

特別版

できる[®]

Chrome ブラウザ

企業向け
導入と
運用管理

Chrome Enterprise Core / Chrome Enterprise Premium

活用編

清水理史&できるシリーズ編集部



※1:当社調べ ※2:大手書店チェーン調べ



インプレス

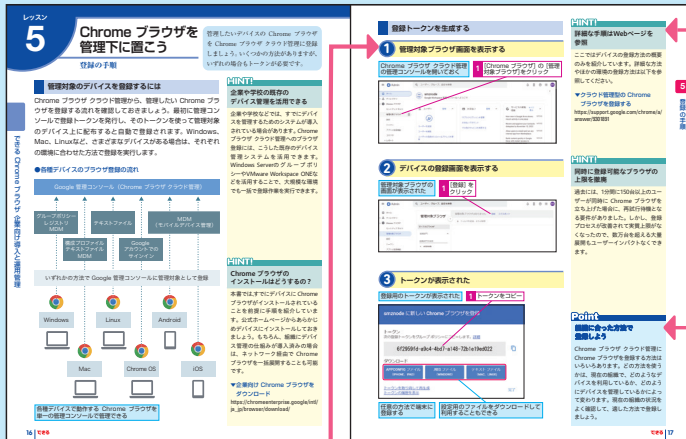
本書の読み方

レッスン

見開き2ページを基本に、
やりたいことを簡潔に解説

●やりたいことが見つけやすいタイトル
「〇〇をするには」や「〇〇ってなに？」など、「やりたいこと」や
「知りたいこと」がすぐに見つけられるタイトルがついています。

●機能名で引けるサブタイトル
「あの機能を使うにはどうするんだっけ？」そんな時に便利。
機能名やサービス名などで調べやすくなっています。



ヒント

レッスンに関連した、さまざまな機能を
紹介したり、一歩進んだ使いこなしのテ
クニックまで解説します。

右ページのつめでは、
知りたい機能で
ページが探せます。

Point

操作の要点をていねいに解説。レッスン
で解説している内容をより深く理解する
ことで、確実に使いこなせるようになります。

手順

必要な手順を、すべての画面とすべての
操作を掲載して解説します。

※ここで紹介している画面はイメージです。本書の内容と一部異なる場合があります。

●用語の使い方

本文中では、使用している用語は、基本的に実際の画面に表示される名称に則っています。

●本書の前提

本書では、「Windows 11」がインストールされているパソコンで、インターネットに常時接続されている環境を前提に画面を再現しています。

●本書に掲載されている情報について

本書に掲載されている情報は、2024年5月現在のものです。本書の発行後に、情報が変更されることもあります。

「できる」「できるシリーズ」は、株式会社インプレスの登録商標です。

本書に記載されている会社名、製品名、サービス名は、一般に各開発メーカーおよびサービス提供元の登録商標または商標です。

なお、本文中には™および®マークは明記していません。

Copyright © 2024 Masashi Shimizu and Impress Corporation. All rights reserved.

本書の内容はすべて、著作権法によって保護されています。著者および発行者の許可を得ず、転載、複写、複製等の利用はできません。

まえがき

社会的な情勢の変化や働き方の変化によって、組織のIT環境も大きく変わりました。かつてはパソコン上のソフトや社内のサーバーを利用し閉じた環境で仕事をしていたのが、今ではクラウドサービス主体へと切り替わり、パソコンだけでなく、スマートフォンやタブレットを使ってどこでも仕事ができるようになりました。

本書は、こうした新しい時代の働き方の中で、ユーザーが利用するエンドポイントとして重要な要素となっている「ブラウザ」を、組織で、より効率的かつ安全に活用する方法を紹介した冊子です。Google が提供する「Chrome ブラウザ」と、その管理ツールである「Chrome ブラウザ クラウド管理 (Chrome Enterprise Core)」そして「Chrome Enterprise Premium」を取り上げ、そのメリットや具体的な活用方法をイラストや実際の操作手順を交えて分かりやすく解説しています。

