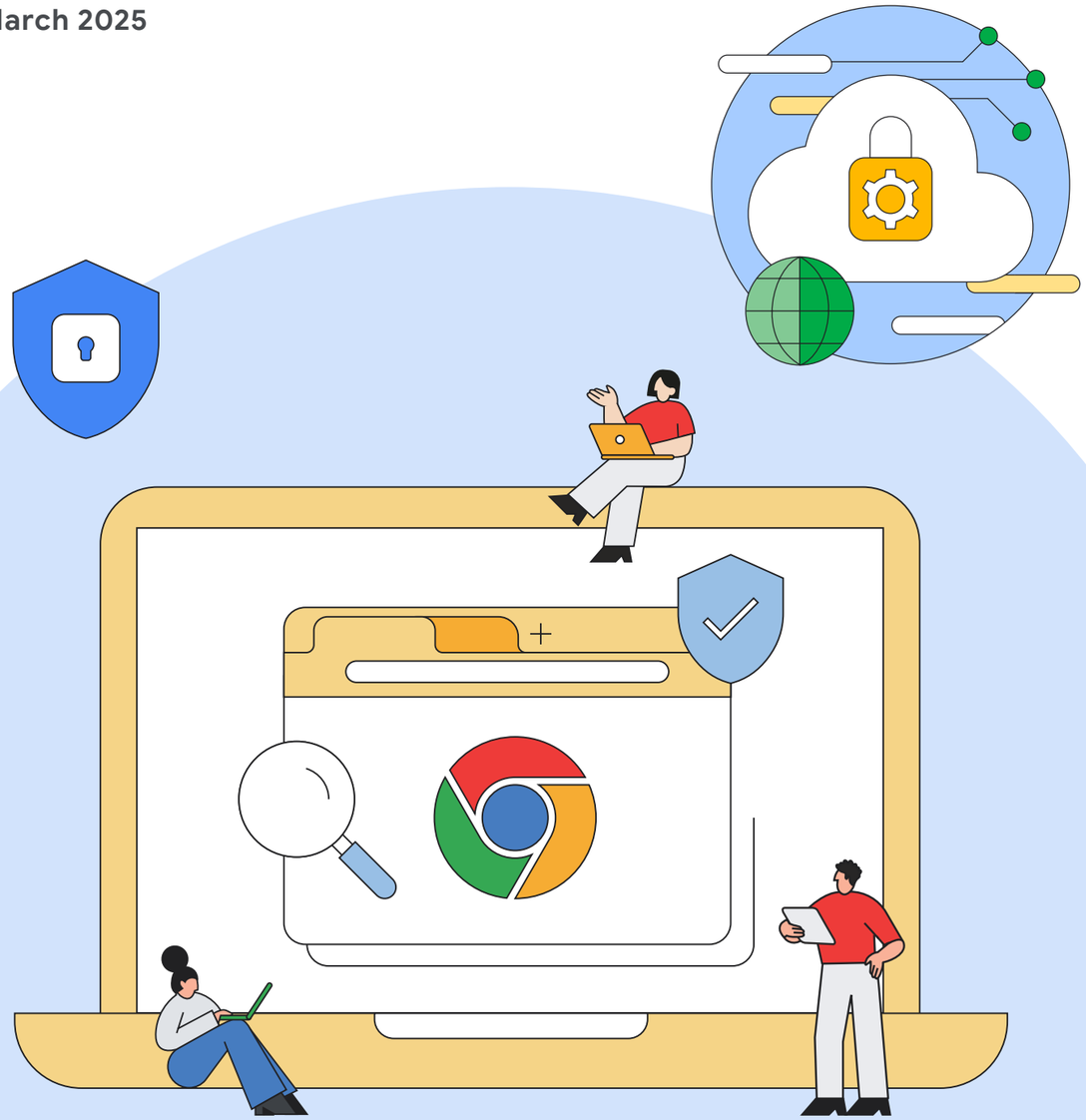
chrome enterprise

Chrome Enterprise ガイドブック

March 2025



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/

chrome enterprise

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。

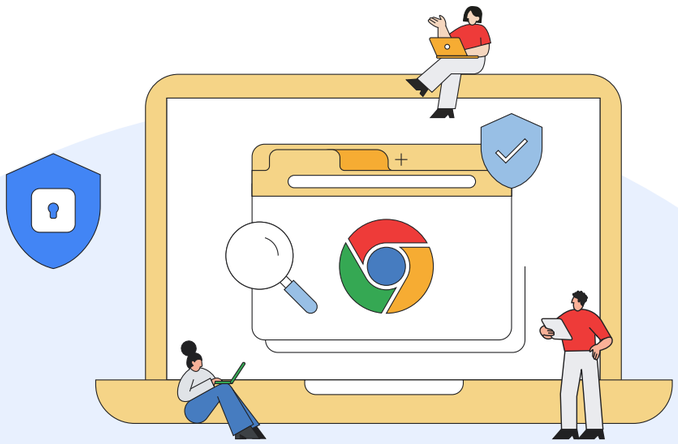
SaaS アプリケーション拡大に伴い、働く人々はより業務でブラウザを操作する時間が増え、さまざまなデジタルデータや情報をブラウザ経由で扱うようになっています。言い換えれば、デジタル時代は、日々の業務がかつてないほどブラウザに依存するようになった時代とも言えます。

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

セーフ ブラウジング シリーズ

セキュリティ シリーズ

chrome enterprise

Contents

Chrome Enterprise Core

パスワード マネージャー シリーズ

更新管理シリーズ

拡張機能シリーズ

作業効率シリーズ

Chrome Enterprise Premium

基本設定

シナリオ1

シナリオ2

シナリオ3

シナリオ4

シナリオ5

シナリオ6

シナリオ7

シナリオ8

chrome enterprise

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。

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。

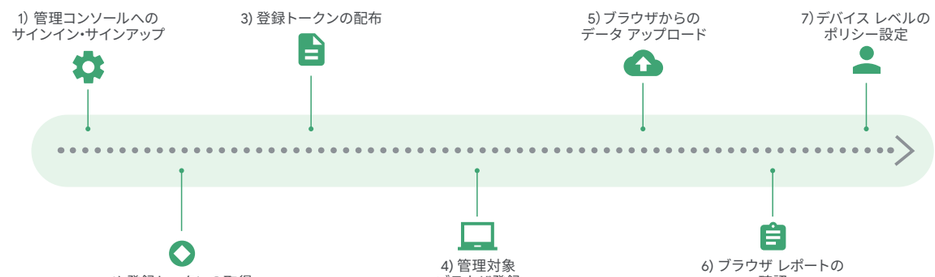
Chrome Enterprise Core の導入メリットを得る

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（ グローバルに一意な識別子）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、プロファイ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。

❶ 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。

❷ [ユーザーとブラウザ] 次に ルート組織部門 を選択します。

❸ [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。

❹ [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。

❺ 編集した内容を保存し、設定は完了です。

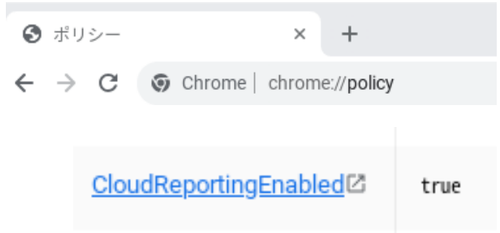
デバイスでの検証　管理対象ブラウザの状態を可視化する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ [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。

