下の作業を実施します。

- ✓ ポリシー適用の優先度の設定
- ✓ セーフ ブラウジングの設定

また、Chrome Enterprise Core では、拡張機能の管理、更新の管理、セキュリティの強化など、Chrome ブラウザによる業務の推進に関するさまざまな要望や課題に対応しています。

基本設定

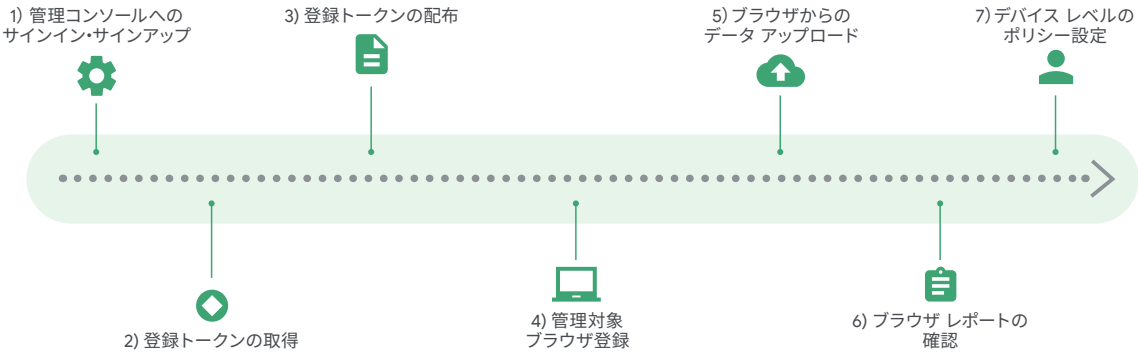
Chrome Enterprise Core の導入メリットを得る

①管理対象とする Chrome ブラウザの登録

Chrome Enterprise Core では、example.com などのドメインごとにデバイスを登録します。ただし、Chrome ブラウザを使用するユーザーが個別に Chrome Enterprise Core にログインしてデバイスを登録する必要はありません。登録のためのトークンを管理者が生成し、トークンを配布することで、デバイスを登録し管理できます。

トークンの GUID（グローバルに一意識別子）は、Chrome Enterprise Core の管理コンソールでランダムに生成できます。そして、トークンは、デバイスを Chrome Enterprise Core に登録する際に一度だけ使用します。多数のデバイスを登録するために 1 つのトークンを使用することも、1 台のデバイスのみを登録するために 1 つのトークンを使用することもできます。

以下に、管理対象ブラウザの登録の流れを示します。



② Chrome ブラウザの使用状態の可視化

トークンによって管理対象として登録した Chrome ブラウザの使用状態を可視化します。これにより、ユーザーによる私的な利用を抑制し、業務に使用する Chrome ブラウザの環境を整えやすくなります。管理対象ブラウザの使用状況は、管理コンソールの [Chrome ブラウザ] → [設定] で [管理対象ブラウザのクラウド レポートを有効にする] ことで可視化できます。

レポートを有効にすると、右記の内容を確認できます。

- ・管理コンソールでの操作
- ・ポリシー名、ポリシーのソース／範囲などのブラウザのポリシー
- ・バージョン、パス、プロファイル名、プロフィールにログインしたユーザーのメールアドレスなどのブラウザに関する情報
- ・拡張機能 ID、ポリシー名などの拡張機能のポリシー
- ・バージョン、名称、説明などの拡張機能に関する情報
- ・マシン名、OS のバージョンなどのマシンに関する情報
- ・ユーザーに表示された警告数、およびユーザーが警告をクリックしてページ移動した回数

⚠ デフォルトでは、レポートは 24 時間ごとに更新されます。この更新間隔は、3~24 時間の範囲で変更できます。

まずはこのポリシーから ① 「CloudReportingEnabled」

管理対象ブラウザに関するレポート

管理コンソールでの設定

管理対象ブラウザの状態を可視化する

私的な利用を防ぐため、ブラウザの状態を可視化し、管理者が環境を整えやすくします。

- 1 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- 2 [ユーザーとブラウザ] 次に ルート組織部門 を選択します。
- 3 [フィルタを追加、または検索] に “ CloudReporting ” と入力し、[管理対象ブラウザに関するレポート] をクリックします。
- 4 [管理対象ブラウザのクラウド レポートを有効にする] を選択します。
- 5 編集した内容を保存し、設定は完了です。

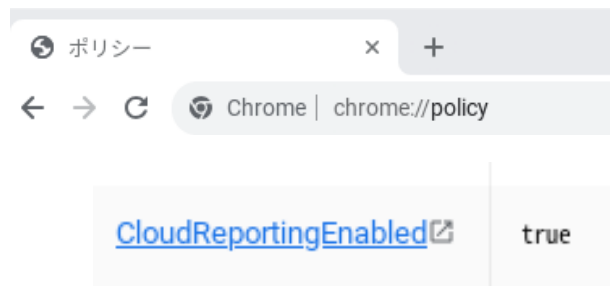


デバイスでの検証

管理対象ブラウザの状態を可視化する

私的な利用を防ぐため、ブラウザの状態を可視化出来ていることを確認します。

- 1 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- 2 [CloudReportingEnabled] が [true] になっていれば適切にポリシーが反映されています。
- 3 この値が見つからない場合は “ chrome://policy ” 画面の “ ポリシーを再読み込み ” を試し、それでもこのポリシーが適用されていない場合は、再度管理コンソールで変更内容が保存されているかご確認ください。



まずはこのポリシーから ② 「OnSecurityEvent EnterpriseConnector」

イベント レポート

管理コンソールでの設定

管理対象ブラウザのイベントを可視化する

ブラウザ上のイベント (パスワードの再利用、マルウェアのダウンロード、拡張機能のインストールなど) を可視化し、管理者が環境を整えやすくします。

- 1 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- 2 [ユーザーとブラウザ] 次に ルート組織部門 を選択します。
- 3 [フィルタを追加、または検索] に “ OnSecurityEventEnterpriseConnector ” と入力し、[イベント レポート] - [以前のビューで編集] をクリックします。
- 4 [イベント レポートを有効にする] を選択します。
- 5 [追加の設定] をクリックし、可視化したいイベントを選択します。
- 6 編集した内容を保存し、設定は完了です。

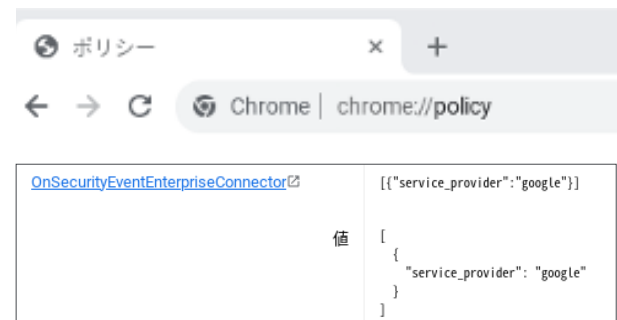


デバイスでの検証

管理対象ブラウザの状態を可視化する

ブラウザのイベントを可視化出来ていることを確認します。

- 1 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- 2 [OnSecurityEventEnterpriseConnector] が設定されていれば適切にポリシーが反映されています。
- 3 この値が見つからない場合は “ chrome://policy ” 画面の “ ポリシーを再読み込み ” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



ポリシーの優先順位のおさらい

管理コンソールでの設定

ポリシーの優先順位について

<https://support.google.com/chrome/a/answer/9037717>

Chrome Enterprise Core は他の管理ソリューション (Group Policy) などで設定したポリシーと共存できるように設計されています。

ポリシーの優先順位の概念として、「デバイス ポリシー」と「ユーザー ポリシー」が存在します。

●**デバイス ポリシー**（クラウド マシンレベル）：
「登録トークン」が埋め込んであるデバイスに対して適用するもの。（会社所有の端末は基本的に「登録トークン」を全てのデバイスに対し配布することをおすすめしております。）

●**ユーザー ポリシー**（クラウド ユーザーレベル）：
会社のドメインに紐づいたアカウントに対して適用されるもの。（Google 管理コンソール内の ディレクトリ下のユーザータブ内のユーザー 注：野良ユーザーには適用されません。）



既定ではマシンレベルのポリシーが優先され、後から優先順位の変更は可能です。

優先順位を変更するポリシー
CloudPolicyOverridesPlatformPolicy /
CloudUserPolicyOverridesCloudMachinePolicy



従来のポリシーはそのまま運用 「CloudPolicyOverrides PlatformPolicy」

ポリシーの優先度

管理コンソールでの設定

従来のポリシーを並行で運用

Group Policy などで設定したポリシーをそのまま引き継げます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “Precedence” と入力し、[ポリシーの優先度] をクリックします。
- 4 デフォルトで [パソコン > パソコンのクラウド > OS ユーザー > Chrome プロフィール] となっています。
- 5 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

Chrome Enterprise Core でのポリシー運用に切り替える

Chrome Enterprise Core での運用に順応してきたら、従来の運用方法で管理していたポリシーは全て移行し、先進的な Chrome Enterprise Core でのポリシー運用に切り替えましょう。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “Precedence” と入力し、[ポリシーの優先度] をクリックします。
- 4 [パソコンのクラウド > パソコン > OS ユーザー > Chrome プロフィール] を選択します。
- 5 編集した内容を保存し、設定は完了です。



従来のポリシーはそのまま運用 「CloudPolicyOverrides PlatformPolicy」

ポリシーの優先度

デバイスでの検証

ポリシーの優先度をブラウザ上で確認する

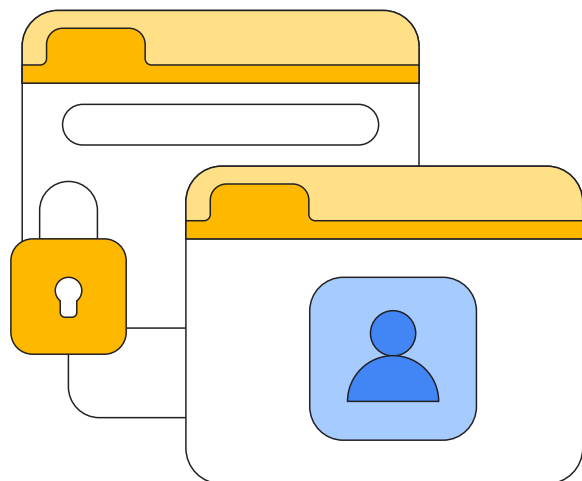
エンドユーザーのブラウザ上でのポリシー優先順位を確認します。

- ① 管理された検証用ブラウザで“chrome://policy”へ移動します。
- ② (ポリシーの優先度を変えた場合は“CloudPolicyOverridesPlatformPolicy”が“true”になっており、) その下の「現在の優先順位」が管理コンソール上で選択した順序になっていれば適切にポリシーが反映されています。
- ③ この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“chrome://policy”画面の“ポリシーを再読み込み”を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

ポリシー

Chrome | chrome://policy

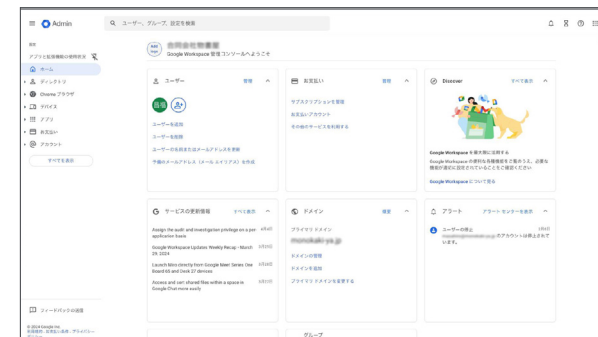
ポリシー名	ポリシーの値	ソース	適用先
CloudPolicyOverride	true	クラウド	マシン
値	true		
情報	このポリシーは想定どおり動作していますが、同じ値が設定されている別のポリシーが優先されています。		
値 (優先)	true	クラウド	現在のユーザ
CloudUserPolicyOver	false	クラウド	マシン
現在の優先順位	クラウドマシン>プラットフォームマシン>プラットフォームユーザー>クラウドユーザー		



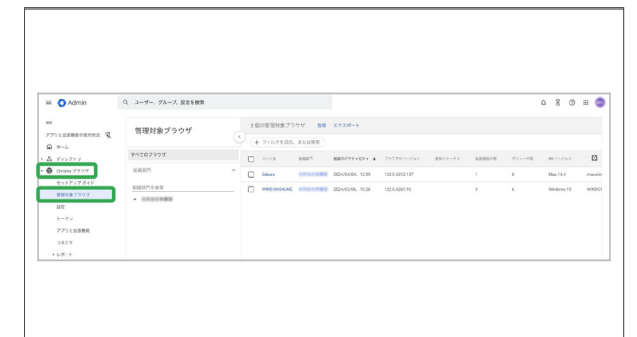
管理対象とする Chrome ブラウザの登録

①登録トークンの生成

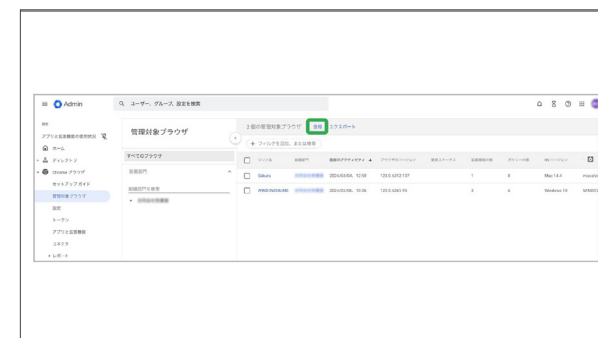
管理対象とする Chrome ブラウザを Chrome Enterprise Core に登録するため、トークンを生成し、対象 OS ごとに設定したのち、登録状況を確認します。まず、Chrome Enterprise Core に登録するためのトークンを生成します。



- ① Chrome Enterprise Core の管理コンソールにログインします。



- ② [Chrome ブラウザ] → [管理対象ブラウザ] を順にクリックします。



- ③ [登録] をクリックします。トークンが表示されます。



- ④ 拡張子 .reg ファイル、テキスト ファイルなどでトークンを取得します。

②トークンの登録

Windows での登録

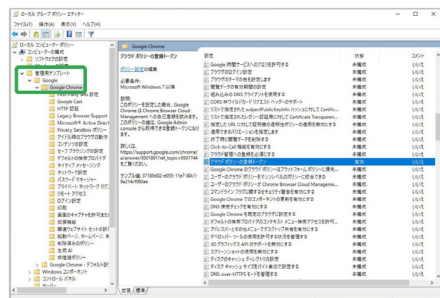
Windows 上で動作する Chrome ブラウザは、右記の方法で Chrome Enterprise Core の管理対象にできます。

- ➡ グループポリシー管理エディターを使用する
- ➡ 拡張子 .reg ファイルを使用する

管理対象とする Chrome ブラウザの登録

②トークンの登録

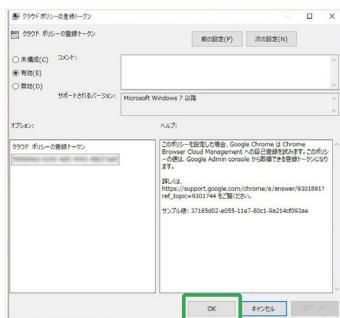
－ グループ ポリシー管理エディターを使用する



①グループ ポリシー管理エディターを起動します。

❗ グループ ポリシー管理エディターは、管理者権限が付与されたユーザーで起動してください。

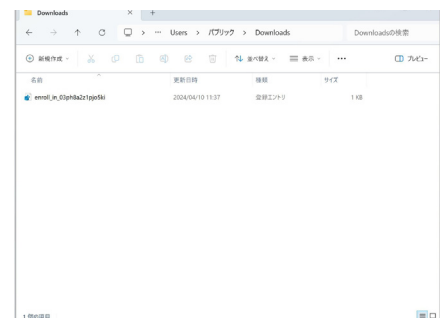
- Chrome の管理用テンプレート (Chrome ADX/ADMX テンプレート) は、以下の Web ページからダウンロードできます。
https://chromeenterprise.google/intl/ja_jp/browser/download/#manage-policies-tab
- ダウンロードした管理用テンプレートは、グループ ポリシー管理エディターに追加してください。