本書を手にとることが、新しい時代の働き方に合わせた効率的なIT環境を構築するためのヒントになれば幸いです。

2024年5月 清水理史

目 次

できる Chrome ブラウザ 企業向け導入と運用管理

① Chrome ブラウザを企業向けに導入する理由	＜進化するブラウザの役割＞	2
② 企業の生産性の中心となる Chrome ブラウザ	＜エンドポイントとしての Chrome ブラウザ＞	4
③ Chrome ブラウザの管理でできることを知ろう	＜Chrome ブラウザ管理の特徴＞	8
④ Chrome ブラウザ クラウド管理を導入しよう	＜設定方法＞	12
⑤ Chrome ブラウザを管理下に置こう	＜登録の手順＞	16
⑥ 管理画面を確認しよう	＜管理画面のメニューと使い方＞	20
⑦ Chrome ブラウザのセキュリティを強化するには	＜Chrome ブラウザのセキュリティ＞	22
⑧ 運用ニーズに沿ってChromeブラウザの更新を管理するには	＜Chromeブラウザの更新管理＞	26
⑨ 利便性と管理の両ニーズを満たす拡張機能の運用をするには	＜拡張機能の管理＞	30
⑩ 求められるセキュアなエンタープライズブラウザ	＜安全なブラウザの利用＞	32
⑪ セキュアなエンタープライズブラウザを使うには	＜Chrome Enterprise Premium＞	34
⑫ どんなリスクを防げるの？	＜Chrome Enterprise Premium の機能＞	36
⑬ エンタープライズブラウザを設定・管理するには	＜Chrome Enterprise Premium の設定とリスクの可視化＞	40

Chrome ブラウザを 企業向けに導入する理由

進化するブラウザの役割

業務遂行の中心となるモダンなブラウザ

メールやカレンダーの利用はもちろんのこと、ビデオ会議への参加、ビジネス文書の作成など、現代のビジネスシーンではブラウザや Web 会議を使って仕事を進めることが多くなりました。調査機関によるデータでは、現代のビジネスパーソンは勤務時間の71%をブラウザを使って仕事をしているという結果も発表されています。もはや、ブラウザは単なるWebページを表示するツールではなく、現代のビジネスシーンに欠かせない業務プラットフォームであり、クラウド上のさまざまなビジネスツールにつながるエンドポイントとして重要な役割を担っています。



リモートワークの普及にともなって、業務にブラウザを利用するシーンが増えてきました。組織として業務に利用するブラウザをどのように管理すればいいのでしょうか？

HINT!

実質的なスタンダードとなる Chrome ブラウザ

ブラウザとは、インターネット上にあるWebサイトを閲覧するときに使われるソフトウェアです。かつてブラウザは、さまざまなメーカーによって、独自のエンジンを利用する製品が開発されてきました。しかし、現在では、多くの製品が「Chromium」という Chrome で採用されているオープンソースのエンジンを採用しています。Chromium ベースのブラウザとしての先駆者である Chrome ブラウザは、現在のブラウザの事実上の業界標準となっています。

HINT!

エンドポイントって どういうこと？

エンドポイントは、通信ネットワークに接続された端末や機器のことを指します。リモートワーク、業務委託先の増加、組織が管理していないデバイスの急増などにより、エンドポイント セキュリティはますます制御が困難になっています。今やブラウザの役割は、企業における重要なデータの取り扱いやコラボレーションのほぼすべてを担う新たなエンドポイントへと進化してきています。Chrome ブラウザをエンドポイントとして捉えて企業内で運用すると、環境に依存しない一元管理が可能となります。

生産性とセキュリティを兼ね備えた Chrome ブラウザ

Chrome ブラウザは、使いやすさと高いセキュリティを兼ね備えたブラウザです。あらゆるパソコンやモバイル機器に対応するうえ、Google 検索などの統合された基本機能、同期やタブ整理などの機能により、さまざまな用途で手軽に利用できます。また、高度な基本設計とセーフブラウジングなどの多彩なセキュリティ機能によってインターネット上の脅威からユーザーを保護する安全なブラウザとなっています。



IT管理者の生産性も向上

ビジネスシーンでのブラウザの重要度が高まる一方で、そのブラウザを組織のルールに従ってどのように管理すればいいかは、IT管理者の頭を悩ませる課題のひとつです。Google では、こうしたブラウザ管理の課題を解決するためのツールとして、「Chrome ブラウザ クラウド管理」を無償で提供しています。あらゆる端末上の Chrome ブラウザに高度なセキュリティを適用したり、利用状況を視覚化したりと、さまざまな管理が可能です。



HINT!