❸ 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。

❶ 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。

❷ [ユーザーとブラウザ] 次に ルート組織部門 を選択します。

❸ [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。

❹ [イベント レポートを有効にする] を選択します。

❺ [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。

❻ 編集した内容を保存し、設定は完了です。

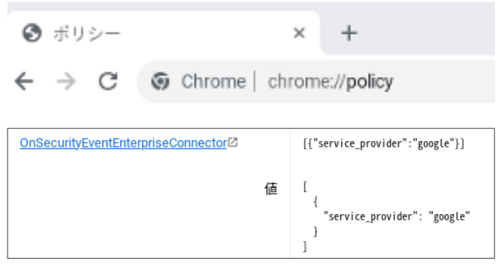
デバイスでの検証　管理対象ブラウザの状態を可視化する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ [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。

❸ 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おります。

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。)

ローカルマシン レベルのポリシー > **クラウドマシン レベルのポリシー** > **ローカル ユーザー レベルのポリシー** > **クラウド ユーザー レベルのポリシー**

例：グループポリシー（端末）、レジストリ設定、MDM

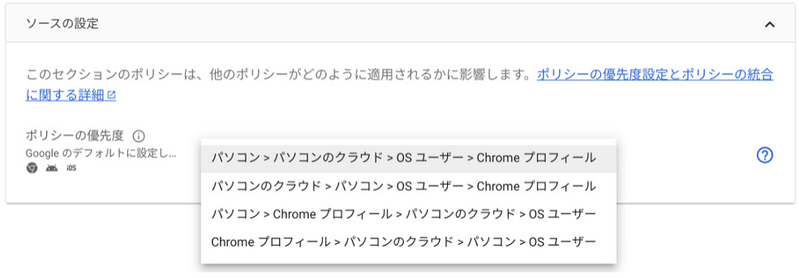
例：Chrome Enterprise Core（端末が所属する組織単位で適用）

例：グループポリシー（ユーザー）

例：Chrome Enterprise Core（ユーザーが所属する組織単位で適用）

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。

❶ 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。

❷ 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。

❸ [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。

❹ 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。

❺ 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。

❶ 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。

❷ 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。

❸ [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。

❹ [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。

❺ 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

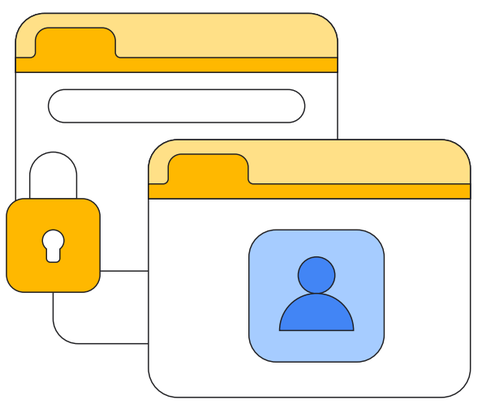
デバイスでの検証　ポリシーの優先度をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ (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。

❸ 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。

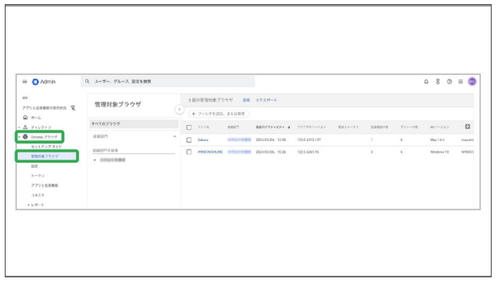


管理対象とする Chrome ブラウザの登録

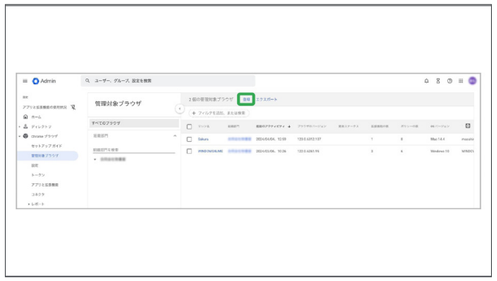
①登録トークンの生成

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

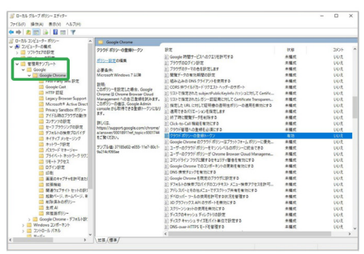
Windows 上で動作する Chrome ブラウザは、右記の方法で Chrome Enterprise Core の管理対象にできます。

- 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

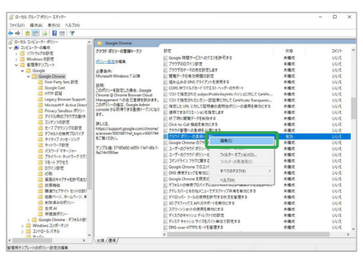
ー グループ ポリシー管理エディターを使用する



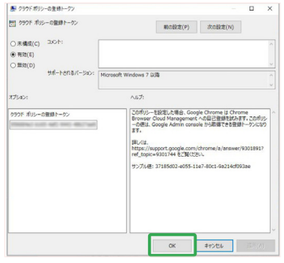
①グループ ポリシー管理エディターを起動します。

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。

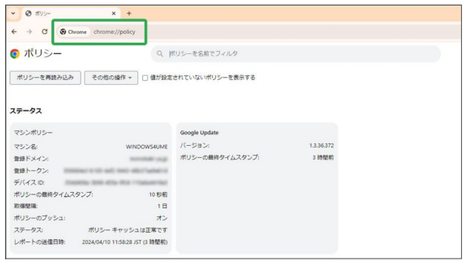
・Chrome の管理用テンプレート（Chrome ADX/ADMX テンプレート）は、以下の Web ページからダウンロードできます。
https://chromeenterprise.google/intl/ja_jp/browser/download/#manage-policies-tab
・ダウンロードした管理用テンプレートは、グループ ポリシー管理エディターに追加してください。



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。



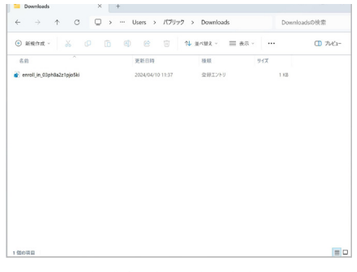
④［オプション］にトークンの値を設定し、［OK］をクリックします。⑤ターミナルを起動し、gpupdate コマンドによってグループ ポリシーを適用します。



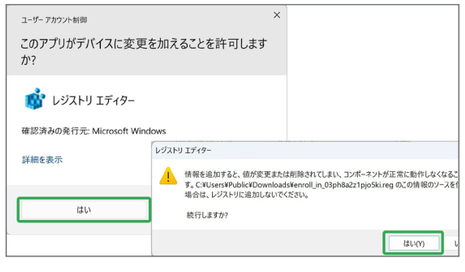
⑥ Chrome ブラウザを起動し、
アドレスバーに「 chrome://policy 」と入力します。
Chrome ブラウザが動作するマシンのポリシーが表示されます。