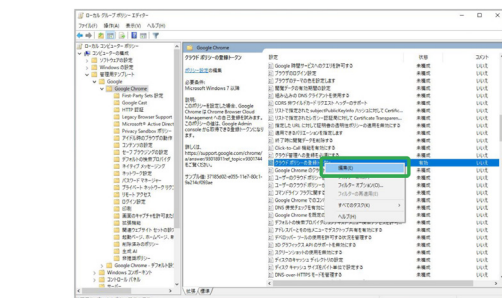
④ [オプション] にトークンの値を設定し、[OK] をクリックします。⑤ターミナルを起動し、gpupdate コマンドによってグループ ポリシーを適用します。

－ 拡張子 .reg ファイルによる登録

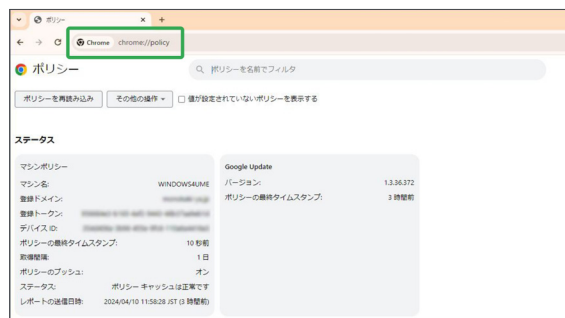
❗ ※拡張子 .reg ファイルによる登録は、管理者権限が付与されたユーザーで実行してください。



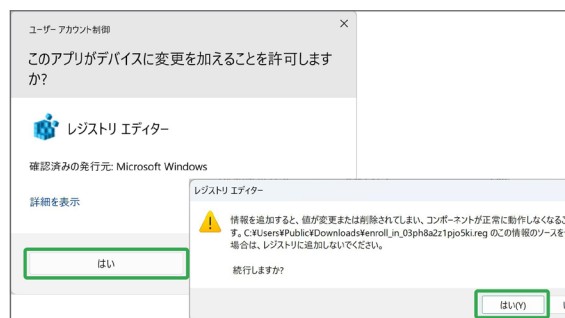
①拡張子 .reg ファイルをダブルクリックします。レジストリ エディターが起動します。



② [コンピューターの構成] → [管理用テンプレート] → [Google] → [Google Chrome] を順に展開します。
③ [クラウド ポリシーの登録トークン] を右クリックして [編集] を選択します。



⑥ Chrome ブラウザを起動し、アドレスバーに「chrome://policy」と入力します。Chrome ブラウザが動作するマシンのポリシーが表示されます。



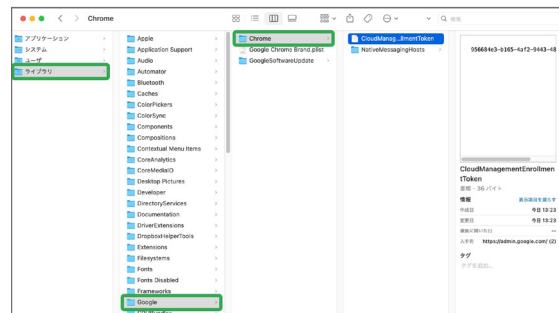
② [はい] をクリックします。注意を促すダイアログ ボックスが表示されます。
③ [はい] をクリックします。トークンのキーと値がレジストリに追加されます。

管理対象とする Chrome ブラウザの登録

①登録トークンの生成

✓ macOS での登録

macOS 上で動作する Chrome ブラウザを Chrome Enterprise Core の管理対象とするため、テキスト ファイル形式で入手したトークンを登録します。



① macOS にログインします。

❗ 管理者権限が付与されたユーザーとしてログインしてください。

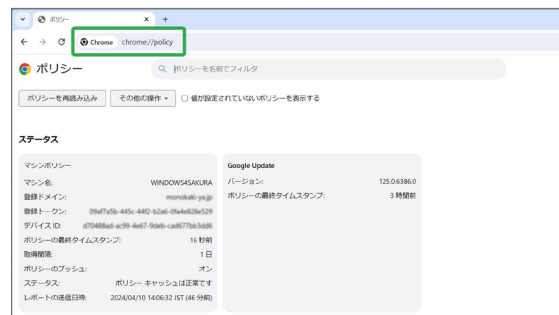
②ダウンロードしたテキストファイル (トークン) を、以下の場所に収めます。
[ライブラリ] → [Google] → [Chrome]



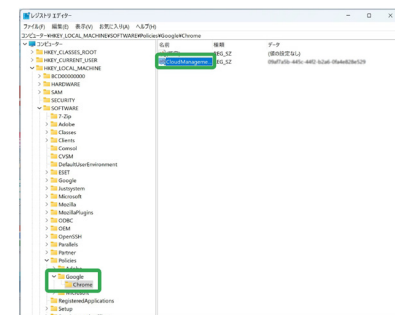
③ Chrome ブラウザを起動し、アドレスバーに「chrome://policy」と入力します。Chrome ブラウザのユーザーに関するポリシーが表示されます。

②トークンの登録

－ 拡張子 .reg ファイルによる登録



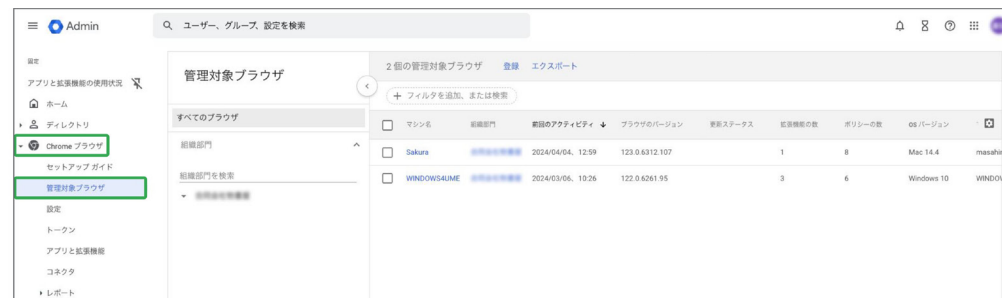
④ Chrome ブラウザを起動し、アドレスバーに「chrome://policy」と入力します。Chrome ブラウザが動作するマシンのポリシーが表示されます。



❗ Chrome ブラウザが動作するマシンのポリシーが表示されるときには、レジストリ エディターを起動して [HKEY_LOCAL_MACHINE] → [SOFTWARE] → [Policies] の配下に [Google] → [Chrome] を作成し、キーとして「CloudManagementEnrollmentToken」、値としてトークンの値をそれぞれ設定してください。

③登録の確認

Chrome ブラウザが管理対象として登録されたことを確認します。



管理コンソールで、[Chrome ブラウザ] → [管理対象ブラウザ] を順にクリックします。管理対象ブラウザが表示されます。

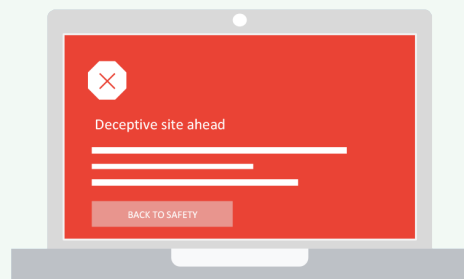
セーフブラウジング

セーフブラウジングでは、不正なソフトウェア、危険な拡張機能、フィッシング、Google のリストに登録された安全でない可能性のあるサイトについて警告を表示します。

セーフブラウジングを使用することで、次のようなサイトから、ユーザーのデバイスにマルウェアが感染することを防ぎ、また情報漏えいのリスクから守ることができます。

- マルウェアなどの不正なソフトウェアをインストールさせようとするサイト
- 正規のサイトになりすまし、ユーザーの ID やパスワードを不正に入力させるフィッシング サイト

本ドキュメントのポリシーを設定することで、ユーザーは警告を無視して危険なサイトにアクセスすることができなくなります。

セーフブラウジングの有効化
「SafeBrowsingProtectionLevel」

セーフブラウジング保護レベル

管理コンソールでの設定

セーフブラウジングを使用することで、ユーザーのデバイスにマルウェアが感染することを防ぎ、情報漏えいのリスクから守ることができます。

- ① 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- ② [ユーザーとブラウザ] をクリックします。
- ③ [フィルタを追加、または検索] に “SafeBrowsingProtectionLevel” と入力し、[セーフブラウジング保護レベル] をクリックします。

Chrome のセーフブラウジング			
設定	設定	継承	サポート対象
セーフブラウジング保護レベル	ユーザーによる決定を許可	Google のデフォルト	

セーフブラウジング保護レベル	ユーザーに対して Google セーフブラウジング を有効にするかどうかマルウェアやフィッシング コンテンツを含む可能性のあるウェブサイトに [セーフブラウジングを強化モードで有効にする] を選択した場合、セーフブラウジングを強化モードで有効にする。このモードではセキュリティが強化されますが、より多くの閲覧情報を Google に提供する必要があります
組織部門	デフォルトでは [ユーザーによる決定を許可] が選択されており、セーフブラウジングを強化モードで有効にする。このモードではセキュリティが強化されますが、より多くの閲覧情報を Google に提供する必要があります
組織部門を検索	
▼ cbcmtest.com	
▶ 01 Region	
▶ 02 Group Company	
▶ 11 Policy Precedence Test	
▶ 12 Customer Engineering Test	
▶ extension-test	
Chromium 名	サポート対象
SafeBrowsingProtectionLevel	Chrome (Windows、Mac、Linux) バージョン 83 以降 ChromeOS バージョン 83 以降 Chrome (Android) バージョン 87 以降 Chrome (iOS) バージョン 88 以降
継承	Google のデフォルトに設定
設定	ユーザーによる決定を許可

セーフブラウジングの有効化
「SafeBrowsingProtectionLevel」

セーフブラウジング保護レベル

管理コンソールでの設定

セーフブラウジングを有効にして、
危険なサイトへのアクセスを禁止する (2)

セーフブラウジングを使用することで、ユーザーのデバイスにマルウェアが感染することを防ぎ、情報漏えいのリスクから守ることができます。

- ④ [セーフブラウジングを標準モードで有効にする] もしくは [セーフブラウジングを強化モードで有効にする] を選択し、[保存] をクリックします。
- ⑤ 保存した内容を確認します。

ユーザーに対して [Google セーフブラウジング](#) を有効にするかどうかを指定します。Chrome のセーフブラウジングは、マルウェアやフィッシング コンテンツを含む可能性のあるウェブサイトからユーザーを保護するのに役立ちます。

[セーフブラウジングを強化モードで有効にする] を選択した場合、セキュリティは強化されますが、より多くの閲覧情報を Google に提供する必要があります。

デフォルトでは [ユーザーによる決定を許可] が選択されており、セーフブラウジングのオン/オフをユーザー自身で切り替えることができます。管理者がセーフブラウジングを有効にした場合、ユーザーが Google Chrome で設定を変更したりオーバーライドしたりすることはできません。

Chromium 名	サポート対象
SafeBrowsingProtectionLevel	Chrome (Windows、Mac、Linux) バージョン 83 以降 ChromeOS バージョン 83 以降 Chrome (Android) バージョン 87 以降 Chrome (iOS) バージョン 88 以降

継承	Google のデフォルトに設定
----	------------------

設定	ユーザーによる決定を許可
	セーフブラウジングを常に無効にする
	セーフブラウジングを標準モードで有効にする
	セーフブラウジングを強化モードで有効にする。このモードではセキュリティが強化されますが、より多くの閲覧情報を Google に提供する必要があります

デバイスでの検証

セーフブラウジングを有効にして、
危険なサイトへのアクセスを禁止する

危険なサイトにアクセスするとメッセージが表示されることを確認します。

- ① 危険なサイトにアクセスすると、警告が表示されます。

参考画像
不正なソフトウェアをインストールさせるサイトにアクセスしたときの例



セーフ ブラウジングの強制 「DisableSafeBrowsingProceedAnyway」

セーフブラウジングの警告の無視を無効にする

管理コンソールでの設定

セーフブラウジングを使用することで、ユーザーのデバイスにマルウェアが感染することを防ぎ、情報漏えいのリスクから守ることができます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 [フィルタを追加、または検索] に “DisableSafeBrowsingProceedAnyway” と入力し、[セーフブラウジングの警告の無視を無効にする] をクリックします。
- 3 [セーフブラウジングの警告の無視をユーザーに許可しない] を選択し、[保存] をクリックします。
- 4 保存した内容を確認します。

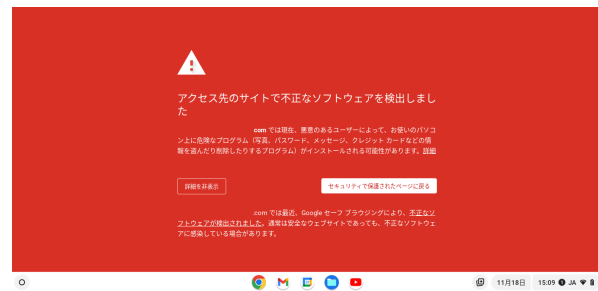


デバイスでの検証

危険なサイトにアクセスするとメッセージが表示され、警告を無視してアクセスできないことを確認します。

- ① 危険なサイトにアクセスすると、警告が表示されます。
- ② [セキュリティで保護されたページに戻る] をクリックして、警告を無視してサイトへアクセスできないことを確認します。

参考画像
不正なソフトウェアをインストールさせるサイトに
アクセスしたときの例



特定ドメインの保護、セーフブラウジングの制御 「SafeBrowsingAllowlistDomains」

セーフブラウジングが許可されているドメイン

管理コンソールでの設定

指定したドメイン（社内ドメインなど）はセーフブラウジングから信頼され、危険なリソース（フィッシング、不正なソフトウェア、迷惑ソフトウェアなど）の確認は行われません。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択し、そのままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “SafeBrowsingAllowlistDomains” と入力し、[セーフ ブラウジングが許可されているドメイン] をクリックします。
- 4 許可するドメインを入力します。
- 5 編集した内容を保存し、設定は完了です。

デバイスでの検証

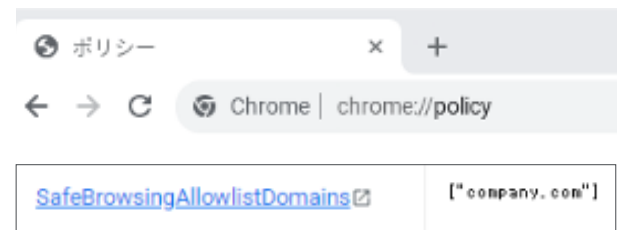
エンドユーザーのブラウザ上での「SafeBrowsingAllowlist Domains」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “SafeBrowsingAllowlistDomains” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

信頼される特定のドメインに対する セーフブラウジングの警告を無効化



「SafeBrowsingAllowlistDomains」を ブラウザ上で確認する



ダウンロードの徹底管理 「DownloadRestrictions」

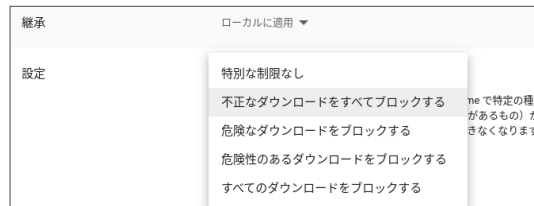
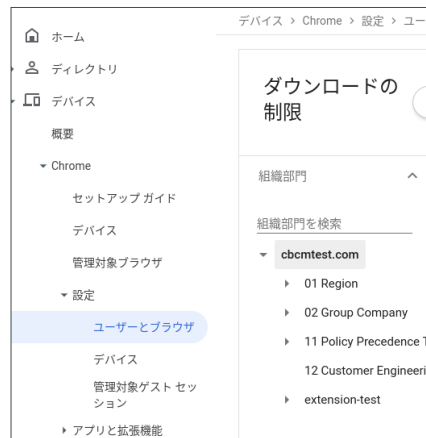
ダウンロードの制限

管理コンソールでの設定

管理対象ブラウザでのダウンロードを制限

ユーザーがマルウェアや感染ファイルなどの危険なファイルをダウンロードできないようにします。

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- [フィルタを追加、または検索] に “ Download ” と入力し、[ダウンロードの制限] をクリックします。
- ダウンロードの制限レベルを設定します。
- 編集した内容を保存し、設定は完了です。