どんなデバイスで使えるの？

Chrome は、さまざまなデバイスに対応しています。パソコンはもちろんのこと、スマートフォンやタブレットなどでも利用できるため、モバイル環境でも利用できます（詳細はレッスン②を参照）。端末間でデータをシームレスに同期できるので、異なる端末で作業を継続することもできます。

HINT!

サポートも受けられる

Chrome ブラウザでは、トラブルシューティングやベストプラクティスを参照したり、質問を投稿したりできるユーザーコミュニティなどの無償サポートを受けられます。また、一定の条件を満たす場合、Chrome ブラウザの導入や運用に関する有償サポートも受けられます。詳しくは付録を参照してください。

Point

Chrome ブラウザで ビジネスシーンを快適に

もはや仕事に欠かせない存在のブラウザをどのように活用し、どう管理していくかは組織にとって大きな課題です。事実上の業界標準で、多機能かつ安全、しかもクラウドでの管理が可能な Chrome ブラウザは、こうした現代のニーズに合った存在です。Chrome ブラウザを管理機能までフルに活用して、快適なビジネス環境を実現してみましょう。

企業の生産性の中心となる Chrome ブラウザ

エンドポイントとしての Chrome ブラウザ

業務で利用するWebアプリを快適に

Chrome ブラウザは、日常業務のほとんどすべてをカバーできるアプリケーションです。Gmail でメールの確認などといった日常的な操作をスムーズに実行したり、リンクからドキュメントやスプレッドシートを開いて文書を作り、それを共有して共同作業したりすることまでできます。テレワークの普及で増えてきたビデオ会議も、Google Meet はもちろんのこと、ほとんどのビデオ会議サービスに対応しており、快適に音声や映像を使ったコミュニケーションが可能です。インターネットにアクセスできるだけでなく、さまざまなクラウドサービスやWebアプリを同時に活用するための機能が統合されたシステム環境となっています。



Chrome ブラウザのメリットを具体的にみていきましょう。普段の業務で利用するユーザーの立場で考えると、どのようなブラウザが「良い」ブラウザなのでしょう。

HINT!

高いシェアを実現

2023年現在、Chrome ブラウザは日本だけでなく世界でも圧倒的に高いシェアを占めているブラウザです。ビジネスはもちろんのこと、個人利用や学習など、さまざまな用途で活用されています。

HINT!

多くのクラウドサービスやWebアプリの対応ブラウザに含まれる

Chrome ブラウザは、ビジネスシーンで利用されるクラウドサービスやWebアプリの推奨ブラウザに含まれています。このため、会計や人事など、多くの業務システムのブラウザとして利用可能です。

HINT!

システム要件を知りたい

各OSのバージョンは以下の通りです。

- Windows 10以降
- macOS Catalina 10.15 以降
- Linux
 - Ubuntu 18.04以降
 - Debian 10以降
 - openSUSE 15.2以降
 - Fedora Linux 32以降
- Android 7.0以降
- iOS 15以降

▼Chrome ブラウザのシステム要件

<https://support.google.com/chrome/a/answer/7100626?hl=ja>

進化するブラウザとクラウドサービス

Chrome ブラウザは、進化し続けているブラウザです。インターネット経由での自動アップデートによって、セキュリティ対策が強化されるだけでなく、新機能が追加され、より使いやすく進化し続けます。また、ブラウザからアクセスするクラウドサービスも内部的なアップデートによって進化を続けています。アクセスするだけで、いつでも最新の機能を活用した効率的な仕事ができるのが魅力です。また、管理者は業務の支障が出ないようなスケジュールでポリシーの更新管理をすることが可能なので、ユーザーはいつでも安心してセキュアな状態のブラウザを活用することができます。



HINT!

Google 検索を活用しよう

Chrome ブラウザではアドレスバーをクリック（またはWindowsで`Ctrl`+`L`キー、macで`command`+`L`キーを押す）して、キーワードを入力するだけで Google 検索が可能です。インターネットにあふれる情報の中から、知りたい情報を的確にピックアップすることができます。

HINT!

Googleドライブでクラウドにデータを保存できる

Chrome ブラウザを使えば、文書や表計算などのデータをインターネット上に保存して、どこからでも参照、編集できます。パソコンで作業中のデータを自動的に同期させることもできるうえ、スマートフォンからもデータを参照できるので生産性向上に役立てましょう。なお、利用には Google アカウントが必要です。

HINT!