ー 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。



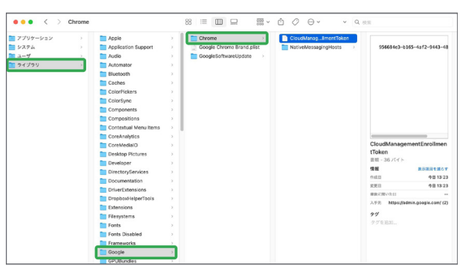
②［はい］をクリックします。
注意を促すダイアログ ボックスが表示されます。
③［はい］をクリックします。
トークンのキーと値がレジストリに追加されます。

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

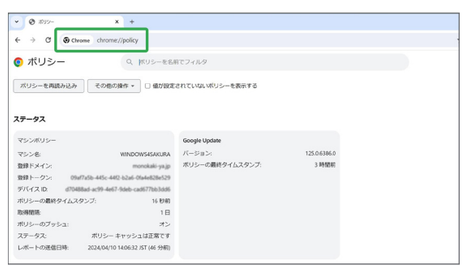
macOS 上で動作する Chrome ブラウザを Chrome Enterprise Core の管理対象とするため、テキスト ファイル形式で入手したトークンを登録します。



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。

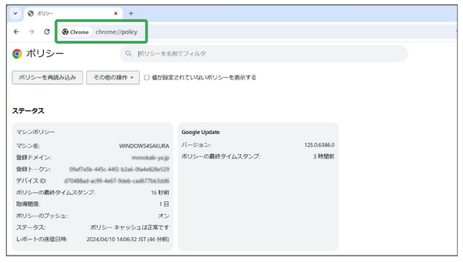
②ダウンロードしたテキストファイル（トークン）を、以下の場所に収めます。
［ライブラリ］→［Google］→［Chrome］



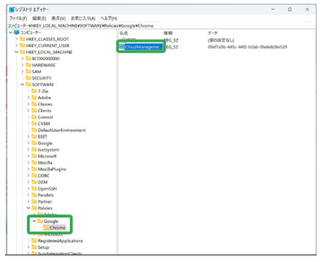
③ Chrome ブラウザを起動し、
アドレスバーに「 chrome://policy 」と入力します。
Chrome ブラウザのユーザーに関するポリシーが表示されます。

②トークンの登録

ー 拡張子 .reg ファイルによる登録



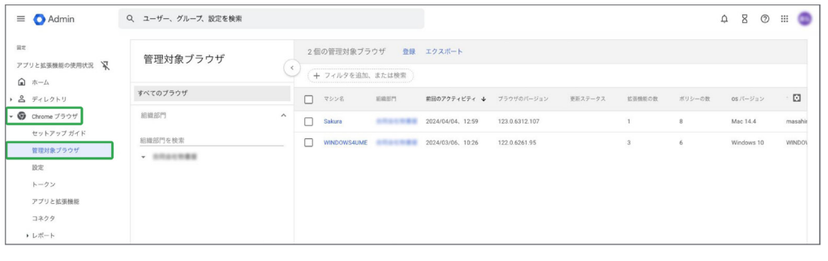
④ Chrome ブラウザを起動し、
アドレスバーに「 chrome://policy 」と入力します。
Chrome ブラウザが動作するマシンのポリシーが表示されます。



Chrome ブラウザが動作するマシンのポリシーが表示されないときには、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。

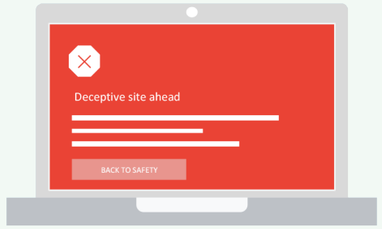
セーフ ブラウジング

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 ブラウジングを有効にして、危険なサイトへのアクセスを禁止する（1）

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。

❶ 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。

❷ [ユーザーとブラウザ] をクリックします。

❸ [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。

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。

❹ [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。

❺ 保存した内容を確認します。

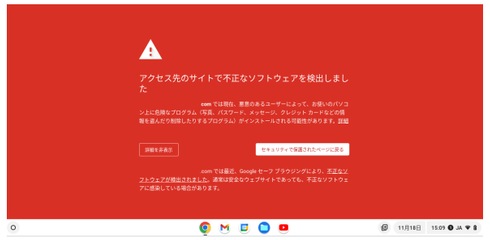
デバイスでの検証

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。

❶ 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 ブラウジングを強制して、危険なサイトへのアクセスを禁止する

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。

❶ 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。

❷ [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。

❸ [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。

❹ 保存した内容を確認します。

デバイスでの検証

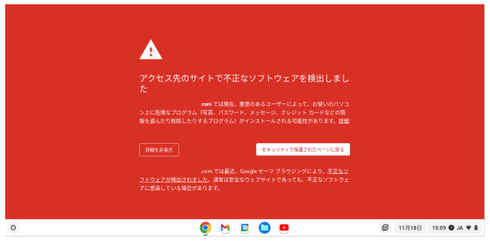
セーフ ブラウジングを有効にして、危険なサイトへのアクセスを禁止する

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

❶ 危険なサイトにアクセスすると、警告が表示されます。

❷ [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

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

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。

❶ 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。

❷ 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。

❸ [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。

❹ 許可するドメインを入力します。

❺ 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

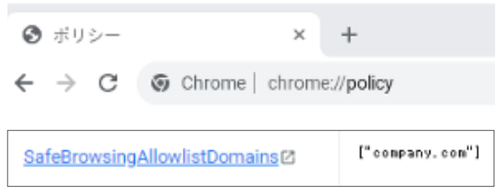
「 SafeBrowsingAllowlistDomains 」をブラウザ上で確認する

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

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。



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。

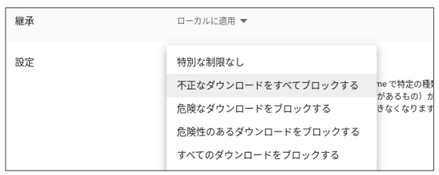
❶ 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。

❷ 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。

❸ [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。

❹ ダウンロードの制限レベルを設定します。

❺ 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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ [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