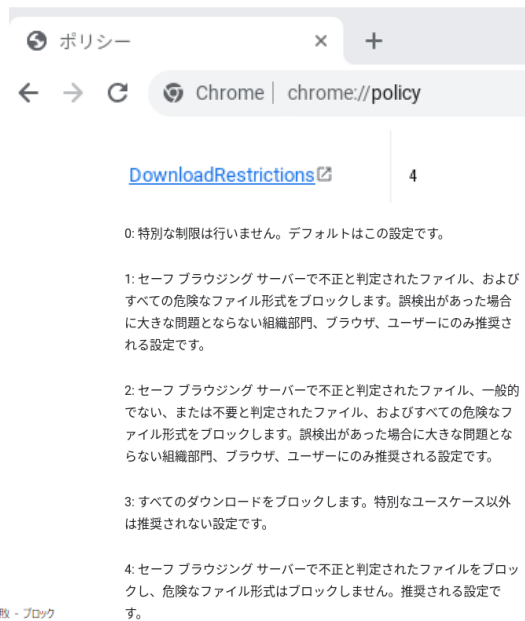


デバイスでの検証

「DownloadRestrictions」をブラウザ上で確認する

エンドユーザーのブラウザ上での「DownloadRestrictions」が動いているか確認します。

- 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- “ DownloadRestrictions ” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- この値が見つからない場合や期待した設定になっていない場合は、“ chrome://policy ” 画面の “ ポリシーを再読み込み ” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



特定のサイトのアクセスをブロック もしくは社内のポータルサイトのみアクセスを許可 「URLBlocklist」

URL のブロック

管理コンソールでの設定

許可されていない URL を設定し、特定のサイトのアクセスをブロック

特定の URL やパターンへのアクセスをブロックすることで、セキュリティリスクを低減し、企業ポリシーに基づいたインターネット利用を実現します。

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- [フィルタを追加、または検索] に “ URLBlock ” と入力し、[URL のブロック] をクリックします。

- [ブロックされる URL] に ブロックしたいサイトの URL を入力し、保存します。

URL の構文については、下記ヘルプ記事を参照ください。

- https://support.google.com/chrome/a/answer/2657289?hl=ja#url_blocklist&zippy=%2Curl-%E3%81%AE%E3%83%96%E3%83%AD%E3%83%83%E3%82%AF

- 保存した内容を確認して、設定は完了です。

設定	設定	継承	サポート対象
URL のブロック	2 件のサブ設定	Google のデフォルト	



特定のサイトのアクセスをブロック もしくは社内のポータル サイトのみアクセスを許可 「URLBlocklist」

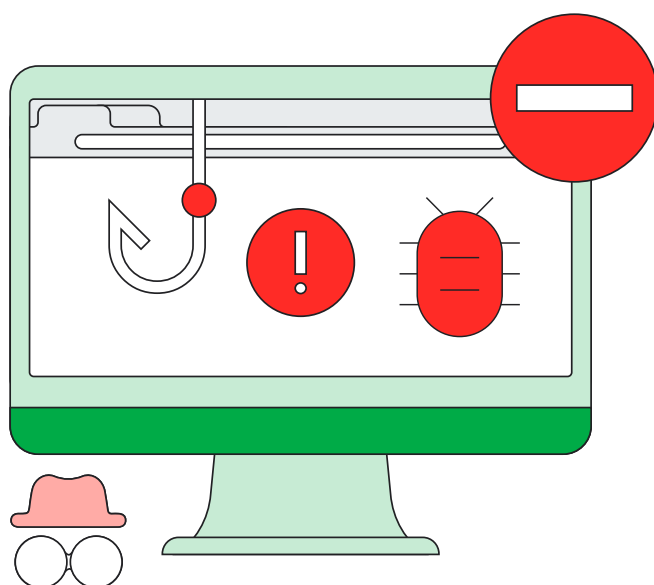
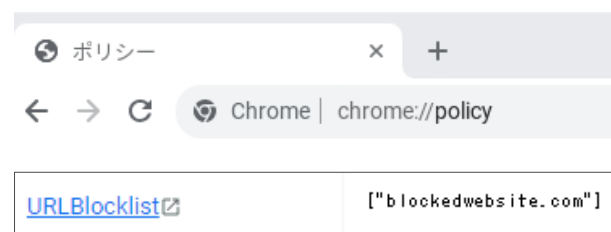
URL のブロック

デバイスでの検証

URL をブロックする

指定したサイト以外でブラウザ アクセスができないことを確認します。

- ① 管理された検証用ブラウザで“chrome://policy”へ移動します。
- ② “URLBlocklist”が設定した URL になっているか確認します。
- ③ この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“chrome://policy”画面の“ポリシーを再読み込み”を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



特定のサイトのアクセスをブロック もしくは社内のポータル サイトのみアクセスを許可 「URLBlocklist」

管理コンソールでの設定

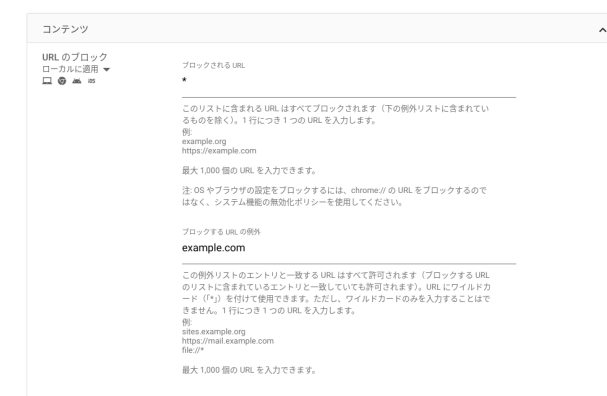
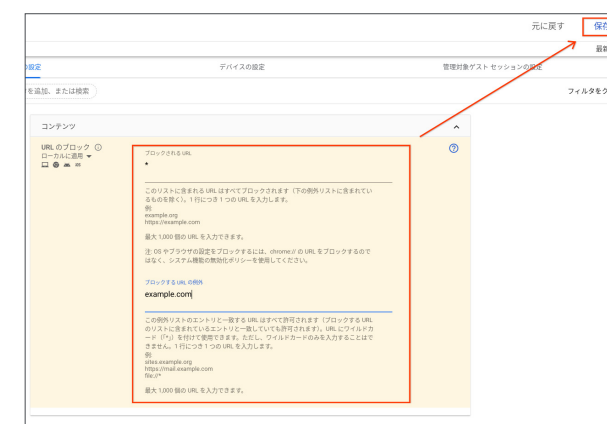
社内のポータル サイトのみアクセスを許可

社内のポータル サイトを除くすべての URL に対してブラウザ アクセスをブロックします。

- ④ [ブロックされる URL] に“*”を入力し、[ブロックする URL の例外] に“[組織のポータル サイトの URL]”を入力し、保存します。

URL の構文については、下記ヘルプ記事を参照ください。

- ⑤ 保存した内容を確認して、設定は完了です。



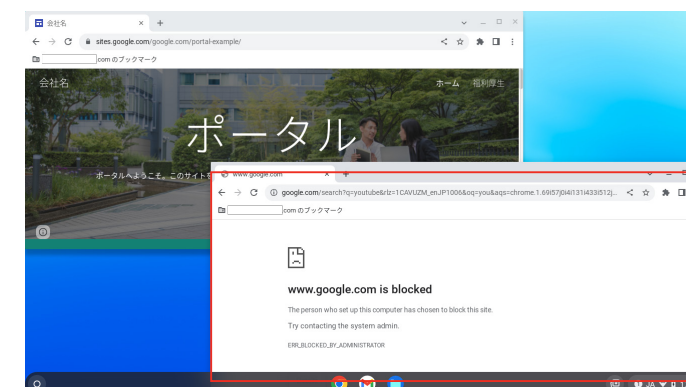
URL のブロック

デバイスでの検証

社内のポータル サイトのみアクセスを許可する (URL をブロックする)

指定したサイト以外でブラウザ アクセスができないことを確認します。

- ① 検証デバイスにログインし、社内のポータル サイトにアクセスします。
- ② ポータル サイトにはアクセスできますが、その他 URL がブロックされていることを確認します。



広告をコントロール、ビジネスに集中 「AdsSettingForIntrusiveAdsSites」

煩わしい広告を含むサイト

管理コンソールでの設定

煩わしい広告をブロックすることで、企業のセキュリティ ポリシーに従った快適なブラウジング環境を提供します。

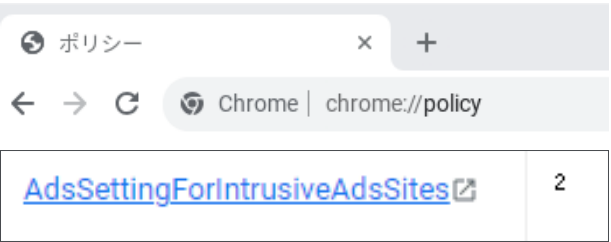
- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “AdsSettingForIntrusiveAdsSites” と入力し、 [煩わしい広告を含むサイト] をクリックします。
- 4 広告の表示設定を選択します。
- 5 編集した内容を保存し、設定は完了です。



デバイスでの検証

エンドユーザーのブラウザ上での「AdsSettingForIntrusiveAdsSites」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “AdsSettingForIntrusiveAdsSites” が設定した値になっているか確認します。
- 3 この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



必要なポップアップだけを許可 またはポップアップをブロック 「DefaultPopupsSetting」

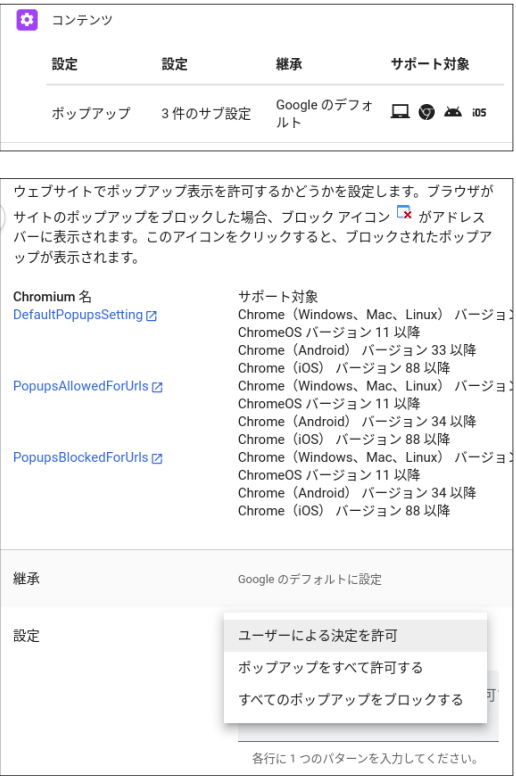
ポップアップ

管理コンソールでの設定

特定の URL に対してポップアップを許可

必要な情報のみをポップアップで表示させることで、ユーザー体験を向上させます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “DefaultPopupsSetting” と入力し、 [ポップアップ] をクリックします。
- 4 ポップアップの許可レベルを設定します。必要であれば選択ボックス下の許可リスト、もしくはブロックリストに URL を入力します。
- 5 編集した内容を保存し、設定は完了です。

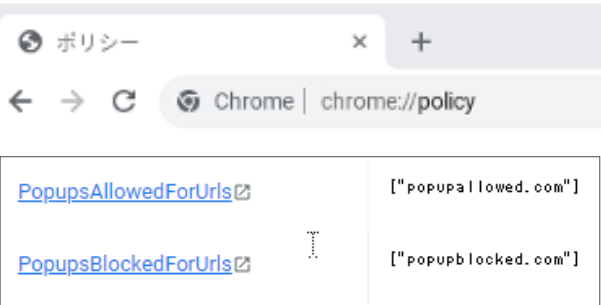


デバイスでの検証

「DefaultPopupsSetting」をブラウザ上で確認する

エンドユーザーのブラウザ上での「DefaultPopupsSetting」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “PopupsAllowedForUrls” もしくは “PopupsBlockedForUrls” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



シークレット モードの無効化で、全てを明確に「IncognitoModeAvailability」

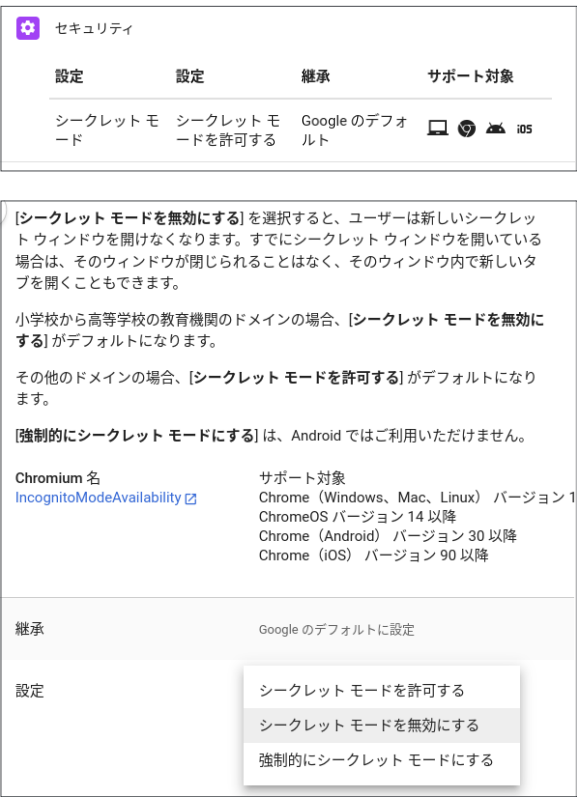
シークレット モード

管理コンソールでの設定

ユーザーのシークレット モード利用を設定

シークレット モードを無効化することで、全てのブラウザ上の動きを可視化し、企業の情報共有とセキュリティを確保します。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “IncognitoModeAvailability” と入力し、[シークレット モード] をクリックします。
- 4 [シークレット モードを無効にする] を選択します。
- 5 編集した内容を保存し、設定は完了です。

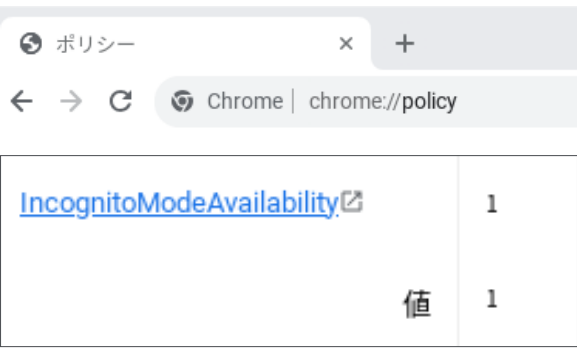


デバイスでの検証

「IncognitoModeAvailability」をブラウザ上で確認する

エンドユーザーのブラウザ上での「IncognitoModeAvailability」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “IncognitoModeAvailability” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



パスワードは自動で管理、安全性と利便性の両立「PasswordManagerEnabled」

パスワード マネージャー

管理コンソールでの設定

ブラウザのパスワード マネージャーを有効化

パスワード マネージャーを有効にすることで、ユーザーのパスワード管理を自動化し、セキュリティを強化しながら利便性を向上させます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “PasswordManagerEnabled” と入力し、[パスワード マネージャー] をクリックします。
- 4 パスワード マネージャーの使用を設定します。
- 5 編集した内容を保存し、設定は完了です。

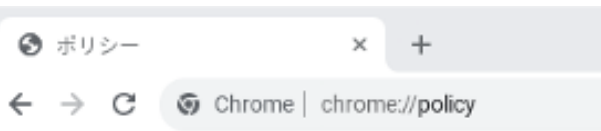


デバイスでの検証

「PasswordManagerEnabled」をブラウザ上で確認する

エンドユーザーのブラウザ上での「PasswordManagerEnabled」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “PasswordManagerEnabled” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



不正利用を未然に防ぐ、パスワード警告システム！ 「PasswordProtectionWarningTrigger」

パスワード アラート

管理コンソールでの設定

許可されていないサイトでの パスワードの再利用を警告する (1)

許可していないサイトでユーザーがパスワードを入力した場合、パスワードを再利用しないように警告することができます。

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- [フィルタを追加、または検索] に “PasswordProtection” と入力し、[パスワード アラート] をクリックします。

- [パスワードが再利用された場合に表示する] を選択し、保存します。

デフォルトは [フィッシング ページでパスワードが再利用されたときに表示する] のため、正規のサイトになりすまし、ユーザーの ID やパスワードを不正に入力させるような危険なサイトでパスワードを入力されたときに警告を表示します。