翻訳や地図も利用できる

Chrome ブラウザでは、翻訳や地図の利用も簡単です。Google 翻訳で外国語のサイトを自動的に翻訳したり、Google マップで訪問先の住所から地図を表示してルートを検索したりすることが簡単にできます。

次のページに続く

時間や場所を選ばない多様な働き方にマッチ

Chrome ブラウザを利用すると、インターネットに接続できる環境であれば、どこからでも業務に必要なクラウドサービスにアクセスできます。また、昨今のWeb標準の技術の進化（HTML、CSS、PWAなど）によりWindowsやMacのネイティブなアプリケーションとWebアプリケーションの差がなくなってきており、Web上でできることが増えていることから環境に依存しない互換性の取れた業務アプリケーションのブラウザ上での活用が進んできています。このため、オフィスのパソコンはもちろんのこと、在宅勤務で自宅のパソコンで利用したり、モバイルパソコンやスマートフォンで移動中に利用したりと、多様な働き方を実現することができます。



HINT!

デバイスによっては標準で搭載されている

Androidスマートフォンや Chrome OS搭載パソコンなどでは、標準で Chrome ブラウザが搭載されています。大規模な展開を検討している場合は、Chrome ブラウザ搭載デバイスを選択することも検討してみるといいでしょう。

HINT!

教育機関でも多く採用されている

Chrome ブラウザや Chrome OS を搭載したデバイスは、教育の現場への普及も進んでいます。文部科学省が主導するGIGAスクール構想での採用例も多く、1人1台導入している公立小中学校の4割以上が Chrome OS を利用しています。また、iOSやWindows上で利用されるブラウザとしても Chrome ブラウザが利用されています。子供の学習環境としても広く利用されていることから、その使いやすさや安全性の高さがうかがえることでしょう。

HINT!

進化したWebアプリをビジネスに活用できる

Webページなどで使われている技術により開発されたアプリを、Webアプリと呼びます。Chrome ブラウザからもメールなどさまざまなサービスをWebアプリとして利用できますが、こうしたWebアプリは、Web標準の技術（HTML、CSS、PWAなど）の進化によって、通常のアプリと変わらぬ操作性や機能が提供されるようになってきました。現在では、ビジネスシーンで必要なアプリのほとんどをWebアプリとして利用できます。

あらゆるデバイスで利用できる Chrome ブラウザ

Chrome ブラウザは、Windows、Mac、Linuxなどのパソコンだけでなく、AndroidやiOS搭載のスマートフォンやタブレットでも利用できます。しかも、それぞれの端末でデータを同期できるので、いつでも、どこからでも同じ環境で作業できます。



仕事の効率を高める拡張機能

Chrome ブラウザには、ブラウザの機能を拡張する「拡張機能」と呼ばれるプログラムを追加できます。クラウドサービスにアクセスしやすくしたり、PDFなどの文書を扱いやすくしたりと、多彩な拡張機能から好みのものを選んでインストールできます。



HINT!

アップデートや拡張機能の利用を制御できる

ビジネスシーンでは、必ずしも最新バージョンを使いたいとは限りません。Chrome ブラウザ クラウド管理を利用すると、全社でバージョンを合わせたり、特定のバージョンに固定したりと、アップデートを制御することもできます。同様に、拡張機能の利用を制御することもできます。

HINT!

個人用のパソコンに Chrome ブラウザをインストールするには

在宅勤務などで自宅のパソコンで Chrome ブラウザを使いたいときは、以下のURLから簡単にビジネス向けの Chrome ブラウザをインストールすることができます。