❺ 保存した内容を確認して、設定は完了です。

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

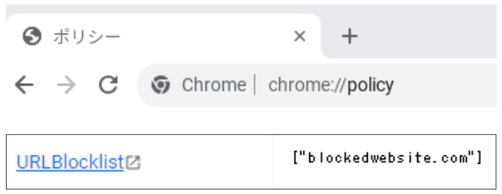
デバイスでの検証　URL をブロックする

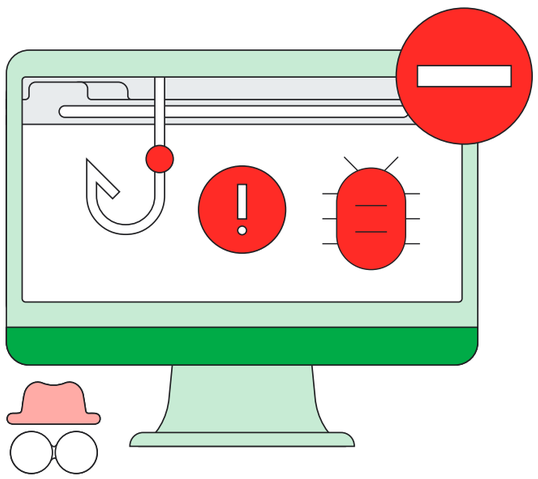
指定したサイト以外でブラウザ アクセスができないことを確認します。

❶ 管理された検証用ブラウザで “chrome://policy” へ移動します。

❷ “URLBlocklist” が設定した URL になっているか確認します。

❸ 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 」

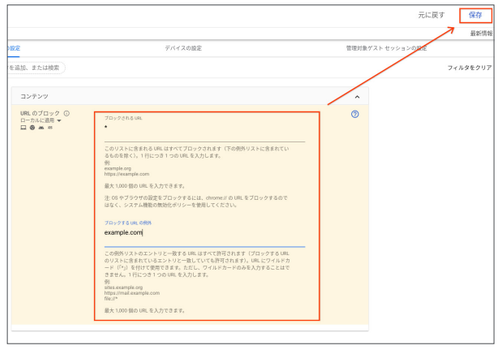
管理コンソールでの設定　社内のポータル サイトのみアクセスを許可

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。

❹ [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。
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

❺ 保存した内容を確認して、設定は完了です。



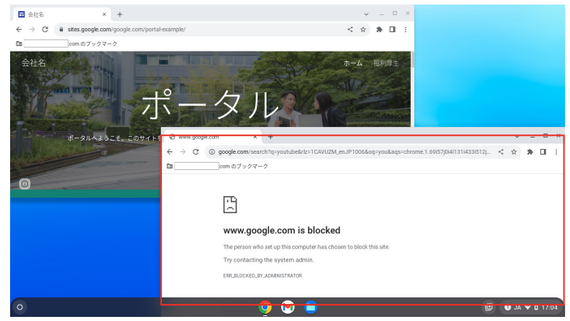
URL のブロック

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。

❶ 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。

❷ 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

煩わしい広告が掲載されるサイトでの広告表示を許可するかブロックするかを管理

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。

❶ 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。

❷ 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。

❸ [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。

❹ 広告の表示設定を選択します。

❺ 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

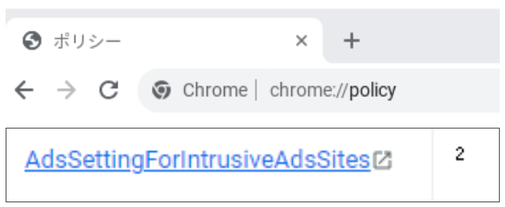
「 AdsSettingForIntrusiveAdsSites 」をブラウザ上で確認する

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

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “AdsSettingForIntrusiveAdsSites” が設定した値になっているか確認します。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ 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。

❺ 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

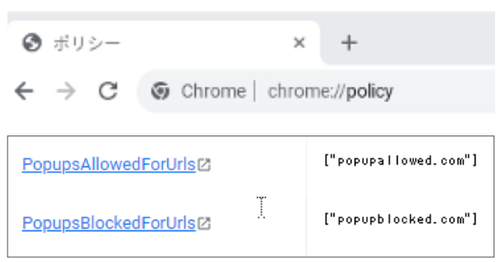
「 DefaultPopupsSetting 」をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。



セキュリティ シリーズ

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。

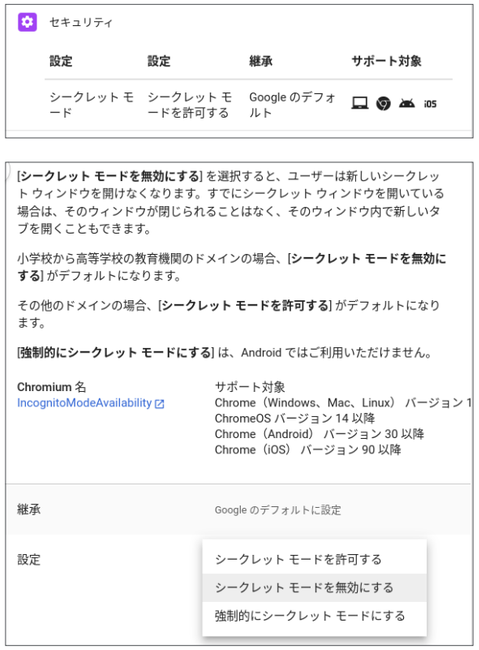
❶ 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。

❷ 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。

❸ [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。

❹ [シークレット モードを無効にする] を選択します。

❺ 編集した内容を保存し、設定は完了です。



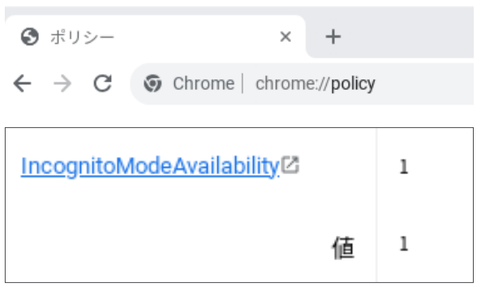
デバイスでの検証　「 IncognitoModeAvailability 」をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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 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 」

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。

❶ 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。

❷ 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。

❸ [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。

❹ パスワード マネージャーの使用を設定します。

❺ 編集した内容を保存し、設定は完了です。

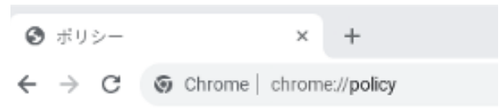
デバイスでの検証　「 PasswordManagerEnabled 」をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ [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。

❺ 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

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。

❻ 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。

❼ 左側の [Chrome] をクリックします。

❽ [設定] 次に [ユーザーとブラウザ] をクリックします。

❾ [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。

❿ [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。

⓫ 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

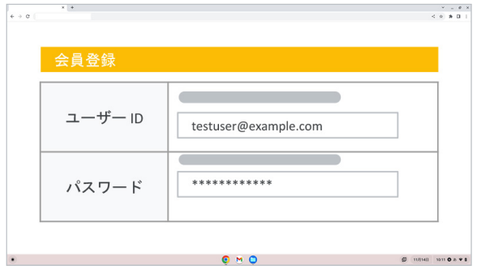
デバイスでの検証

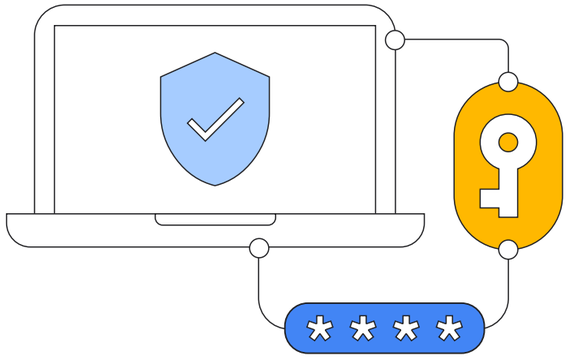
許可されていないサイトでのパスワードの再利用を警告する

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。

❶ 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。

❷ 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「 PasswordProtectionChangePasswordURL 」