- 保存した内容を確認して設定は完了です。

Chrome のセーフ ブラウジング			
設定	設定	継承	サポート対象
パスワード アラート	3 件のサブ設定	Google のデフォルト	  

危険なウェブサイト、または組織の許可リストに登録されていないウェブサイトで、ユーザーのパスワードの再利用を禁止することができます。複数のウェブサイトでのパスワードの再利用を禁止することで、組織のアカウントを不正使用から保護できます。

セーフ ブラウジング リストに記載されている URL の例外とするドメインを指定します。許可リストに登録されているドメインについては、以下の確認が行われません。

- パスワードの再利用
- フィッシング サイトや不正なソーシャルエンジニアリング サイト
- マルウェアや不正なソフトウェアをホストするサイト
- 有害なダウンロード

ユーザーが通常はパスワードを入力してアカウントにログインするウェブページの URL を指定します。ログイン プロセスが 2 ページに分割されている場合は、ユーザーがパスワードを入力するウェブページの URL を追加します。ユーザーがパスワードを入力すると、復元不可能なハッシュがローカルに保存され、パスワードの再利用の検出に使用されます。パスワード変更 URL を指定する際は、URL が [ガイドライン](#) に準拠していることをご確認ください。

Chromium 名	サポート対象
PasswordProtectionChangePass...	Chrome (Windows, Mac, Linux) バージョン 69 以降
PasswordProtectionLoginURLs	ChromeOS バージョン 69 以降
PasswordProtectionWarningTrigg...	Chrome (Windows, Mac, Linux) バージョン 69 以降
	ChromeOS バージョン 69 以降

継承

Google のデフォルトに設定

パスワード保護の警告を無効にする

パスワードが再利用された場合に表示する

フィッシング ページでパスワードが再利用されたときに表示する

パスワードの保護に関する警告の表示を制御します。 [パスワードの保護に関する詳細](#) をご覧ください。

パスワードの変更 URL

ユーザーが自分のパスワードを変更できるウェブページの URL を入力します。

ログイン URL

パスワード保護サービスで指紋によるパスワード認証を行う、企業のログイン URL のリストを入力します。1 行につき 1 つの項目を入力してください。

不正利用を未然に防ぐ、パスワード警告システム！ 「PasswordProtectionWarningTrigger」

パスワード アラート

管理コンソールでの設定

許可されていないサイトでの パスワードの再利用を警告する (2)

許可していないサイトでユーザーがパスワードを入力した場合、パスワードを再利用しないように警告することができます。

- 管理コンソールのホームページからデバイスをクリックします。
- 左側の [Chrome] をクリックします。
- [設定] 次に [ユーザーとブラウザ] をクリックします。
- [フィルタを追加、または検索] に “セーフ ブラウジングが許可されているドメイン” と入力し、[設定 含む: “セーフ ブラウジングが許可されているドメイン”] をクリックします。
- [許可するドメイン] に任意のドメイン (会社ドメインなど) を入力し、保存します。
- 保存した内容を確認して設定は完了です。



不正利用を未然に防ぐ、パスワード警告システム！ 「PasswordProtectionWarningTrigger」

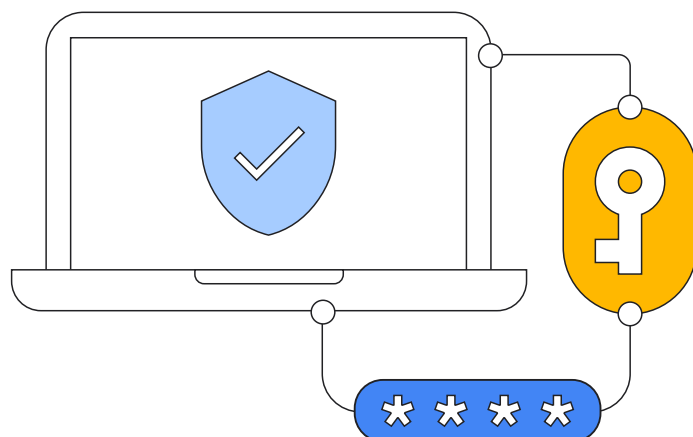
パスワード アラート

デバイスでの検証

許可されていないサイトでのパスワードの再利用を警告する

許可していないサイトでパスワードを入力した際、パスワードの再利用をしないよう警告されることを確認します。

- ① 検証用デバイスで、指定したサイト以外で検証用アカウントのパスワードを入力します。
- ② メッセージが表示され、パスワードの再利用をしないよう警告されることを確認します。



パスワード変更の URL を指定 「PasswordProtectionChange PasswordURL」

パスワード アラート

管理コンソールでの設定

企業のセキュリティ ポリシーに合わせたパスワード変更
ページへのリダイレクトで、データ保護を強化

ブラウザで警告が表示された後にユーザーがパスワードを変更するための URL を設定できます。不正利用が疑われる場合、ユーザーは企業指定の URL にリダイレクトされ、パスワードの変更が促されます。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] に “PasswordProtection” と入力し、[パスワード アラート] をクリックします。
- ④ [パスワードの変更に使用する URL] の欄に URL を入力します。
- ⑤ 編集した内容を保存し、設定は完了です。

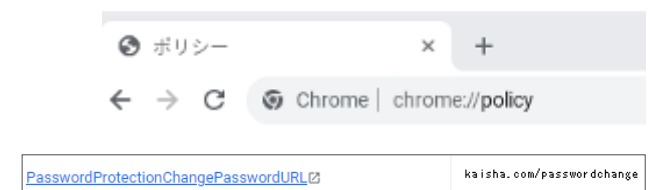


デバイスでの検証

「PasswordProtectionChangePasswordURL」を
ブラウザ上で確認する

エンドユーザーのブラウザ上での「PasswordProtectionChangePasswordURL」が動いているか確認します。

- ① 管理された検証用ブラウザで “chrome://policy” へ移動します。
- ② “PasswordProtectionChangePasswordURL” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- ③ この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



企業のログインページの保護を強化 「PasswordProtectionLoginURLs」

パスワード アラート

管理コンソールでの設定

企業のログインページの保護を強化し、
不正利用を未然に防ぐ

ブラウザで警告が表示された後にユーザーがパスワードを変更するための URL を設定できます。不正利用が疑われる場合、ユーザーは企業指定の URL にリダイレクトされ、パスワードの変更が促されます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “PasswordProtection” と入力し、[パスワード アラート] をクリックします。
- 4 [ログイン URL] の欄に社内アプリケーションへのログイン URL を入力します。
- 5 編集した内容を保存し、設定は完了です。

設定	設定	継承	サポート対象
パスワード アラート	3 件のサブ設定	Google のデフォルト	  

危険なウェブサイト、または組織の許可リストに登録されていないウェブサイトで、ユーザーのパスワードの再利用を禁止するかどうかを指定します。複数のウェブサイトでのパスワードの再利用を禁止することで、組織のアカウントを不正使用から保護できます。

セーフ ブラウジング リストに記載されている URL の例外とするドメインを指定します。許可リストに登録されているドメインについては、以下の確認が行われません。

- パスワードの再利用
- フィッシング サイトや不正なソーシャル エンジニアリング サイト
- マルウェアや不正なソフトウェアをホストするサイト
- 有害なダウンロード

ユーザーが通常はパスワードを入力してアカウントにログインするウェブページの URL を指定します。ログイン プロセスが 2 ページに分割されている場合は、ユーザーがパスワードを入力するウェブページの URL を追加します。ユーザーがパスワードを入力すると、復元可能なハッシュがローカルに保存され、パスワードの再利用の検出に使用されます。パスワード変更 URL を指定する際は、URL が [ガイドライン](#) に準拠していることをご確認ください。

Chromium 名	サポート対象
PasswordProtectionChangePass...	Chrome (Windows, Mac, Linux) バージョン 69 以降
PasswordProtectionLoginURLs	Chrome (Windows, Mac, Linux) バージョン 69 以降
PasswordProtectionWarningTrigg...	Chrome (Windows, Mac, Linux) バージョン 69 以降

継承	Google のデフォルトに設定
設定	パスワード保護の警告を設定する フィッシング ページでパスワードが再利用されたときに表示する ▼ パスワードの保護に関する警告の表示を制御します。 パスワードの保護についての詳細 をご覧ください。 パスワードの変更に使用する URL ユーザーが自分のパスワードを変更できるウェブページの URL を入力します。 ログイン URL パスワード保護サービスで指紋によるパスワード認証を行う、企業のログイン URL のリストを入力します。1 行につき 1 つの項目を入力してください。

デバイスでの検証

「PasswordProtectionLoginURLs」を
ブラウザ上で確認する

エンドユーザーのブラウザ上での「PasswordProtection LoginURLs」が動いているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 “PasswordProtectionLoginURLs” が表示され、その設定が管理コンソール上で選択した制限レベルになっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

ポリシー	
PasswordProtectionLoginURLs	["kaisha.com/login"]

更新管理もお手の物 「Chrome ブラウザのバージョンの固定」

目的のバージョンのプレフィックス

管理コンソールでの設定

ブラウザのバージョンの固定

特定のバージョンのブラウザ環境を維持するため、特定のバージョン以降の Chrome の自動更新を防ぎます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “ブラウザの更新” と入力し、[Chrome ブラウザの更新] をクリックします。
- 4 [目的のバージョンのプレフィックス] に、適用する Chrome ブラウザのバージョン番号を入力します。

設定	設定	継承	サポート対象
ブラウザの更新	3 件のサブ設定	Google のデフォルト	  

危険なウェブサイト、または組織の許可リストに登録されていないウェブサイトで、ユーザーのパスワードの再利用を禁止するかどうかを指定します。複数のウェブサイトでのパスワードの再利用を禁止することで、組織のアカウントを不正使用から保護できます。

セーフ ブラウジング リストに記載されている URL の例外とするドメインを指定します。許可リストに登録されているドメインについては、以下の確認が行われません。

- パスワードの再利用
- フィッシング サイトや不正なソーシャル エンジニアリング サイト
- マルウェアや不正なソフトウェアをホストするサイト
- 有害なダウンロード

ユーザーが通常はパスワードを入力してアカウントにログインするウェブページの URL を指定します。ログイン プロセスが 2 ページに分割されている場合は、ユーザーがパスワードを入力するウェブページの URL を追加します。ユーザーがパスワードを入力すると、復元可能なハッシュがローカルに保存され、パスワードの再利用の検出に使用されます。パスワード変更 URL を指定する際は、URL が [ガイドライン](#) に準拠していることをご確認ください。

Chromium 名	サポート対象
PasswordProtectionChangePass...	Chrome (Windows, Mac, Linux) バージョン 69 以降
PasswordProtectionLoginURLs	Chrome (Windows, Mac, Linux) バージョン 69 以降
PasswordProtectionWarningTrigg...	Chrome (Windows, Mac, Linux) バージョン 69 以降

継承	Google のデフォルトに設定
設定	パスワード保護の警告を設定する フィッシング ページでパスワードが再利用されたときに表示する ▼ パスワードの保護に関する警告の表示を制御します。 パスワードの保護についての詳細 をご覧ください。 パスワードの変更に使用する URL ユーザーが自分のパスワードを変更できるウェブページの URL を入力します。 ログイン URL パスワード保護サービスで指紋によるパスワード認証を行う、企業のログイン URL のリストを入力します。1 行につき 1 つの項目を入力してください。

継承	ローカルに適用 ▼
設定	更新を無効にする ▼ 目的のバージョンのプレフィックス 114. どのバージョンの Chrome ブラウザに更新するかを指定します。値を設定すると、その値から始まるバージョンに Chrome が更新されます。たとえば、「55」と設定した場合、Chrome は 55 のマイナー バージョンのいずれか（例：55.24.34.0 または 55.60.2.10）に更新されます。「55.2」と設定すると、55.2 のマイナー バージョンのいずれか（例：55.2.34.100 または 55.2.2.1）に更新されます。「55.24.34.1」と設定すると、そのバージョンに更新されます。なお、指定したバージョンが直近の 3 つのメジャー バージョンより古い場合は、Chrome で更新が停止されたり、ロールバックされなかったりすることがあります。

管理コンソールでの設定

ブラウザのバージョンの固定 &
目的のバージョンにロールバック

特定のバージョンのブラウザ環境を維持するため、特定のバージョン以降の Chrome の自動更新を防ぎます。

- 5 最大 4 つの部分で構成されるバージョン番号（116.0.3987.162 など）を使用できます。
- 6 正確なバージョンを指定しない場合は、バージョン番号の後にピリオド（.）を付けます。ピリオドで指定したバージョンを使用する場合、その番号の最新のバージョンに更新が固定されます。（例：116.）
- 7 編集した内容を保存し、設定は完了です。
- 8 また、以前のバージョンにロールバックが必要という場合は、[更新を無効にする] を選択後、[目的のバージョン プレフィックス] でバージョンを指定し、[目的のバージョンにロールバック] を選択し、保存します。指定したバージョンが直近の 3 つのメジャー バージョンより古い場合は、ロールバックされない可能性があるのをご確認ください。

継承	ローカルに適用 ▼
設定	更新を無効にする ▼ 目的のバージョンのプレフィックス 114. どのバージョンの Chrome ブラウザに更新するかを指定します。値を設定すると、その値から始まるバージョンに Chrome が更新されます。たとえば、「55」と設定した場合、Chrome は 55 のマイナー バージョンのいずれか（例：55.24.34.0 または 55.60.2.10）に更新されます。「55.2」と設定すると、55.2 のマイナー バージョンのいずれか（例：55.2.34.100 または 55.2.2.1）に更新されます。「55.24.34.1」と設定すると、そのバージョンに更新されます。なお、指定したバージョンが直近の 3 つのメジャー バージョンより古い場合は、Chrome で更新が停止されたり、ロールバックされなかったりすることがあります。 Dev チャンネル ▼ 対象バージョンにロールバックしない ▼

対象バージョンにロールバックしない
目的のバージョンにロールバック

更新管理もお手の物 「Chrome ブラウザのバージョンの固定」

目的のバージョンのプレフィックス

デバイスでの検証

バージョンが固定されているかブラウザ上で確認する

エンドユーザーのブラウザ上でのバージョン制御が動いているか確認します。

- ① 管理された検証用ブラウザで “chrome://version” へ移動します。
- ② [Google Chrome:] の欄が指定したバージョンになっていることを確認します。

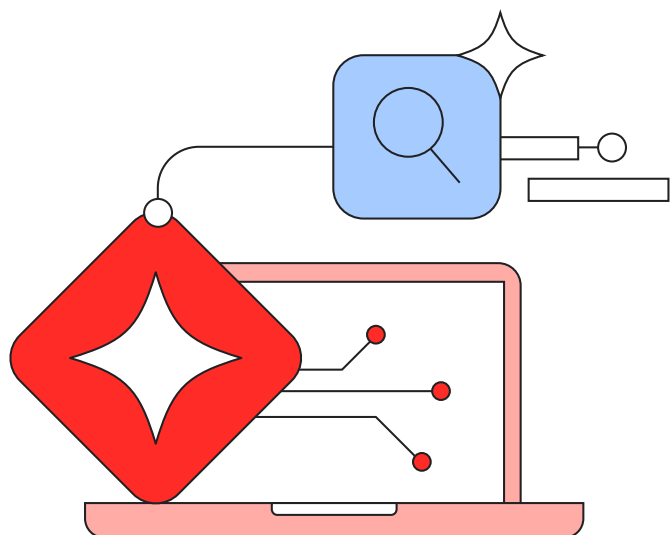
もしくは

- ① 管理された検証用ブラウザで “chrome://policy” へ移動します。
- ② “Google Update Policies” 下の “TargetVersionPrefix” が指定したバージョンになっていることを確認します。

Google Chrome: 114.0.5735.239 (Official Build) (64 ビット)

Google Update Policies

ポリシー名	ポリシーの値
RollbackToTargetVersion	false
TargetChannel	stable
TargetVersionPrefix	114.
UpdatePolicy	3



ブラウザの更新は計画的に自動化 「AutoUpdateCheckPeriodMinutes」

自動更新のチェックを停止する & 自動更新のチェック間隔

管理コンソールでの設定

ブラウザの更新チェックの間隔を設定 ①

自動更新のチェック間隔を 分単位 で設定できます。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] で カテゴリ を選択し、“Chrome の更新” と入力し、[自動更新チェックの間隔] をクリックします。更新チェックの間隔を設定します（“0” と設定すると自動更新チェックを停止します）。
- ④ 編集した内容を保存し、設定は完了です。