▼企業向けChrome ブラウザのダウンロード

https://chromeenterprise.google/intl/ja_jp/browser/download/#windows-tab

Point

クラウド時代のビジネスプラットフォーム Chrome ブラウザ

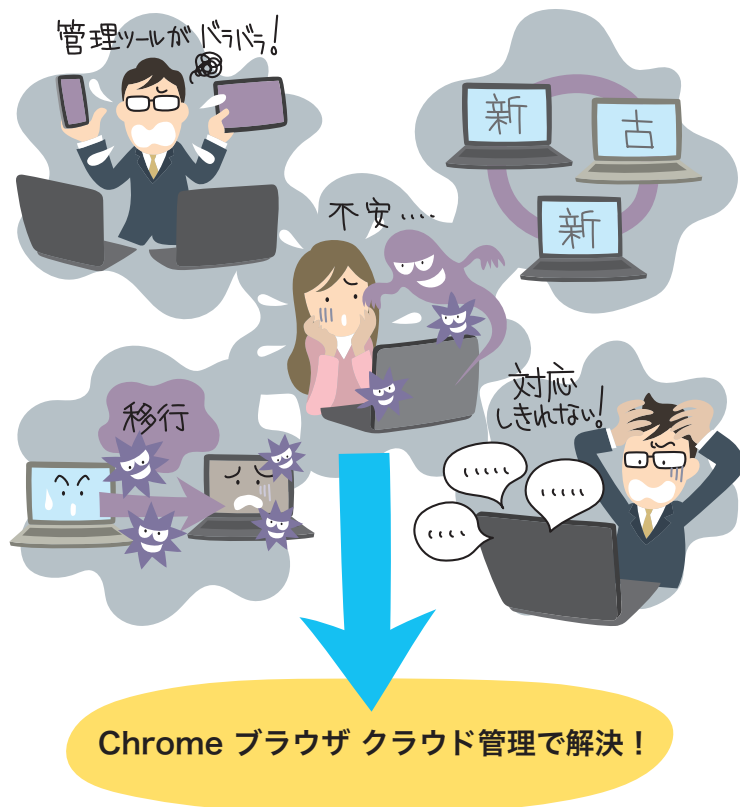
今やブラウザは、仕事のための中心的なツールとなっていますが、中でも Chrome は多くの企業で実際に業務に活用され、その利便性の高さや安全性が評価されているブラウザです。多くのプラットフォームで利用でき、クラウドサービスとの親和性が高く、新機能が次々に追加され、しかも拡張機能によってブラウザの枠を超えて生産性を上げることが可能です。さまざまなビジネスシーンで活用できるエンドポイントといえるでしょう。

Chrome ブラウザの管理で できることを知ろう

Chrome ブラウザ管理の特徴

ブラウザに対する運用の課題を解決

組織内のブラウザの管理に困っていませんか？ 管理ツールがパソコンとスマートフォンで別々だったり、更新が把握できずにバージョンが混在していたり、セキュリティ設定がずさんで情報漏えいのリスクに直面していたりと、IT管理者を悩ませる課題は多くあります。こうした課題を解決できるのが、「Chrome ブラウザ クラウド管理」です。Chrome ブラウザ クラウド管理は、Chrome Enterprise Core という無償の製品内で提供されている、組織内のブラウザを管理するシステムです。Chrome ブラウザ クラウド管理を用いて普段使っている Chrome ブラウザを、管理対象として登録します。これによりシンプルな管理画面で、高度な組織のセキュリティとコンプライアンスをブラウザ上で実現します。



Chrome ブラウザを導入するには、組織内のブラウザの状況を把握・管理する仕組みが不可欠です。「Chrome ブラウザ クラウド管理」でできることを見てみましょう。

HINT!

Internet Explorerの サポート終了をきっかけに

2022年6月16日で、マイクロソフトはInternet Explorerのサポートを終了しました。これまで Internet Explorerでしか動作しないサイトの利用などのためにブラウザの移行が進まなかった環境でも、これを機会に新たなブラウザ環境へと移行しています。サポートが切れたブラウザから、最新の Chrome ブラウザと Chrome ブラウザ クラウド管理によるセキュアな環境への移行を組織に提案してみましょう。なお、Chrome ブラウザ クラウド管理は機能名で、管理対象として登録することでポリシーの効いた Chrome Enterprise Core になります。普段使っているブラウザとは変わりがなく、ポリシー制御が効いた状態が整います。

HINT!