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。

❶ 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。

❷ 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。

❸ [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。

❹ [パスワードの変更に使用する URL] の欄に URL を入力します。

❺ 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

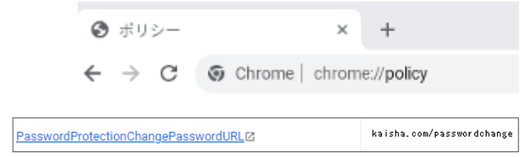
「 PasswordProtectionChangePasswordURL 」をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ [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。

❺ 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

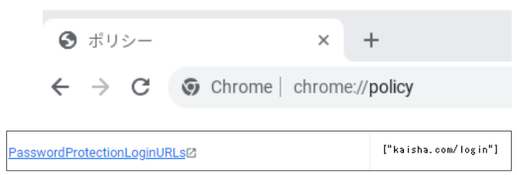
「 PasswordProtectionLoginURLs 」をブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❸ 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。



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

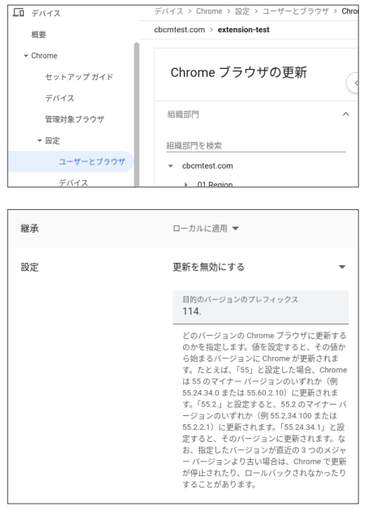
特定のバージョンのブラウザ環境を維持するため、特定のバージョン以降の Chrome の自動更新を防ぎます。

❶ 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。

❷ 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。

❸ [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。

❹ [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。



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。

❺ 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。

❻ 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. ）

❼ 編集した内容を保存し、設定は完了です。

❽ 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でご注意ください。

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。

❶ 管理された検証用ブラウザで “ chrome://version ” へ移動します。

❷ [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

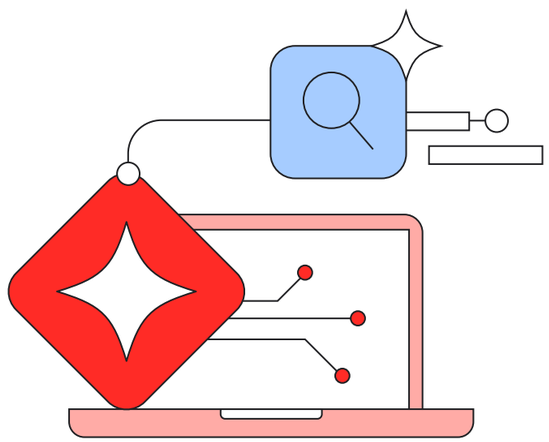
❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ “ 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。

❶ 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。

❷ 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。

❸ [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）。

❹ 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、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。

デバッグ

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。

❶ 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。

❷ 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。

❸ [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。

❹ 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)

❺ 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 時までは更新を行わないように設定されています。)

❻ 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

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。

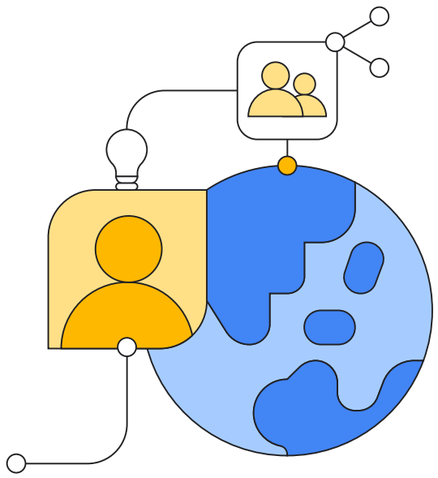
❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ [Google Update Policies] 下の [UpdatesSuppressdStart Hour] (時) [UpdateSuppressedStartMinute] (分) が指定した時間になっていることを確認します。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ [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。

❺ [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。

❻ [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。

❼ [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。

❽ [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。

❾ 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

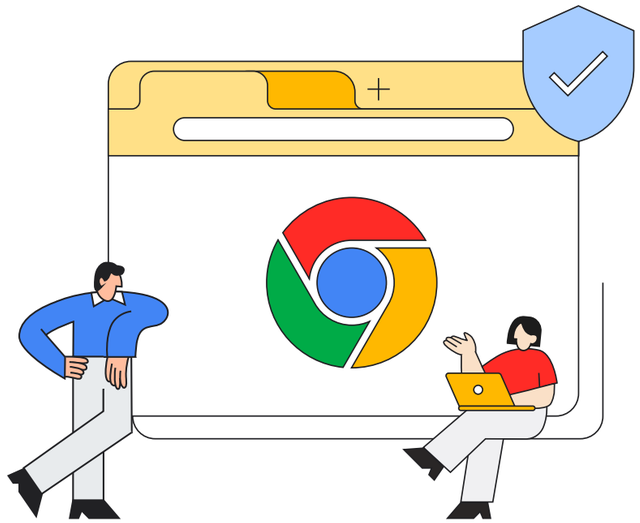
再起動の通知設定が指定された状態になっているか確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ [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。

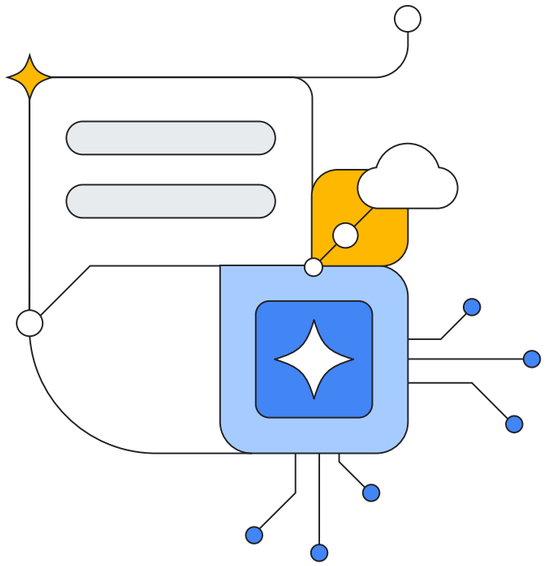
❶ 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。

❷ 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。

❸ [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。

❹ [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。

❺ 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

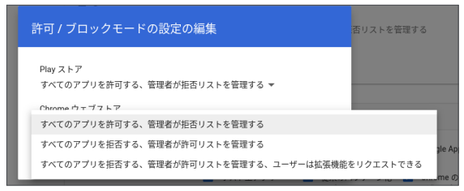
ブラウザのセキュリティと拡張機能を管理者がコントロール

❶ 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。

❷ 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。

❸ [許可 / ブロックモード] 内の編集をクリックします。

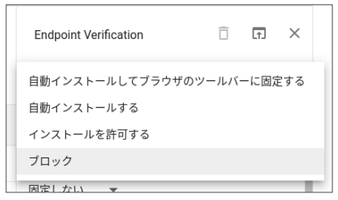
❹ ドロップダウン内から使用する設定を選択します。



❺ 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。

❻ 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。

❼ 編集した内容を保存し、設定は完了です。



拡張機能シリーズ

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。

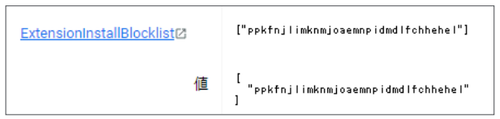
デバイスでの検証　拡張機能のポリシーをブラウザ上で確認する

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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷「 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。