自動更新のチェック間隔 Google のデフォルトに設定	自動更新チェック間隔 (分) 自動更新のチェックをすべて無効にするには、 デバッグ 値を 0 に設定してください。空欄にすると、デフォルトの 295 分となります。
---------------------------------	--

管理コンソールでの設定

ブラウザの更新チェックの間隔を設定 ②

業務時間外に更新を設定し、ブラウザ更新による業務への影響を抑えます。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] で カテゴリ を選択し、“Chrome の更新” と入力し、[自動更新のチェックを停止する] をクリックします。
- ④ 開始時間のボックスにブラウザ更新のチェックを停止する時間帯の開始時刻を 24 時間形式 (hh:mm) で入力します。（例：09:00）
- ⑤ 次に、ブラウザの更新チェックを停止する時間を分単位で入力します。（例：180 - この設定では業務開始時間の 9 時からランチタイムの 12 時までには更新を行わないように設定されています。）
- ⑥ 最後に [保存] をクリックして設定を保存します。

自動更新のチェックを停止する

Chrome ブラウザの更新の自動チェックを行わない時間帯（毎日）を指定します。次のように入力します。

- 開始時間 - ブラウザ更新のチェックを停止する時間帯（毎日）の開始時刻（24 時間形式 (hh:mm)）
- 期間 (分) - ブラウザの更新チェックを停止する時間の長さ（分単位）

継承	Google のデフォルトに設定				
設定	<table><tr><td>開始時間</td></tr><tr><td>自動更新のチェック停止の開始時刻（24 時間形式（hh:mm））。</td></tr><tr><td>期間（分） 0</td></tr><tr><td>自動更新のチェックを、上で指定した開始時刻から、ここで指定した期間（分）だけ停止します。この期間では夏時間が考慮されません。</td></tr></table>	開始時間	自動更新のチェック停止の開始時刻（24 時間形式（hh:mm））。	期間（分） 0	自動更新のチェックを、上で指定した開始時刻から、ここで指定した期間（分）だけ停止します。この期間では夏時間が考慮されません。
開始時間					
自動更新のチェック停止の開始時刻（24 時間形式（hh:mm））。					
期間（分） 0					
自動更新のチェックを、上で指定した開始時刻から、ここで指定した期間（分）だけ停止します。この期間では夏時間が考慮されません。					

ブラウザの更新は計画的に自動化 「AutoUpdateCheckPeriodMinutes」

自動更新のチェックを停止する & 自動更新のチェック間隔

デバイスでの検証

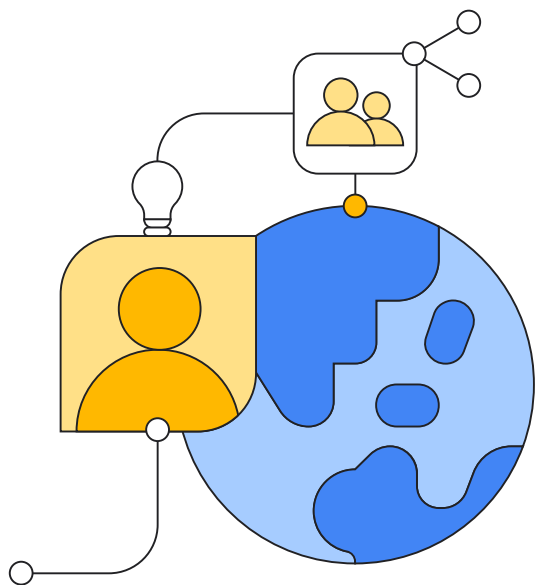
アップデート設定が指定された状態になっているか確認する

エンドユーザーのブラウザ上でのバージョン制御が動いているか確認します。

- ① 管理された検証用ブラウザで“chrome://policy”へ移動します。
- ② [Google Update Policies] 下の [UpdatesSuppressedStartHour] (時) [UpdateSuppressedStartMinute] (分) が指定した時間になっていることを確認します。
- ③ 同じく [UpdatesSuppressedDurationMin] が自動更新の停止 (分) で指定した値になっているか確認します。

Google Update Policies

ポリシー名	ポリシーの値
RollbackToTargetVersion	false
TargetChannel	stable
TargetVersionPrefix	114.
UpdatePolicy	3
UpdatesSuppressedDurationMin	720
UpdatesSuppressedStartHour	9
UpdatesSuppressedStartMinute	0



再起動を通知、アップデートのスムーズな実施 「RelaunchNotification」

再起動通知

管理コンソールでの設定

ブラウザの最新状態を保ち、セキュリティを強化

保留中のアップデートの適用に再起動が必要であることをユーザーに通知します。再起動が「推奨」か「必須」かを設定し、必要に応じて自動的に再起動する警告を表示します。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] に“RelaunchNotification”と入力し、[再起動通知] をクリックします。
- ④ [再起動を推奨する通知を表示] または [一定期間が経過したら自動的に再起動する] を選択します。
- ⑤ [期間] では再起動が必要であることをユーザーに通知する期間を 1 ～ 168 時間 (最大 7 日間) で設定します。
- ⑥ [初期通知保留時間] では ChromeOS デバイスに対して、最初の再起動通知を表示するまでの保留時間を指定します。
- ⑦ [再起動する時間帯の開始時刻] では更新の適用に伴う自動再起動が始まる時間を 24 時間形式で指定します。
- ⑧ [再起動する時間帯の長さ] では Chrome ブラウザと ChromeOS デバイスが再起動し、更新を適用する時間枠の長さを分単位で設定します。
- ⑨ 編集した内容を保存し、設定は完了です。



再起動を通知、アップデートのスムーズな実施 「RelaunchNotification」

再起動通知

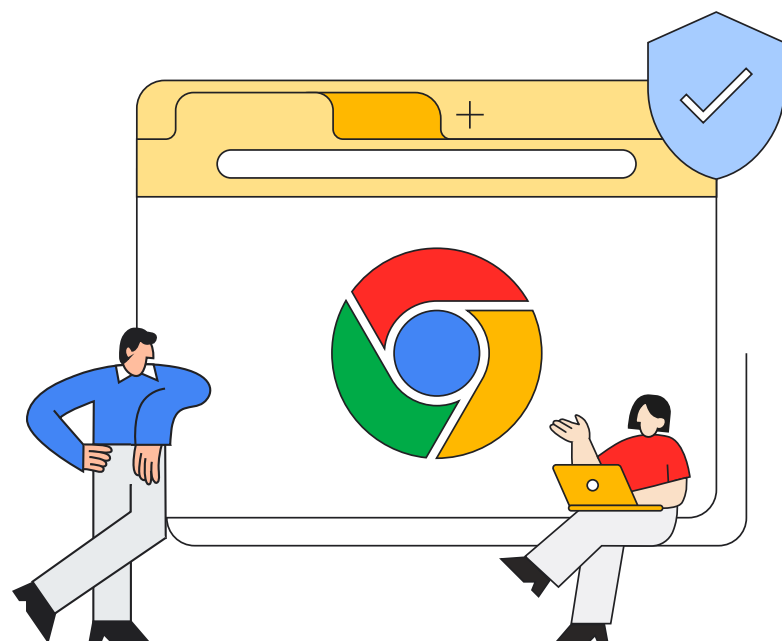
デバイスでの検証

再起動の通知設定が指定された状態になっているか確認する

エンドユーザーのブラウザ上での再起動通知設定が適用されているか確認します。

- 1 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 2 [RelaunchHeadsUpPeriod] [RelaunchNotification]
[RelaunchNotificationPeriod] が指定した設定になっていることを確認します。

RelaunchHeadsUpPeriod	583200000
RelaunchNotification	2
RelaunchNotificationPeriod	605000000



帯域幅の削減、アップデートの効率化 「Cacheable URLs」

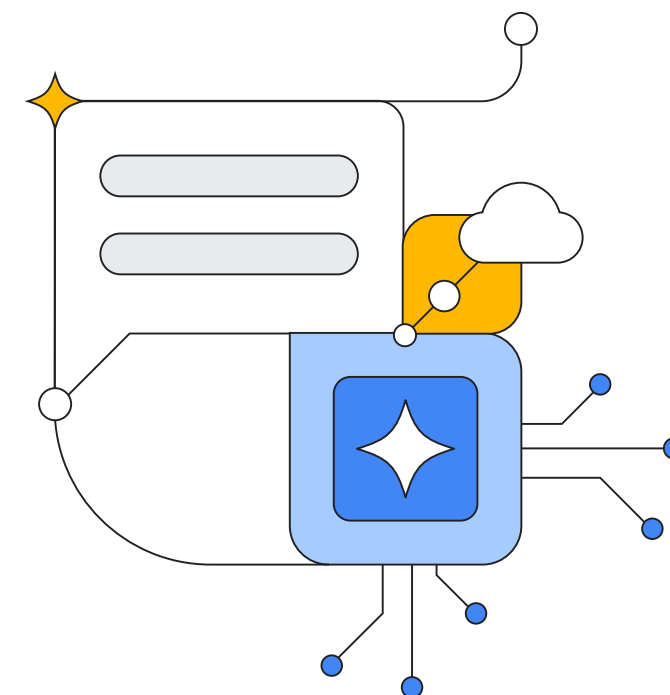
キャッシュに保存可能な URL

管理コンソールでの設定

Chrome ブラウザの更新をキャッシュする

組織のネットワークに中間プロキシ キャッシュが設定されている場合、Chrome の更新をキャッシュに保存することができます。効果的に帯域幅を削減し、応答時間を改善します。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “キャッシュ” と入力し、[キャッシュに保存可能な URL] をクリックします。
- 4 [指定しない] または [キャッシュ フレンドリーのダウンロード用 URL の提供を試みます] を選択します。
- 5 編集した内容を保存し、設定は完了です。



徹底的な拡張機能の管理 「ExtensionInstallAllowlist」& 「ExtensionInstallForcelist」& 「ExtensionInstallBlocklist」

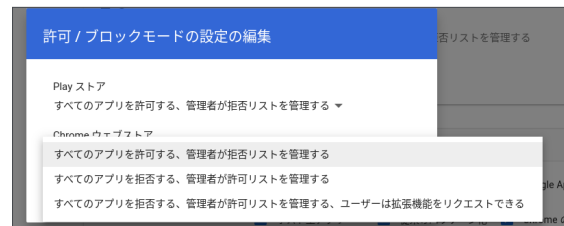
拡張機能のホワイトリスト、強制インストール、ブラックリスト

管理コンソールでの設定

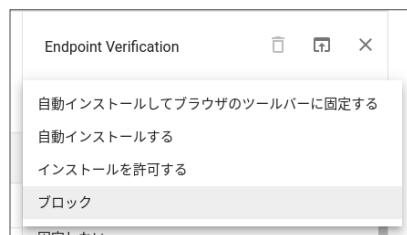
許可または、ブロックする拡張機能を指定 ①

ブラウザのセキュリティと拡張機能を管理者がコントロール

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択します。それ以外の場合は、子の組織単位を選択します。
- [許可 / ブロックモード] 内の編集をクリックします。
- ドロップダウン内から使用する設定を選択します。



- 先程の [Chrome ブラウザ] → [設定] → [アプリと拡張機能] → [ユーザーとブラウザ] で組織部門を選択した画面へ戻り、右下の黄色い + マークを押し、拡張機能を検索、管理コンソールに追加します。
- 先程追加した拡張機能をクリックし、右側から出てくるバーにて、「自動インストール」、「インストールを許可する」、「ブロック」などのオプションを選択します。
- 編集した内容を保存し、設定は完了です。



徹底的な拡張機能の管理 「ExtensionInstallAllowlist」& 「ExtensionInstallForcelist」& 「ExtensionInstallBlocklist」

拡張機能のホワイトリスト、強制インストール、ブラックリスト

管理コンソールでの設定

許可または、ブロックする拡張機能を指定 ②

ブラウザのセキュリティと機能を管理者がコントロール

Tips:

[Chrome ブラウザ] → [レポート] → [アプリと拡張機能の使用状況] をクリックし、アプリや拡張機能が組織全体でどれだけ使用されているのか一元で管理可能です。

特定の拡張機能やアプリの詳細を見るためには、アプリ名をクリックしましょう。アプリの詳細内に [リスクの評価] という項目が存在します。こちらはサードパーティが Chrome 拡張機能の安全性などを算出した値です。これらは管理者がどの Chrome 拡張機能を追加し、どれをブロックするのかなど判断する基準となります。

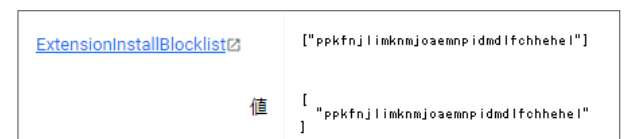


デバイスでの検証

拡張機能のポリシーをブラウザ上で確認する

エンドユーザーのブラウザ上での「ExtensionInstallAllowlist」、「ExtensionInstallForcelist」または「ExtensionInstallBlocklist」が動いているか確認します。

- 管理された検証用ブラウザで “chrome://policy” へ移動します。
- 「ExtensionInstallAllowlist」、「ExtensionInstallForcelist」または「ExtensionInstallBlocklist」が表示され、その設定が管理コンソール上で選択した拡張機能の ID リストになっていれば、適切にポリシーが反映されています。
- この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



外部拡張機能のインストールをブロック「BlockExternalExtensions」

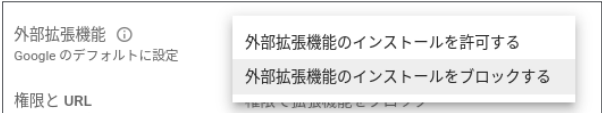
外部拡張機能

管理コンソールでの設定

不要な外部拡張機能のインストールを防ぎ、企業のニーズに応じて拡張機能を管理

外部拡張機能のインストールがブロックされます。企業のセキュリティポリシーに応じて、必要な拡張機能のみを許可し、不要なものを排除することが可能です。

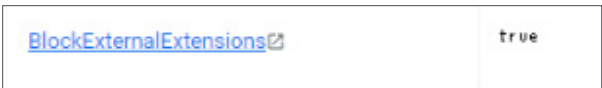
- 1 管理コンソールのホームページで [Chrome ブラウザ] → [アプリと拡張機能] → [追加の設定] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択します。それ以外の場合は、子の組織単位を選択します。
- 3 [外部拡張機能] の右のドロップダウンをクリックします。
- 4 ドロップダウン内から使用する設定を選択します。
- 5 編集した内容を保存し、設定は完了です。



デバイスでの検証

外部拡張機能のポリシーをブラウザ上で確認する

エンドユーザーのブラウザ上での「BlockExternalExtensions」が動いているか確認します。



- 1 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- 2 「BlockExternalExtensions」が表示され、その設定が管理コンソール上で選択した値になっていれば、適切にポリシーが反映されています。
- 3 この値が見つからない場合や期待した設定になっていない場合は、“chrome://policy”画面の“ポリシーを再読み込み”を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

ワンクリックでホームへ、作業の効率化！「ShowHomeButton」

ホームボタン

管理コンソールでの設定

ブラウザのツールバーにホームボタンを表示

ホームボタンを表示することで、ユーザーはワンクリックで直ちにホームページにアクセスでき、ブラウジング体験を向上させます。

- 1 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 2 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択します。それ以外の場合は、子の組織単位を選択します。
- 3 [フィルタを追加、または検索] に “ ShowHomeButton ” と入力し、[ホームボタン] をクリックします。
- 4 必要に応じて設定を有効にします。
- 5 編集した内容を保存し、設定は完了です。

ツールバーにホームボタンを表示するかどうかを指定します。このポリシーは、Chrome の [設定] で行うユーザー設定 ([ホームボタンを表示する]) に相当します。

Chromium 名 ShowHomeButton	サポート対象 Chrome (Windows、Mac、Linux) バージョン 110 ChromeOS バージョン 111 以降
継承	Google のデフォルトに設定
設定	ユーザーによる決定を許可 ホームボタンを常に表示 ホームボタンを表示しない

デバイスでの検証

ホームボタンが表示されているか確認

エンドユーザーの管理対象ブラウザでホームボタンが表示されているか確認



- 1 管理された検証用ブラウザを開き、リロードボタンの右にホームボタンが表示されているか確認します。

もしくは

- 1 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- 2 「ShowHomeButton」が [true] になっているか確認します。
- 3 この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“chrome://policy”画面の“ポリシーを再読み込み”を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