中小規模の環境でも 導入できる

Chrome ブラウザ クラウド管理は、導入が簡単で、管理の方法もシンプルです。このため、「ひとりIT管理者」や専任のIT管理者が不在の中小規模の環境でも不安なく導入できます。むしろIT管理に多くの時間やコストをかけられない環境こそ、Chrome ブラウザ クラウド管理による効率化を検討すべきでしょう。

高度なセキュリティでユーザーを保護

Chrome ブラウザ クラウド管理を利用すると、管理コンソールからの設定で、リモートから、デバイスにインストールされているブラウザのセキュリティ設定を制御できます。例えば、マルウェアやフィッシングサイトなどの悪意のあるサイトへのアクセスを警告するセーフブラウジングを有効化し、警告を無視したアクセスを禁止できます。管理者によっては情報漏えいを防ぐために企業ドメインで証明された Google アカウントに利用を限定したいというニーズもありますが、個人の Gmail アカウントの利用を禁止することで対策を講じることができます。このほか、パスワード保護やブラウザのセキュリティ状態の把握、拡張機能のセキュアな運用管理や展開なども可能です。



HINT!

パスワード保護が可能

Chrome ブラウザ クラウド管理では、ユーザーにパスワードの保存を許可するかどうかを制御できるだけでなく、パスワードの使い回しを検知したり、パスワードが漏えいしているかどうかをチェックし、変更を促したりすることもできます。

HINT!

ブラウザのセキュリティ状態の把握もできる

ブラウザのセキュリティ状態も簡単に把握できます。ブラウザのバージョンやデバイスの詳細情報、利用されている拡張機能など、組織におけるブラウザの利用状況を確認できます。さらに、セキュリティ上の課題やコンプライアンスの課題がないかをチェックできます。

HINT!

拡張機能のセキュアな運用

「拡張機能」とは、Chrome ブラウザに機能を追加するプログラムです。Chrome ブラウザ クラウド管理で管理されているブラウザには、拡張機能のインストールを制限することも可能です。許可リストで登録した拡張機能のみを利用可能にしたり、拡張機能を追加したいユーザーが管理者に許可を求めるフローを作成したりすることもできます。

次のページに続く

分かりやすくシンプルな運用が可能

Chrome ブラウザ クラウド管理では、さまざまなデバイスを統一された管理コンソールから管理できるシンプルなスタイルが魅力です。マルチOS上の Chrome ブラウザを一元管理することができ、一括ですべての端末にポリシーを適用することもできます。管理対象ブラウザとして登録されたデバイスを一覧表示したり、ユーザーやブラウザ向けの設定を変更したりと、初めてでも迷わず操作できます。



ブラウザの利用状況を可視化

デバイスの種類や Chrome のバージョン、アプリや拡張機能の使用状況など、組織全体の利用状況をレポートとして表示できます。もちろん、疑わしい拡張機能をブロックするなど、可視化された情報を元に次のアクションにつなげることもできます。



HINT!

モバイル向けのブラウザも管理できる

Chrome ブラウザ クラウド管理では、Windows、Mac、Linuxなどのパソコン向けだけでなく、AndroidやiOSなどのモバイル向けのブラウザも同様に管理できます。

HINT!

可視化して得られた情報を活用できる

可視化された情報は、組織のセキュリティ強化や生産性向上に役立てることができます。例えば、業務に必要なのに利用状況が低いアプリがある場合は、使い方を紹介するなどの啓発活動を計画すると効果的です。

HINT!

拡張機能も管理できる

Chrome ブラウザ クラウド管理では、ブラウザの設定だけでなく、ブラウザに追加できる拡張機能も管理できます。組織内でインストールを許可、または禁止する拡張機能を簡単に設定できます。

ニーズに合わせた管理の柔軟性を実現

Chrome ブラウザ クラウド管理を利用すると、数百を超える制御ポリシーで社内の組織体制や業務レベルなどのニーズに合わせた柔軟な管理が可能です。例えば、IT部門だけに最新のDev Channelのバージョンを提供するなど、組織内のブラウザの利用状況に合わせてバージョン管理や自動更新ポリシーを設定できます。また、役割ベースのアクセスを設定することで、部署単位で管理権限を変更したり、ユーザーからのリクエスト（利用許可申請）を受け付けてその都度、拡張機能の許可／拒否を決定したりすることができます。昨今ハイブリッドな働き方が増える中で個人所有の端末からブラウザで社内ツールにアクセスすることが増えていますが、個人のプロファイルと会社のプロファイルを分けて、会社で適用したポリシーが個人領域に影響しないようにデータを隔離することもできます。



HINT!