❸ 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。



拡張機能シリーズ

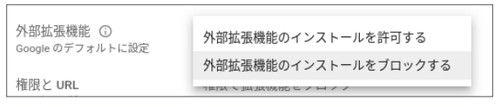
外部拡張機能のインストールをブロック「 BlockExternalExtensions 」

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。



❶ 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。

❷ 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。

❸ [外部拡張機能] の右のドロップダウンをクリックします。

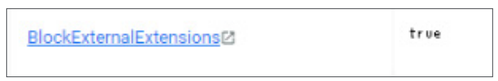
❹ ドロップダウン内から使用する設定を選択します。

❺ 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。



❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷「 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。

❸ 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。

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 」

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。

❶ 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。

❷ 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。

❸ [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。

❹ 必要に応じて設定を有効にします。

❺ 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

❶ 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

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷「 ShowHomeButton 」が [true] になっているか確認します。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ 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。

❺ 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。

❶ 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

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷「 HomepageLocation 」が設定した URL になっているか確認します。

❸ 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。

❶ 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。

❷ 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。

❸ [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。

❹ 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。

❺ 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。

❶ 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

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷「 RestoreOnStartupURLs 」が設定した URL になっているか確認します。

❸ 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。

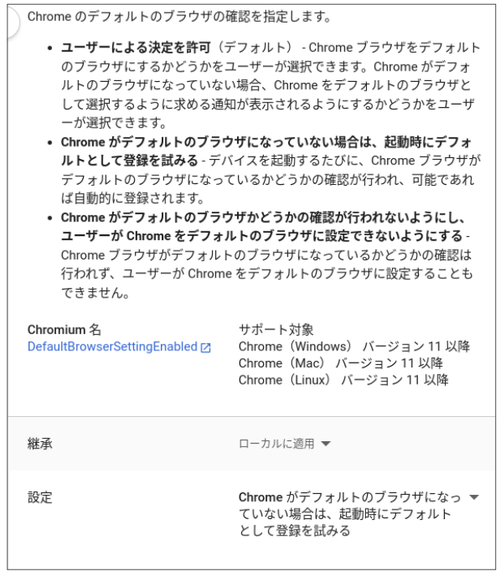
❶ 管理コンソールのホームページで [Chrome ブラウザ] → [設定] → [ユーザーとブラウザ] をクリックします。

❷ 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。

❸ [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。

❹ 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。

❺ 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。

❶ 管理された検証用ブラウザで “ chrome://policy ” へ移動します。

❷ [DefaultBrowserSettingEnabled] が　[true] になっているか確認します。

❸ 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。

❶ 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。

❷ [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。

❸ 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。

❹ 編集した内容を保存し、設定完了です。

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。

❶ 管理された検証用ブラウザで “chrome://policy” へ移動します。

❷ “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。

❶ 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。

❷ [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。

❸ 必要に応じて動作リストを選択し、設定します。

❹ 編集した内容を保存し、設定完了です。

作業効率シリーズ

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

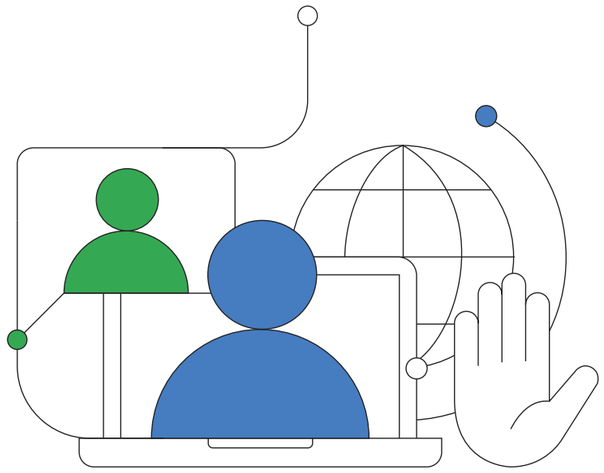
ブラウザのアイドル タイムアウト

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。

❶ 管理された検証用ブラウザで “chrome://policy” へ移動します。

❷ “IdleTimeout” および “IdleTimeoutActions” が設定した内容になっているか確認します。



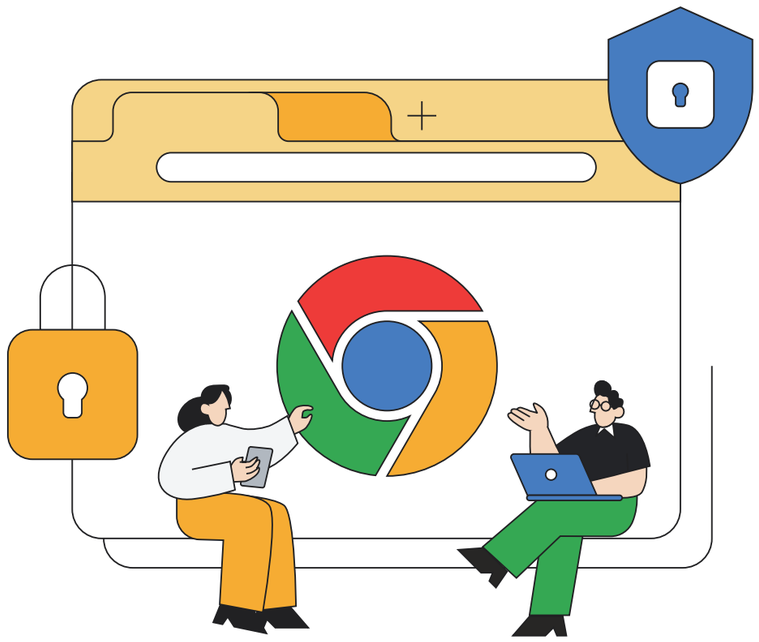
chrome enterprise

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。



基本設定

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 ...