ホームは社内ページから、効率化の極！ 「HomepageLocation」

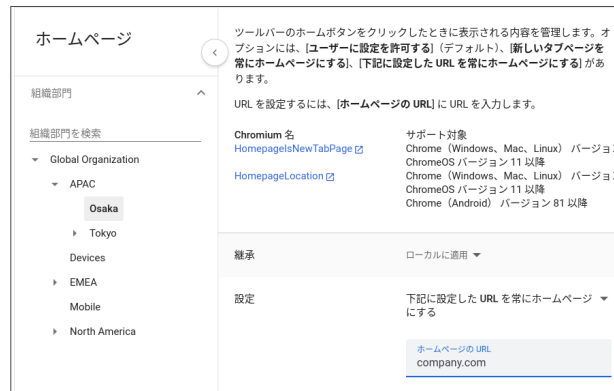
ホームページ

管理コンソールでの設定

開かれるデフォルトのホームページ URL を指定

社内ポータルや重要なウェブページを全員のホームページに設定することで、情報共有を円滑にし、作業効率を向上させます。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] に “ HomepageLocation ” と入力し、[ホームページ] をクリックします。
- ④ ドロップダウンから [下記に設定した URL を常にホームページにする] を選択し、テキスト ボックスに URL を入力します。
- ⑤ 編集した内容を保存し、設定は完了です。



デバイスでの検証

ホームページが正しく設定されているかの確認

エンドユーザーのブラウザでホームページが正しく設定されているか確認します。

- ① 管理された検証用ブラウザを立ち上げ、リロードボタン右のホームボタンを押し、ホームページを確認します。
- もしくは
- ① 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
 - ② 「HomepageLocation」が設定した URL になっているか確認します。
 - ③ この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“ chrome://policy ” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。



起動時に最重要ページへ、生産性の向上！ 「RestoreOnStartupURLs」

起動時に開く URL

管理コンソールでの設定

ブラウザが起動時に開くページの URL を指定

社員の作業効率を向上させ、必要な情報へのアクセスを迅速化させましょう。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- ③ [フィルタを追加、または検索] に “ Restore ” と入力し、[起動時に読み込むページ] をクリックします。
- ④ ドロップダウンから [URL のリストを開く] を選択し、テキストボックスに URL を入力します。
- ⑤ 編集した内容を保存し、設定は完了です。



デバイスでの検証

起動時に開くページの URL の確認

エンドユーザーのブラウザで起動時に開くページが正しく設定されているか確認します。

- ① 管理された検証用ブラウザを立ち上げ、開くページを確認します。
- もしくは
- ① 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
 - ② 「RestoreOnStartupURLs」が設定した URL になっているか確認します。
 - ③ この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“ chrome://policy ” 画面の “ポリシーを再読み込み” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

Chrome を既定に、ブラウジングを最適化！ 「DefaultBrowserSettingEnabled」

デフォルトのブラウザの確認

管理コンソールでの設定

Chrome ブラウザをデフォルトのブラウザとして設定する。

全てのウェブページを Chrome ブラウザで一貫して開くことで、ブラウジング体験を最適化し、作業効率を向上させましょう。

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- 全てのブラウザに設定を適用する場合は、最上位の組織単位を選択したままにします。それ以外の場合は、子の組織単位を選択します。
- [フィルタを追加、または検索] に “ DefaultBrowserSetting Enabled ” と入力し、[デフォルトのブラウザの確認] をクリックします。
- ドロップダウンから [Chrome がデフォルトのブラウザになっていない場合は、起動時にデフォルトとして登録を試みる] を選択します。
- 編集した内容を保存し、設定は完了です。

Chrome のデフォルトのブラウザの確認を指定します。	
• ユーザーによる決定を許可（デフォルト） - Chrome ブラウザをデフォルトのブラウザにするかどうかをユーザーが選択できます。Chrome がデフォルトのブラウザになっていない場合、Chrome をデフォルトのブラウザとして選択するように求める通知が表示されるようになるかどうかをユーザーが選択できます。 • Chrome がデフォルトのブラウザになっていない場合は、起動時にデフォルトとして登録を試みる - デバイスを起動するたびに、Chrome ブラウザがデフォルトのブラウザになっているかどうかの確認が行われ、可能であれば自動的に登録されます。 • Chrome がデフォルトのブラウザかどうかの確認が行われないようにし、ユーザーが Chrome をデフォルトのブラウザに設定できないようにする - Chrome ブラウザがデフォルトのブラウザになっているかどうかの確認は行われず、ユーザーが Chrome をデフォルトのブラウザに設定することもできません。	
Chromium 名 DefaultBrowserSettingEnabled	サポート対象 Chrome (Windows) バージョン 11 以降 Chrome (Mac) バージョン 11 以降 Chrome (Linux) バージョン 11 以降
継承	ローカルに適用 ▼
設定	Chrome がデフォルトのブラウザになっ ▼ ていない場合は、起動時にデフォルト として登録を試みる

デバイスでの検証

起動時のデフォルト ブラウザ チェックが 有効になっているか確認

エンドユーザーの既定ブラウザを Chrome ブラウザにするように促しているか確認。

- 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- [DefaultBrowserSettingEnabled] が [true] になっているか確認します。
- この値が見つからない場合はデフォルト値になっているか、変更した場合で見つからない場合は、“ chrome://policy ” 画面の “ ポリシーを再読み込み ” を試し、それでもこのポリシーが適用されていない場合は再度管理コンソールで変更内容が保存されているかご確認ください。

閲覧データの自動消去、セキュリティを確保！ 「BrowsingDataLifetime」

閲覧データの有効期間の設定

管理コンソールでの設定

Chrome ブラウザ の閲覧データの有効期間の設定

このポリシーでは、Chrome ブラウザの閲覧データの有効期間を設定します。データの種類ごとに削除タイミングを設定し、機密性の高い顧客データ等を保護します。

- 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- [フィルタを追加、または検索] に “ BrowsingDataLifetime ” と入力し、[閲覧データの有効期間] をクリックします。
- こちらの設定で選択したデータが設定期間後に自動削除されるようになります。
- 編集した内容を保存し、設定完了です。

閲覧データの有効期間	ブラウザのデータ（履歴、Cookie、パスワードなど）を Chrome に保存しておく期間を指定できます。この設定は、機密データを扱うユーザーが利用すると便利です。
ブラウザ	▼
ユーザー	▼
グループ	▼
組織部門	▲
組織部門を検索	
▼ Global Organization	
▶ APAC	
Crash Report Test	
Devices	
▶ EMEA	
LTR dogfood	
Mobile	
▶ North America	
Chromium 名 BrowsingDataLifetime	サポート対象 Chrome (Windows、Mac、Linux) バージョン 89 以降 ChromeOS バージョン 89 以降 Chrome (Android) バージョン 96 以降
継承	Google のデフォルトに設定
保存	キャンセル

デバイスでの検証

Chrome ブラウザ の閲覧データの 有効期間の設定が適用されているか確認

エンドユーザーのブラウザで閲覧データの有効期間の設定がされているか確認します。

- 管理された検証用ブラウザで “ chrome://policy ” へ移動します。
- “ BrowsingDataLifetime ” が設定した内容になっているか確認します。

このポリシーは企業のデータ保護とセキュリティ管理を強化し、機密情報の取り扱いを効率的に管理します。

アイドル状態の対応、企業のルールで決定！ 「IdleTimeout」 & 「IdleTimeoutActions」

ブラウザのアイドル タイムアウト

管理コンソールでの設定

PC がアイドル状態のときの待機時間と動作の設定

これらのポリシーは、ユーザーがアクティブでないときの Chrome の動作を管理し、無操作時のセキュリティ リスクを軽減します。

● IdleTimeout (アイドル タイムアウト):

- パソコンがアイドル状態になってから “IdleTimeoutActions” で指定された動作をトリガーするまでの時間を設定します。
- 最小設定時間は 1 分。
- 「ユーザー入力」はマウスの動きやキーボード入力などを含みます。

IdleTimeoutActions (アイドル タイムアウト アクション):

- “IdleTimeout” で設定された時間に達した際に行う動作のリストです。
- サポートされる動作には、「close_browsers」（ブラウザを閉じる）や「show_profile_picker」（プロフィール選択ツールの表示）などが含まれます。
- 閲覧データの消去やウェブページの再読み込みも指定可能。

ブラウザが指定した期間アイドル状態になったときに実行させるアクションを選択できます。

[ブラウザのアイドル タイムアウト (分単位)] フィールドに、選択したアクションをブラウザが実行するまでの待機時間（ユーザ入力がない期間）を入力します。指定できる最小値は 1 分です。

[ブラウザのアイドル タイムアウト (分単位)] フィールドを空白のままにしたり、アクションを選択しなかったりすると、ブラウザは何のアクションも実行しません。

「ユーザー入力」はオペレーティング システムの API によって定義され、マウスの移動やキーボード入力などが該当します。

Chromium 名 IdleTimeout IdleTimeoutActions	サポート対象 Chrome (Windows、Mac、Linux) バージョン 116 以降 Chrome (Windows、Mac、Linux) バージョン 116 以降
継承	Google のデフォルトに設定
設定	ブラウザのアイドル タイムアウト (分単位) 一定時間マウスまたはキーボードによる入力がない状態が続くと、Chrome は以下に設定されているアクションを実行します。 アイドル状態の場合に実行するブラウザ操作 ☐ ブラウザを閉じる ☐ プロフィール選択ツールを表示する ☐ 閲覧履歴を消去する ☐ ダウンロード履歴を消去する ☐ Cookie と他のサイトデータを消去する ☐ キャッシュされた画像とファイルを消去する ☐ パスワード ログインを消去する ☐ 自動入力した情報を消去する ☐ サイトの設定を消去する ☐ ホストされているアプリデータを消去する ☐ ページを再読み込みする これらのアクションは、アイドル タイムアウトがトリガーされたときに、事前に定義された順序で実行されます。プロファイルが複数ある場合は、開いているプロファイルでのみ実行されます。

- ① 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。
- ② [フィルタを追加、または検索] に “IdleTimeout” もしくは “IdleTimeoutActions” と入力し、設定を行います。
- ③ 必要に応じて動作リストを選択し、設定します。
- ④ 編集した内容を保存し、設定完了です。

Chromium 名 IdleTimeout IdleTimeoutActions	サポート対象 Chrome (Windows、Mac、Linux) バージョン 116 以降 Chrome (Windows、Mac、Linux) バージョン 116 以降
継承	Google のデフォルトに設定
設定	ブラウザのアイドル タイムアウト (分単位) 一定時間マウスまたはキーボードによる入力がない状態が続くと、Chrome は以下に設定されているアクションを実行します。 アイドル状態の場合に実行するブラウザ操作 ☐ ブラウザを閉じる ☐ プロフィール選択ツールを表示する ☐ 閲覧履歴を消去する ☐ ダウンロード履歴を消去する ☐ Cookie と他のサイトデータを消去する ☐ キャッシュされた画像とファイルを消去する ☐ パスワード ログインを消去する ☐ 自動入力した情報を消去する ☐ サイトの設定を消去する ☐ ホストされているアプリデータを消去する ☐ ページを再読み込みする これらのアクションは、アイドル タイムアウトがトリガーされたときに、事前に定義された順序で実行されます。プロファイルが複数ある場合は、開いているプロファイルでのみ実行されます。

アイドル状態の対応、企業のルールで決定！ 「IdleTimeout」 & 「IdleTimeoutActions」

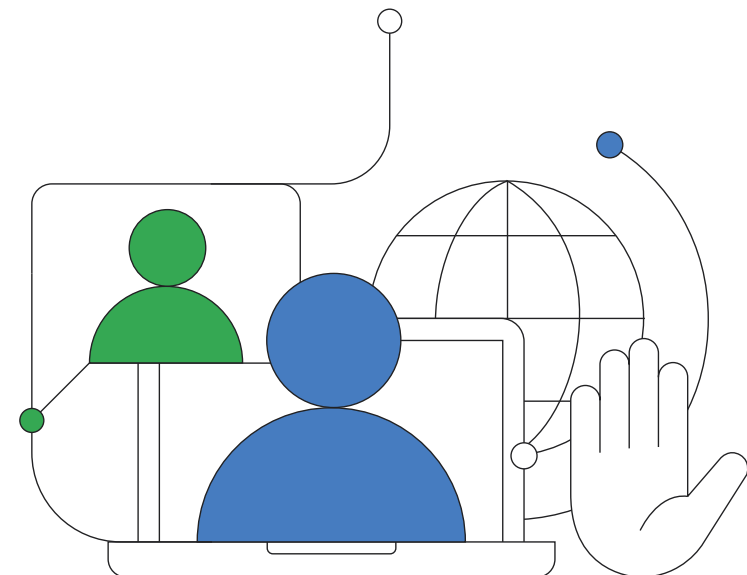
ブラウザのアイドル タイムアウト

デバイスでの検証

アイドル タイムアウトの設定が適用されているか確認

エンドユーザーのブラウザでアイドル タイムアウトの設定がされているか確認します。

- ① 管理された検証用ブラウザで “chrome://policy” へ移動します。
- ② “IdleTimeout” および “IdleTimeoutActions” が設定した内容になっているか確認します。



Chrome Enterprise Premium

より強力なセキュリティ機能をブラウザのみで実現

ここまでのページで説明したように、「Chrome Enterprise Core」を用いることで、組織で利用するブラウザに関する設定やポリシーを一元管理することができます。これに加えて、不正なサイトへのアクセス制御やファイル アップロードによる社内情報漏えい抑止など、より高度なセキュリティ機能を実現するのに役立つのが、「Chrome Enterprise Premium」です。

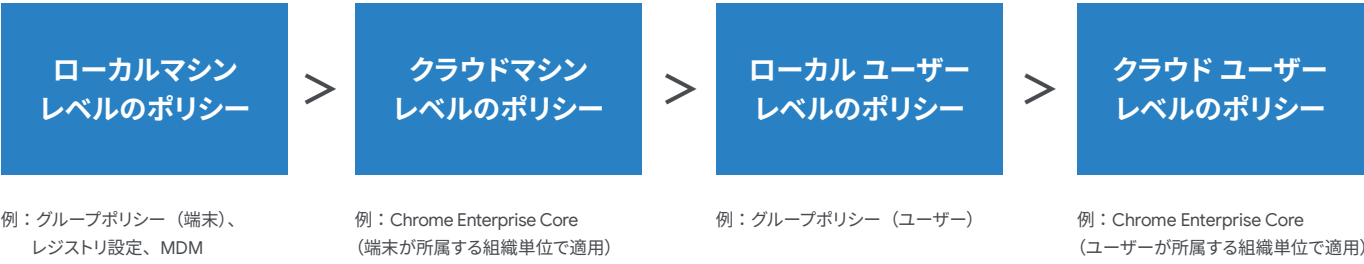
Chrome Enterprise Premium では、個人情報が入ったファイルのアップロード・ダウンロードの制御、URL カテゴリに基づく Web サイトへのアクセス ブロック、昨今活用が広まる生成 AI でのコンテンツ貼り付けの制御など、多彩な機能をブラウザのみで実現することができます。ここでは、Chrome Enterprise Premium の基本的な設定から、よく用いられるポリシー設定例を解説します。



ポリシーの優先順位のおさらい

管理コンソールでの設定

Chrome Enterprise Premium を設定する前に ...