自動更新のスケジュールを制御できる

Chrome ブラウザ クラウド管理を利用すると、ネットワークのトラフィックを考慮して、業務時間以外に自動更新をスケジュールしたり、テストなどの目的で更新タイミングをずらして段階的に更新を適用したりすることができます。最新版の Chrome ブラウザをいつ、どのようなタイミングで、どこから展開するのかを制御できます。

HINT!

レガシーなブラウザもサポート

業務アプリで特定のバージョンのブラウザでしか表示できないクラウドサービスやWebアプリを利用している場合は、そのURLを指定して自動的にレガシーブラウザで表示するように制御できます。ブラウザの使い分けでユーザーが混乱することを避けられるでしょう。

Point

ブラウザ管理がスマートになる

Chrome ブラウザ クラウド管理を利用すると、ブラウザの状態、設定などをIT管理者が適切に管理できるようになります。セキュリティ設定などを一括で簡単に設定できるだけでなく、ニーズに合わせた柔軟な設定が可能です。組織内での Chrome ブラウザの利用状況が分かることで、セキュリティ設定の判断や次のIT戦略の計画に反映することなどができるのも大きな魅力です。

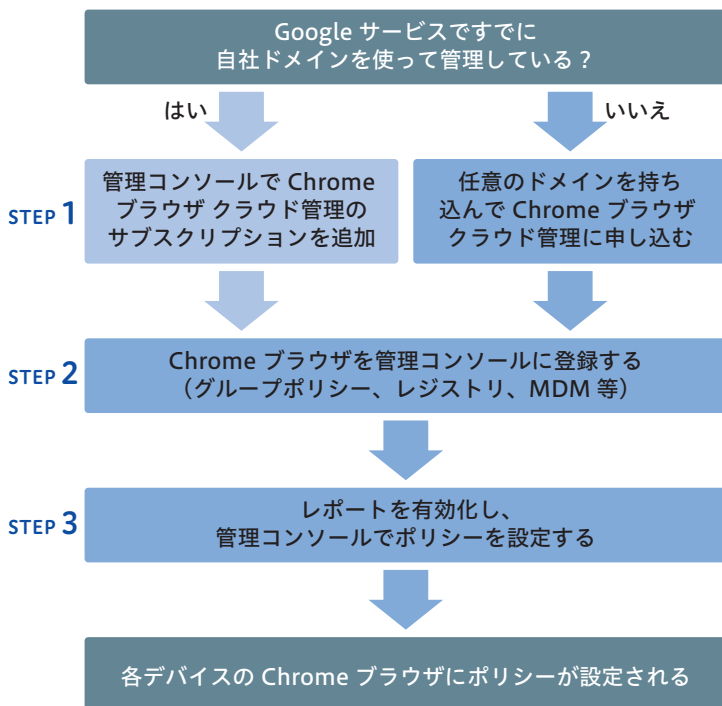
Chrome ブラウザ クラウド管理を導入しよう

設定方法

実際にChrome ブラウザ クラウド管理を使えるようにしてみましょう。申し込みから利用まで無償で使いはじめることができます。

Chrome ブラウザ クラウド管理の設定の流れ

Chrome ブラウザ クラウド管理を利用するには、管理対象のブラウザをドメインに関連付ける必要があります。すでに Google Workspace などを利用している場合は管理コンソールからサブスクリプションを追加することで管理可能になります。一方、Google のサービスを利用していない場合は、自社で管理しているドメインを使ってサインアップすることで、わずか数分で管理コンソールが利用可能になります。管理コンソールが利用可能になったら、管理したい Chrome ブラウザを登録することで設定したポリシーが適用されます。その後、詳細な情報（ポリシーの適用状況、拡張機能の活用状況、更新状況など）を取得するために管理コンソールで Chrome ブラウザのレポートを有効化し、Chrome ブラウザがポリシーを受け取ると組織全体のブラウザを管理できるようになります。



HINT!

登録方法の違いはあるが デバイスを問わず管理可能

Chrome ブラウザ クラウド管理では、パソコンやスマートフォンなどさまざまなデバイス上の Chrome ブラウザを管理できます。OSごとに登録方法が異なる場合がありますが、一度、登録してしまえば、どのデバイスも管理コンソールから統合管理が可能です。

HINT!