ローカルマシン レベルのポリシー > **クラウドマシン レベルのポリシー** > **ローカル ユーザー レベルのポリシー** > **クラウド ユーザー レベルのポリシー**

例：グループポリシー（端末）、レジストリ設定、MDM

例：Chrome Enterprise Core（端末が所属する組織単位で適用）

例：グループポリシー（ユーザー）

例：Chrome Enterprise Core（ユーザーが所属する組織単位で適用）

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
❶ 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]
❷ 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。

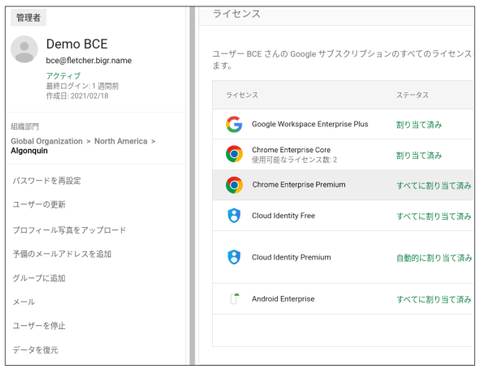
Chrome Enterprise Premium の機能はユーザーに Chrome Enterprise Premium のライセンスが付与されていないと機能しません。

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

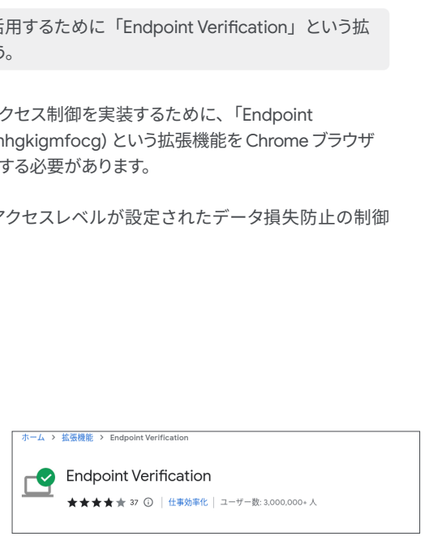
管理コンソールでの設定

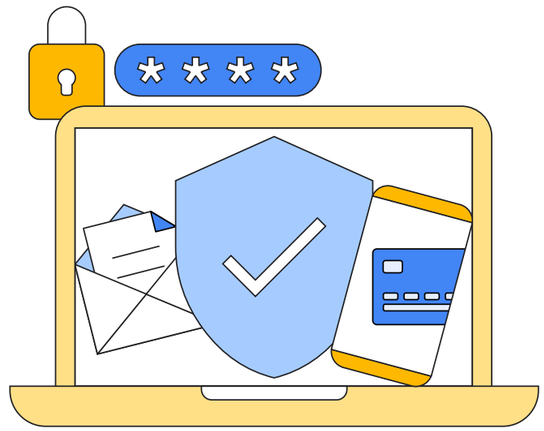
Chrome Enterprise Premium を設定する前に ...

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: callobklhcbilhphinckomhgkigmfocg) 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。

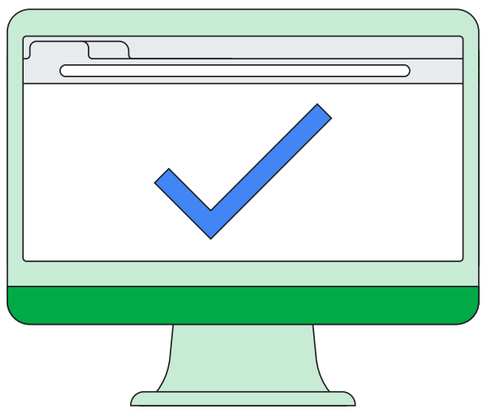
❶ 管理コンソールのホームページで左側の [Chrome ブラウザ] をクリックし、ドロップダウン内の [設定] をクリックします。

❷ [ユーザーとブラウザ] 次に ルート組織部門 を選択します。

❸ [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。

❹ [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。

❺ 編集した内容を保存し、設定は完了です。



「 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　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。

❶ 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。

❷ [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。

❸ [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。

❹ [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。

❺ 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。

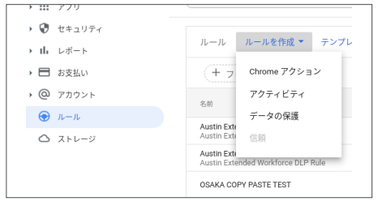
❻ 編集した内容を保存し、設定は完了です。

管理コンソールでの設定　次にルール設定

❼ 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。

❽ [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。

❾ 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。



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」

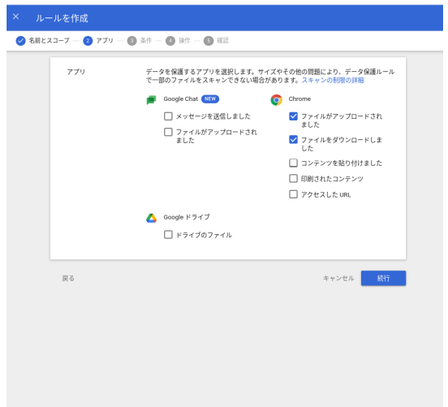
管理コンソールでの設定　次にルール設定

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。

シナリオ2

「 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。

❶ 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。

❷ [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。

❸ [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。

❹ [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。

❺ 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。

❻ 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

❼ 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。

❽ [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。

❾ 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。

シナリオ2

「URL のカテゴリによるフィルタリング」

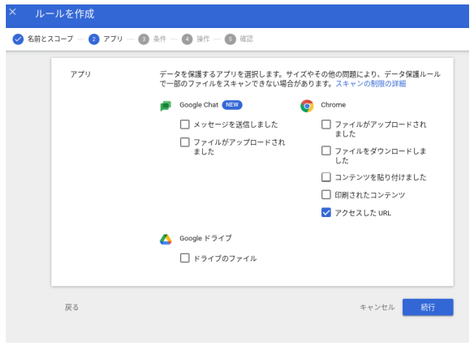
管理コンソールでの設定　次にルール設定

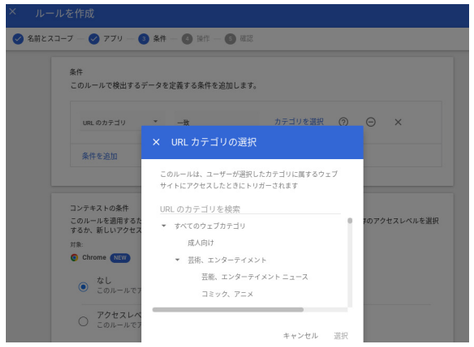
⑩ アクセスした URL　のチェックボックスをチェックし、続行をクリックします。

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。

シナリオ3

「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。

❶ 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。

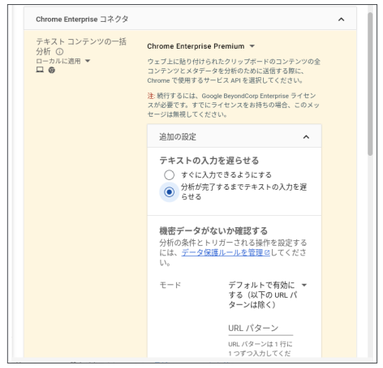
❷ [ユーザーとブラウザ] 次に設定を適用する組織部門、もしくはルートを選択します。

❸ [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。

❹ [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。

❺ 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。

❻ 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

❼ 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。

❽ [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。

❾ 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。

シナリオ3

「 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

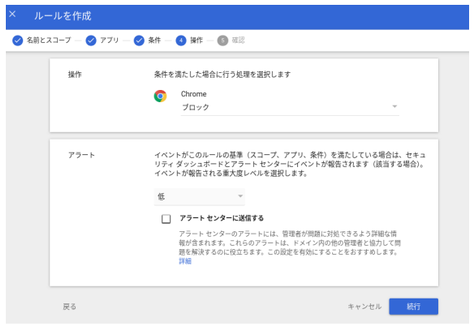
⑩ アクセスした URL のチェック ボックスをチェックし、続行をクリックします。