この仕組みは Chrome Enterprise Premium でも使用することが可能です。

- 例としては
- ① ユーザー ポリシーでデータ損失防止を設定し、ダウンロード を [ブロック]
 - ② デバイス ポリシーでデータ損失防止を設定し、ダウンロード を [許可]

このような設定を施すと、ダウンロードは会社のデバイスでのみ可能になり、個人所有のデバイスでは会社プロファイルでログインしてもダウンロードはできなくなります。

デバイスレベルでポリシーを適用させると Incognito モード（シークレット モード）でもポリシーが当たるのでより強固なセキュリティ設定を施すことが可能です。

		会社所有の管理されたデバイス		管理されていない個人所有のデバイス	
		会社プロファイル	個人プロファイル	会社プロファイル	個人プロファイル
Chrome Enterprise Core	Group Policy	○	○		
	デバイス ポリシー	○	○		
	ユーザー ポリシー	○		○	

注意：Policy の統合を設定していない場合はすべての場合において最上位のポリシーが適用されます。

Chrome Enterprise Premium ライセンスの有効化

管理コンソールでの設定

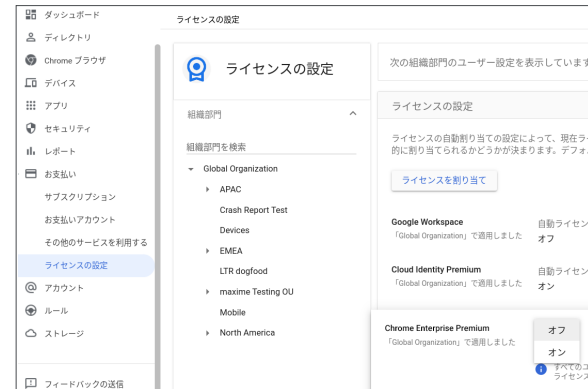
Chrome Enterprise Premium を設定する前に ...

ライセンスをユーザーに割り当てましょう。

Chrome Enterprise Premium のライセンスをお試し または ご購入 いただきありがとうございます。

Chrome Enterprise Premium の機能はユーザーに Chrome Enterprise Premium のライセンスが付与されていないと機能しません。

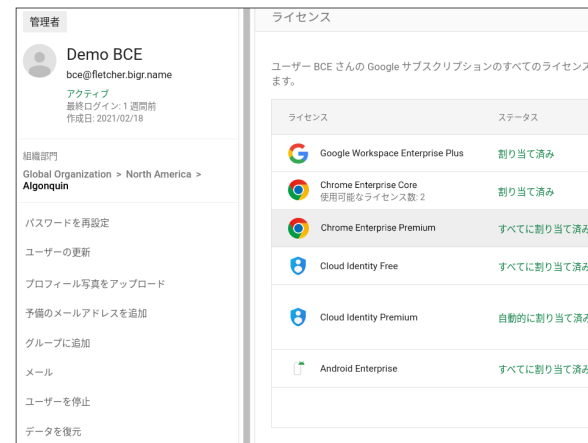
管理コンソール内の左側 「お支払い」 タブから「ライセンスの設定」をクリックし、Chrome Enterprise Premium のライセンスを指定した組織単位内のユーザーに自動で割り当てるように設定しましょう。



ライセンスをユーザーに割り当てられているか確認しましょう。

Chrome Enterprise Premium の設定を施す前に、テストするユーザーに Chrome Enterprise Premium のライセンスが付与されているか必ず確認してください。

「ディレクトリ」タブ下のユーザーから特定のユーザーを選択し、「ライセンス」という項目の中で Chrome Enterprise Premium が「割り当て済み」と記載されているか確認してください。



Chrome Enterprise Premium をフルに活用する為に

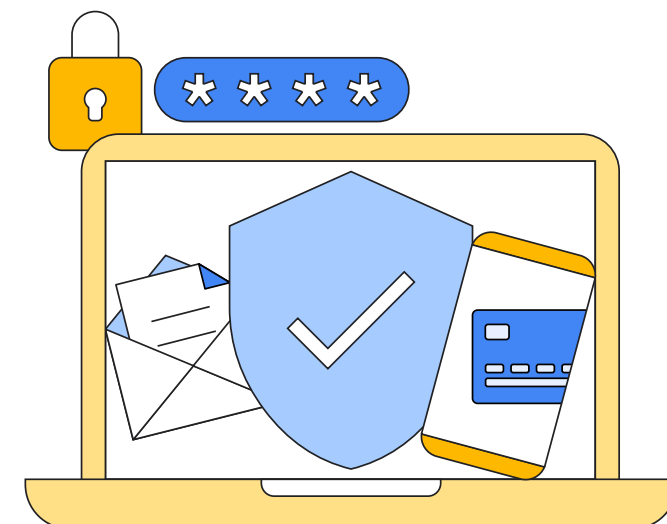
管理コンソールでの設定

Chrome Enterprise Premium を設定する前に ...

Chrome Enterprise Premium をフルに活用するために「Endpoint Verification」という拡張機能をユーザーレベルで配布しましょう。

Chrome Enterprise Premium の機能でアクセス制御を実装するために、「Endpoint Verification」(id: callobklhcbilphnckomhkgigmfocg) という拡張機能を Chrome ブラウザの全ユーザーに「自動インストール」配布する必要があります。

この拡張機能を利用することによって、アクセスレベルが設定されたデータ損失防止の制御なども設定可能となります。



まずはこのポリシーから
「エンタープライズ コネクタを許可する」

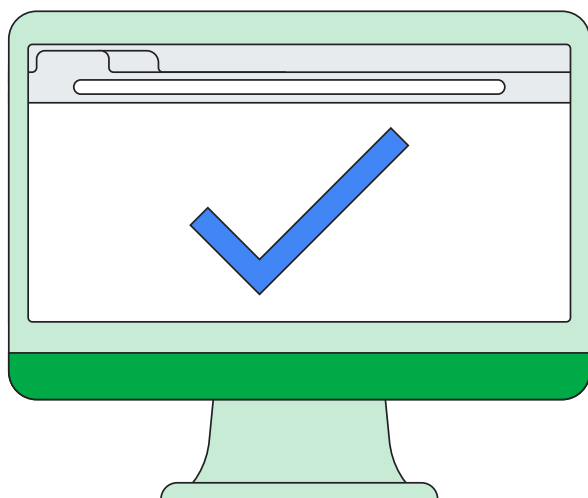
管理コンソールでの設定

Chrome Enterprise Premiumを設定する前に...

Chrome Enterprise Premiumの設定の一番最初にしないといけないことを説明します。

- 1 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- 2 [ユーザーとブラウザ] 次に ルート組織部門 を選択します。
- 3 [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- 4 [エンタープライズ コネクタを許可する] を選択し、“ユーザーに Enterprise Connectors の有効化を許可する” を選択します。
- 5 編集した内容を保存し、設定は完了です。

Chrome Enterprise コネクタ	
エンタープライズ コネクタ を許可する Google のデフォルトに設定 	ユーザーに Enterprise Connectors の有効化を許可する ▼ コネクタ ポリシーを管理する



「個人情報が入ったファイルのダウンロードとアップロードの禁止」

管理コンソールでの設定

まずはポリシー設定

ファイル コンテンツを分析し、内容に応じたダウンロード禁止、アップロード禁止の設定方法を説明します。

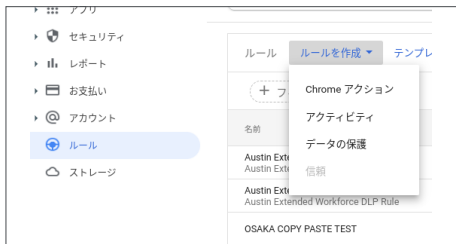
- 1 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- 2 [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- 3 [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- 4 [アップロード コンテンツの分析]、もしくは [ダウンロード コンテンツの分析] を選択し、“ Chrome Enterprise Premium ” を選択します。
- 5 必要であれば追加の設定をクリックし、編集してください。
- 6 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にルール設定

- 管理コンソールのホームページで左側の [ルール] をクリックします。
- [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。

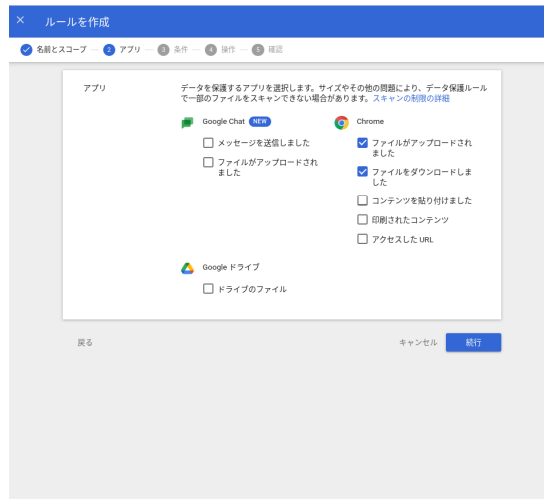


「個人情報が入ったファイルのダウンロードとアップロードの禁止」

管理コンソールでの設定

次にルール設定

- ⑩ ファイルがアップロードされました、及び ファイルをダウンロードしました のチェックボックスをチェックし、続行をクリックします。
- ⑪ すべてのコンテンツを選択し、事前定義されたデータを選択します。
- ⑫ 事前定義されたデータではメールアドレス、ドメイン名、他にも日本特有のプリセットではマイナンバー、運転免許証番号なども指定できます。
- ⑬ その後しきい値を設定し、続行を押します。



- ⑭ Chrome での操作を設定し、続行をクリック
- ⑮ アラートを受けたい場合はアラートの箇所も設定します。
- ⑯ 以上で設定は完了です。



「URL のカテゴリによるフィルタリング」

管理コンソールでの設定

まずはポリシー設定

URL カテゴリに応じたポリシーの設定方法を説明します。

- ① 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- ② [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- ③ [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- ④ [リアルタイムでの URL のチェック] を選択し、“ Chrome Enterprise Premium ” を選択します。
- ⑤ 必要であれば追加の設定をクリックし、編集してください。
- ⑥ 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にルール設定

- ⑦ 管理コンソールのホームページで左側の [ルール] をクリックします。
- ⑧ [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ⑨ ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。

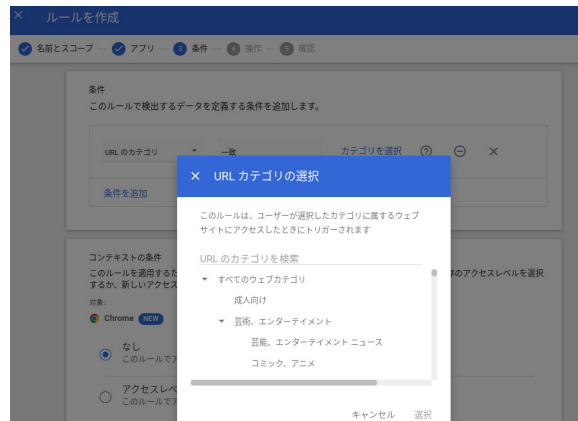
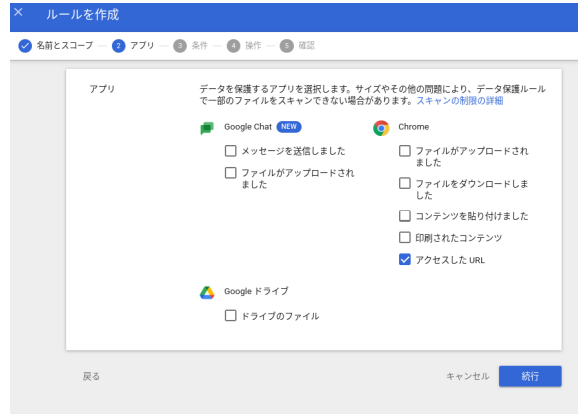


「URL のカテゴリによるフィルタリング」

管理コンソールでの設定

次にルール設定

- ⑩ アクセスした URL のチェックボックスをチェックし、続行をクリックします。
- ⑪ URL のカテゴリ を選択し、カテゴリ を選択します。
- ⑫ カテゴリ オプションとしては、成人向け、ショッピング、エンターテインメントなどがあります。
- ⑬ カテゴリを選んだあとは、続行を押します。



- ⑭ Chrome での操作を設定し、続行をクリック
注：監査は URL のチェック では使用ができません。
- ⑮ アラートを受けたい場合はアラートの箇所も設定します。
- ⑯ 以上で設定は完了です。



「生成 AI サイトへのコードの貼り付けの禁止」

管理コンソールでの設定

まずはポリシー設定

特定のサイトへの保護されたデータの貼り付けを禁止する方法を解説します。

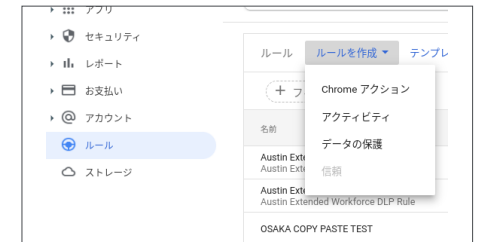
- ① 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- ② [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- ③ [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- ④ [リアルタイムでの URL のチェック] および [テキスト コンテンツの一括分析] を選択し、“ Chrome Enterprise Premium ” を選択します。
- ⑤ 必要であれば追加の設定をクリックし、編集してください。
- ⑥ 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にルール設定

- ⑦ 管理コンソールのホームページで左側の [ルール] をクリックします。
- ⑧ [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ⑨ ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。

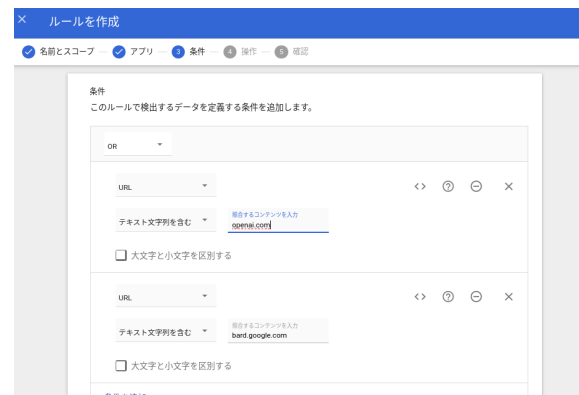


「生成 AI サイトへのコードの貼り付けの禁止」

管理コンソールでの設定

次にルール設定

- ⑩ アクセスした URL のチェック ボックスをチェックし、続行をクリックします。
- ⑪ URL を選択し、生成 AI 系のサイトを手打ち
もしくは
URL のカテゴリを選択し、生成 AI を選択します。



- ⑫ Chrome での操作を設定し、続行をクリック
- ⑬ アラートを受けたい場合はアラートの箇所も設定します。
- ⑭ 以上で設定は完了です。



「管理されていないブラウザからの生成 AI サイトへのアクセス管理」

管理コンソールでの設定

まずはポリシー設定

管理対象となっていないブラウザからの特定の URL へのアクセス制御の方法を説明します。

- ① 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- ② [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- ③ [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- ④ [リアルタイムでの URL のチェック] を選択し、“ Chrome Enterprise Premium ” を選択します。
- ⑤ 必要であれば追加の設定をクリックし、編集してください。
- ⑥ 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にアクセスレベル設定

- ⑦ 管理コンソールのホームページで左側の [セキュリティ] をクリックし、ドロップダウン内の [アクセスとデータ管理] [コンテキスト アウェアアクセス] をクリックします。
- ⑧ [アクセスレベル] 次にアクセスレベルの作成を選択します。



「管理されていないブラウザからの生成 AI サイトへのアクセス管理」

管理コンソールでの設定

次にアクセスレベル設定

- ⑨ アクセスレベルの作成ではアクセスレベルの名前をつけ、コンテキストの条件を詳細モードもしくは基本モードで記入

- ⑩ こちらは詳細モードで記載しています。

詳しくはこちら参照：

<https://support.google.com/a/answer/11368990?sjid=6499435835312746404-AP#zippy=%2Callow-access-only-from-a-managed-chrome-browser-with-latest-updates>

<https://cloud.google.com/access-context-manager/docs/browser-attributes?hl=ja>

× アクセスレベルを作成

詳細

名前と説明

新しいアクセスレベルの名前と説明を設定してください

- 1 コンテキストウェア アクセスマスまたはデータ保護ルールにアクセスレベルを使用できます。ルール適用を適用できる名前を設定することをおすすめします。例「DLP 用のデバイスの条件」。

アクセスレベルの名前

非管理対象ブラウザ

説明

コンテキストの条件

コンテキストウェア アクセスマス ポリシーまたはデータ保護ルールで使用するコンテキスト条件を作成します。基本モードまたは詳細モードのどちらかを使用します。保存時には、現在選択されているモードの条件のみが保存されます。[コンテキストの条件の詳細](#)

次の点にご注意ください。

- コンテキストウェア アクセスマスの場合: ユーザーにアプリへのアクセスを許可するタイミングは、コンテキストの条件によって異なります。
- データ保護ルールの場合: コンテキストの条件は、ルールを適用するタイミングを判断するのに役立ちます。

[例を見る](#)

基本 詳細

条件を、Common Expression Language (CEL) を使用して記述します。 [詳細](#)

```
1 device.chrome.management_state == ChromeManagementState.CHROME_MANAGEMENT_STATE_BROWSER_MANAGED
```