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。



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 」

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。

❶ 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。

❷ [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。

❸ [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。

❹ [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。

❺ 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。

❻ 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

❼ 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。

❽ [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

❾ 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

❿ こちらで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

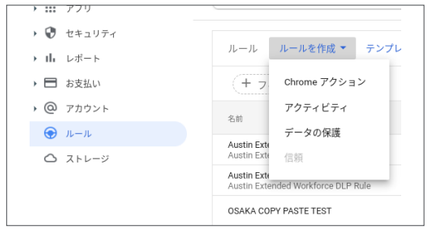
https://cloud.google.com/access-context-manager/docs/browser-attributes?hl=ja

管理コンソールでの設定　次にルール設定

⓫ 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。

⓬ [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。

⓭ 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。



「 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

⓮ 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。

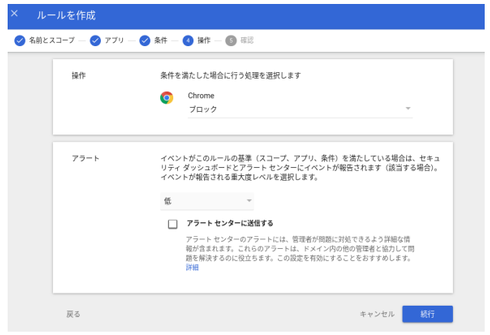
⓯ URL を選択し、生成 AI 系のサイトを手打ちします。

⓰ 先程設定したアクセスレベルを設定します。

⓱ Chrome での操作を設定し、続行をクリック

⓲ 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。

⓳ 以上で設定は完了です。



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 」

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。

❶ 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。

❷ [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。

❸ [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。

❹ [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。

❺ 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。

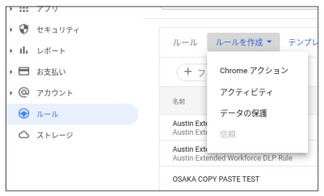
❻ 編集した内容を保存し、設定は完了です。

管理コンソールでの設定　次にルール設定

❼ 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。

❽ [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。

❾ 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。



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 」

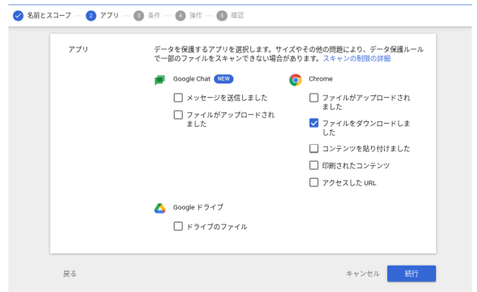
管理コンソールでの設定　次にルール設定

❿ 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。

⓫ 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。

⓬ 条件の追加を押し、ファイルサイズの条件を追加します。

⓭ 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。



⓮ Chrome での操作を設定し、続行をクリック

⓯ 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。

⓰ 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。

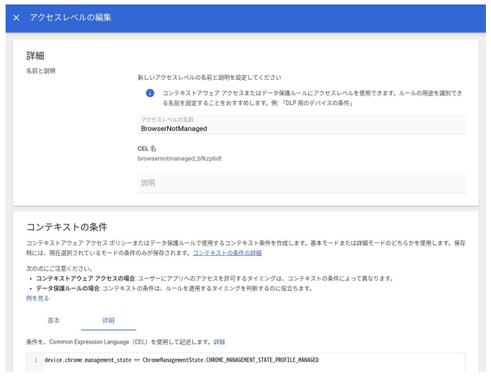
❶ 管理コンソールのホームページで左側の [セキュリティ] をクリックし、ドロップダウン内の [アクセスとデータ管理] [コンテキスト アウェア アクセス] をクリックします。

❷ [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。

❸ 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



管理コンソールでの設定　次にルール設定

❹ 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。

❺ [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。

❻ 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。

「 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

❼ Chrome「ファイルのダウンロード」を選択します。

❽ データの条件を設定します。（例：全ファイル→ 1 byte 以上）

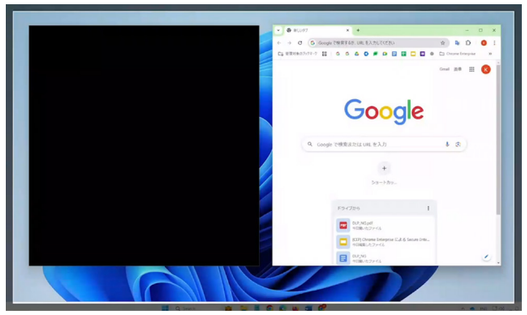
❾ 先程設定したアクセスレベルを設定します。

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_MAN AGED

●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。



シナリオ7

「 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。

❶ 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。

❷ [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。

❸ [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。

❹ [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。

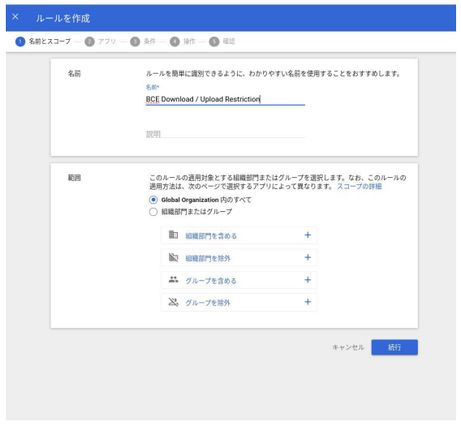
❺ 編集した内容を保存し、設定は完了です。

管理コンソールでの設定　次にルール設定

❻ 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。

❼ [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。

❽ 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。



シナリオ7

「 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

❾ 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。

❿ 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。

⓫ （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）

❿ Chrome での操作を「監査のみ」に設定し、続行をクリック

⓭「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。

⓮ 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。

⓯ 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。

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 」

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。

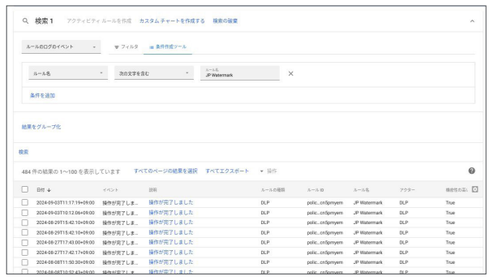
❶ 管理コンソールのホームページで左側の [ルール] をクリックします。

❷ [調査] をクリックします。

❸ 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。）

❹ 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。

❺ 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。



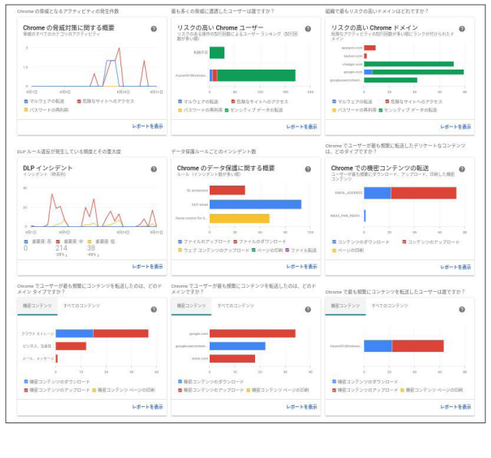
シナリオ8

「 DLP ルールをトリガーした アクションを調査する 」

管理コンソールでの設定

❻ セキュリティ→ セキュリティ センター → ダッシュボードに移動します。

❼ 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。