管理コンソールでの設定

次にルール設定

- ⑪ 管理コンソールのホームページで左側の [ルール] をクリックします。
- ⑫ [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ⑬ ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。

アプリ

セキュリティ

レポート

お支払い

アカウント

ルール

ストレージ

ルール

ルールを作成

テンプレート

Chrome アクション

アクティビティ

データの保護

名前

Austin Exti

Austin Exti

Austin Exti

Austin Extended Workforce DLP Rule

信頼

OSAKA COPY PASTE TEST

× ルールを作成

名前とスコープ

アプリ

条件

操作

確認

名前

ルールを簡単に識別できるように、わかりやすい名前を使用することをおすすめします。

名前

BCE Download / Upload Restriction

説明

範囲

このルールの適用対象とする組織部門またはグループを選択します。なお、このルールの適用方法は、次のページで選択するアプリによって異なります。[スコープの詳細](#)

☒ Global Organization 内のすべて

☐ 組織部門またはグループ

☐ 組織部門を含める

☐ 組織部門を除外

☐ グループを含める

☐ グループを除外

キャンセル 続行

「管理されていないブラウザからの生成 AI サイトへのアクセス管理」

管理コンソールでの設定

次にルール設定

- ⑭ アクセスした URL のチェック ボックスをチェックし、続行をクリックします。
- ⑮ URL を選択し、生成 AI 系のサイトを打ちします。
- ⑯ 先程設定したアクセスレベルを設定します。

× ルールを作成

名前とスコープ

アプリ

条件

操作

確認

条件

このルールで検出するデータを定義する条件を追加します。

URL

テキスト文字列を含む

大文字と小文字を区別する

条件を追加

コンテキストの条件

このルールを適用するためにユーザーが満たす必要があるコンテキストの条件を定義するには、既存のアクセスレベルを選択するか、新しいアクセスレベルを作成します。[コンテキストの条件の詳細](#)

例:

Chrome

なし

このルールでアクセスレベルを使用しません

アクセスレベルを選択する

このルールでアクセスレベルを使用します

BrowserNotManaged

詳細 (CEL) モードを使用して作成されたアクセスレベルの詳細は利用できません

CBCM managed

ユーザーは次のアクセスレベルの条件を満たす必要がある。JP ONLY BROWSER

アクセスレベル

BrowserNotManaged

詳細 (CEL) モードを使用して作成されたアクセスレベルの詳細は利用できません

他のアクセスレベルが必要ですか？

- ⑰ Chrome での操作を設定し、続行をクリック
- ⑱ アラートを受けたい場合はアラートの箇所も設定します。
- ⑲ 以上で設定は完了です。

× ルールを作成

名前とスコープ

アプリ

条件

操作

確認

操作

条件を満たした場合に行う処理を選択します

Chrome

ブロック

アラート

イベントがこのルールの基準 (スコープ、アプリ、条件) を満たしている場合は、セキュリティ デッシュボードとアラートセンターにイベントが報告されます (該当する場合)。イベントが報告される最大レベルを選択します。

低

☐ アラートセンターに送信する

アラートセンターのアラートには、管理者が問題に対処できるよう詳細な情報が含まれます。これらのアラートは、ドメイン内の他の管理者と協力して問題を解決するのに役立ちます。この設定を有効にすることをおすすめします。

[詳細](#)

戻る

キャンセル

続行

「オンラインストレージからの大量ダウンロードの検知」

管理コンソールでの設定

まずはポリシー設定

オンラインストレージからの異常なデータ転送の監視が可能です。

- 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- [リアルタイムでの URL のチェック] および [ダウンロード コンテンツの分析] を選択し、“ Chrome Enterprise Premium ” を選択します。
- 必要であれば追加の設定をクリックし、編集してください。

Tips: Chrome Enterprise Premium では 50mb 以上のファイルはスキャンされないため、50mb 以上のファイルのダウンロードをブロックしたい場合は一番下の設定を施してください。

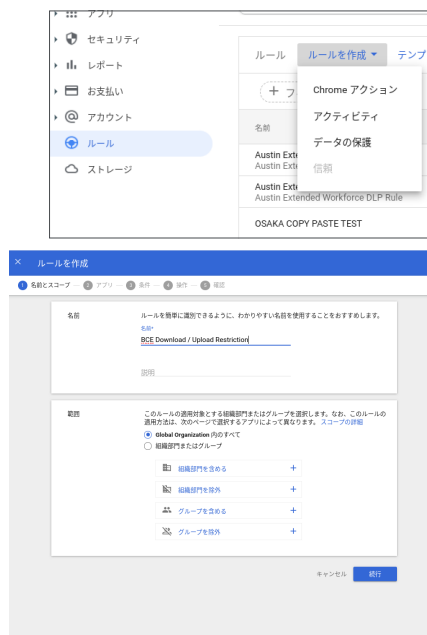
- 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にルール設定

- 管理コンソールのホームページで左側の [ルール] をクリックします。
- [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。



「オンラインストレージからの大量ダウンロードの検知」

管理コンソールでの設定

次にルール設定

- ファイルをダウンロードしました のチェック ボックスをチェックし、続行をクリックします。
- URL のカテゴリを選択し、カテゴリから クラウドストレージを選択します。
- 条件の追加を押し、ファイルサイズの条件を追加します。
- ファイルサイズではバイト数を入力するので 1,048,576 byte は1メガバイト相当となります。



- Chrome での操作を設定し、続行をクリック
- アラートを受けたい場合はアラートの箇所も設定します。
- 以上で設定は完了です。



「BYOD 上のブラウザからのデータのダウンロード禁止」

管理コンソールでの設定

アクセスレベル設定のおさらい

個人所有の端末のアクセス制御及びデータ損失防止のルールを設定する方法について解説します。

- 1 管理コンソールのホームページで左側の [セキュリティ] をクリックし、ドロップダウン内の [アクセスとデータ管理] [コンテキスト アウェアアクセス] をクリックします。
- 2 [アクセスレベル] 次にアクセスレベルの作成を選択します。
- 3 アクセスレベルの作成ではアクセスレベルの名前をつけ、コンテキストの条件を詳細モードで記載します。

詳しくはこちら参照：

<https://support.google.com/a/answer/11368990>

<https://cloud.google.com/access-context-manager/docs/browser-attributes>



「BYOD 上のブラウザからのデータのダウンロード禁止」

管理コンソールでの設定

次にルール設定

- 7 Chrome 「ファイルのダウンロード」を選択します。
- 8 データの条件を設定します。(例：全ファイル→ 1 byte 以上)
- 9 先程設定したアクセスレベルを設定します。

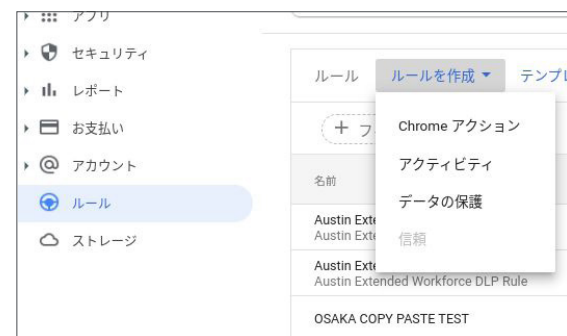
プロファイル ベースのポリシーだけあたっているブラウザのアクセスレベル
`device.chrome.management_state ==`
`ChromeManagementState.CHROME_MANAGEMENT_STATE_PROFILE_MANAGED`



管理コンソールでの設定

次にルール設定

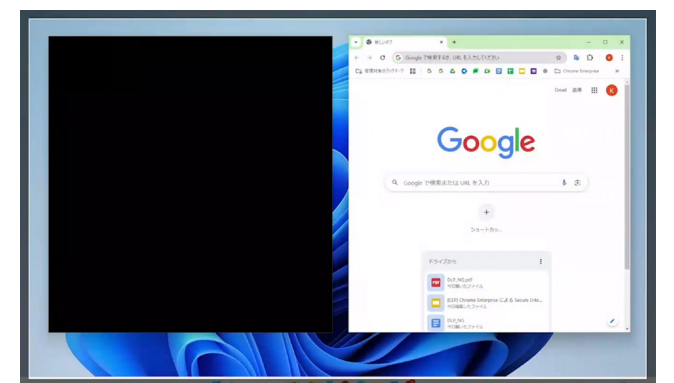
- 4 管理コンソールのホームページで左側の [ルール] をクリックします。
- 5 [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- 6 ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。



●スクリーンショットによる情報流出を防止

たとえ、ファイルのダウンロードを制御したとしても、例えば画面のスクリーンショットを撮るなどして情報を社外に持ち出されてしまう可能性があります。

Chrome Enterprise Premium では、上記に説明したダウンロード制御の機能のほか、スクリーンショットのツールを実行した際に、個人所有の端末上にて保護されているページのみ画面をブラックアウトできる機能も備えています。



「オンラインストレージへの透かしの追加」

管理コンソールでの設定

まずはポリシー設定

オンラインストレージ内のファイルに、不正利用を防ぐための透かしを追加する方法を解説します。

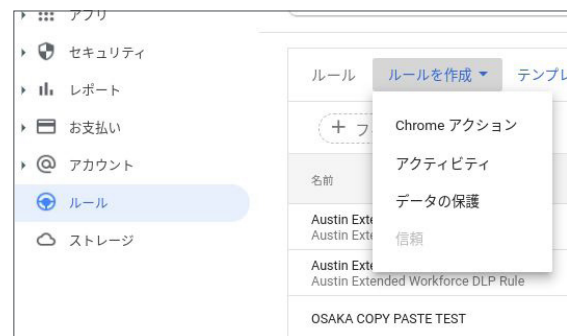
- 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。
- [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。
- [フィルタを追加、または検索] に “ Chrome Enterprise コネクタ ” と入力しカテゴリを選択し、検索します。
- [リアルタイムでの URL のチェック] を選択し、“ Chrome Enterprise Premium ” を選択します。
- 編集した内容を保存し、設定は完了です。



管理コンソールでの設定

次にルール設定

- 管理コンソールのホームページで左側の [ルール] をクリックします。
- [ルールの作成] をクリック、ドロップダウン内の [データの保護] をクリックします。
- ルールの作成内でルール名を入力し、組織単位を選択または全ての組織単位を選択し、続行をクリックします。

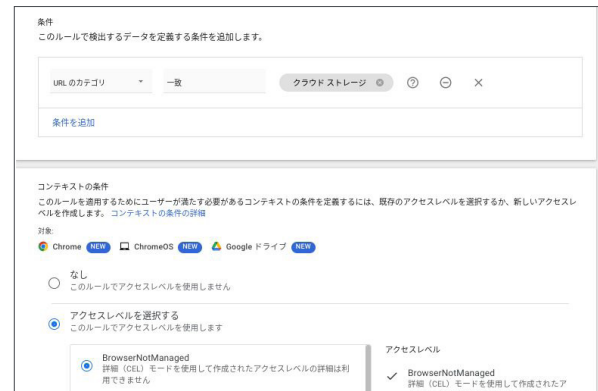
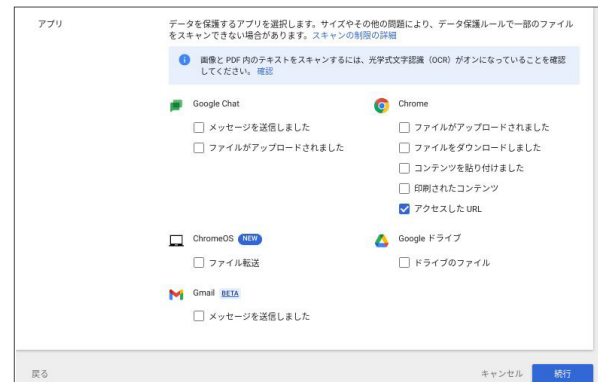


「オンラインストレージへの透かしの追加」

管理コンソールでの設定

次にルール設定

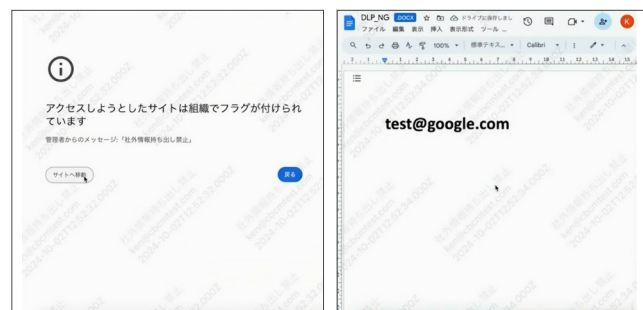
- アクセスした URL のチェック ボックスをチェックし、続行をクリックします。
- URL のカテゴリを選択し、カテゴリから クラウド ストレージを選択します。
- (必要であればコンテキストの条件内でアクセスレベルを選択します)



- Chrome での操作を「監査のみ」に設定し、続行をクリック
- 「ページのコンテンツに透かしを追加する」のチェックボックスを選択し、必要であれば「透かしメッセージをカスタマイズする」をチェックしカスタム メッセージを入力します。
- アラートを受けたい場合はアラートの箇所も設定します。
- 以上で設定は完了です。

設定完了後の画面

個人所有の端末からアクセスがあった際に、それをアラートするほか、社外持ち出しである旨を透かしとして表示し、スマートフォンでの撮影などによる情報流出を抑止します。

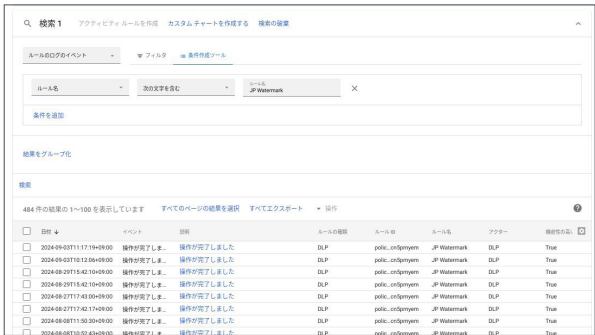


「DLP ルールをトリガーした アクションを調査する」

管理コンソールでの設定

今まで設定したルールに反するアクションが起きた際に、原因となった操作の特定が可能です。

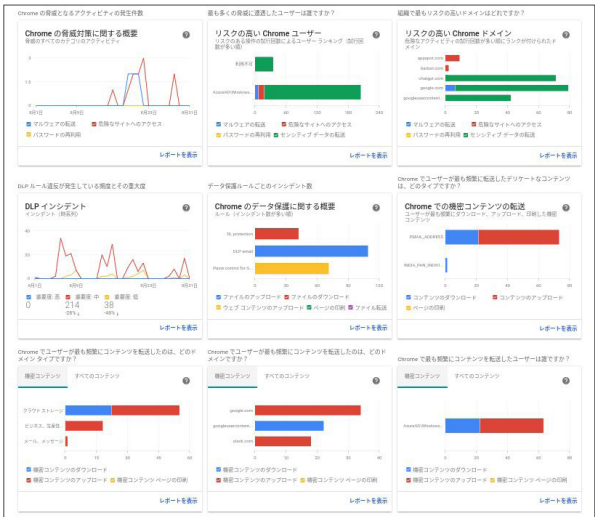
- ① 管理コンソールのホームページで左側の「ルール」をクリックします。
- ② 「調査」をクリックします。
- ③ こちらのページでは全てのルールに反したデータ損失防止イベントがログされています。(半年間保存されます。)
- ④ また特定のルールを調査したい場合は「条件を追加」をクリックし、ルール名やルール id などで検索をかけることも可能です。
- ⑤ そして調査ログをもっと詳しく見たい場合は青文字で書いてある「操作が完了しました」をクリックいただくと、より詳しいログが閲覧可能です。



「DLP ルールをトリガーした アクションを調査する」

管理コンソールでの設定

- ⑦ リスクのあるユーザー・リスクのあるドメイン・機密コンテンツが頻繁にやり取りされているカテゴリ、ユーザー、ドメイン等のインサイダーリスクのレポートを確認することができます。



●管理コンソールでログを一元管理

Chrome Enterprise Premium の管理コンソールでは、Chrome ブラウザ上でのユーザーの行動を一元的に管理し、さまざまな脅威情報を可視化できます。

全体傾向と同様に、1つひとつの細かなセキュリティ ログも追跡でき、エンドポイント側のデータの操作まで細かくトラッキングすることが可能です。