数百を超えるポリシーを 設定可能

Chrome ブラウザ クラウド管理では、管理対象となるデバイス上の Chrome ブラウザに対して、数百を超えるポリシーを適用できます。例えば、すべてのデバイスで統一されたホームページを設定したり、プロキシ設定をユーザーに許可するかどうかを設定する等のルールや制限項目をそれぞれポリシーとして反映します。

STEP1 : Chrome ブラウザ クラウド管理に申し込む

Google のサービスを利用していない場合は、まず自社で管理しているドメインを持ち込んで Chrome ブラウザ クラウド管理をセットアップする必要があります。以下のアドレスから管理者アカウントのメールアドレスを入力して申し込みをしましょう。申し込みが完了すると、管理者アカウントでサインインすることで Chrome ブラウザ クラウド管理の管理コンソールにアクセスできます。

▼Chrome ブラウザ クラウド管理に申し込む

<https://support.google.com/chrome/a/answer/9301420>

Chrome ブラウザ クラウド管理の申し込みページを開いておく

1 組織のドメインで利用しているメールアドレスを入力

2 [次へ]をクリック

3 管理者の名前や会社名、会社規模などの情報を入力

[続行] をクリックして申し込みを進める

申し込みが完了すると、「<https://admin.google.com>」から管理画面にアクセスできるようになる

HINT!

「Chrome ブラウザ クラウド管理」を追加する

申し込みの際に、サブスクリプションの追加画面が表示されます。Chrome ブラウザを管理するには、「Chrome ブラウザ クラウド管理」のサブスクリプション（無料）が必要です。

HINT!

ドメインの所有権の証明が必要

Chrome ブラウザ クラウド管理で、WindowsやMac、Linuxなどの端末で動作する Chrome ブラウザにポリシーを設定するには、ドメインの所有権を証明する必要があります。[アカウント]の[ドメイン]にある[ドメインの管理]からドメインの所有権を証明しましょう。組織管理しているDNSレコードに指定されたTXTレコードを追加して、ドメインの所有権を証明しましょう。

HINT!

Google Workspace 利用者は申し込み不要

すでに Google Workspace などの Google サービスを契約している場合は、Google Workspace の管理コンソールの [お支払い] の [サブスクリプション] で [Chrome ブラウザ クラウド管理] を追加することで、Chrome ブラウザの管理が可能になります。新たな申し込みは不要なので、次ページに進んでください。

次のページに続く

STEP2 : Chrome ブラウザを管理コンソールに登録する

次に、管理対象にしたい Chrome ブラウザを登録します。Chrome ブラウザクラウド管理では、管理対象以外のブラウザが登録されてしまうことを防ぐために登録時にトークンが必要です。管理コンソールで登録用のトークンを生成し、管理対象のデバイスにトークンを登録しましょう。トークンの配布方法は、いくつか用意されています。具体的なトークンの生成方法や配布方法については、次のレッスン⑤で解説します。

管理コンソールで登録用のトークンを生成する

smznode に新しい Chrome ブラウザを登録

トークン

次の登録トークンをグループ ポリシーにコピーします。 [詳細](#)

6f2959fd-a9c4-4bd7-a148-72b1e19ed022



ダウンロード

APPCONFIG ファイル
(IPHONE, IPAD)

.REG ファイル
(WINDOWS)

テキストファイル
(MAC, LINUX)

[トークンを取り消して再生成](#)
[トークンの履歴を表示](#)

完了



環境に合った方法でトークンを管理対象のデバイスに配信する
(Windows の場合)

数台～十数台

手動でデバイスのレジストリファイルを編集して登録

個別にデバイス上で reg ファイルを実行して登録

数十台～

Windows グループポリシーで一括登録

VMware Workspace ONE で一括登録

レジストリの一括適用

マスタイメージへのレジストリ適用

HINT!

MacやLinuxも管理できるの？

このページでは、主にWindows環境の登録方法を紹介していますが、MacやLinux上で動作する Chrome ブラウザも、同様にトークンの生成と配布という流れによって管理できます。MacやLinux環境でどのようにトークンを配布すればいいのかは19ページで詳しく解説します。

HINT!

一括配布/自動配布の環境を整えよう

管理対象のブラウザが多い環境では、デバイス管理システムを活用してトークンを配布する方が効率的です。台数が多くても一括でトークンを配布できるうえ、後から購入したデバイスや新しく加入したメンバーのブラウザなどにも自動的にトークンを配布できます。

STEP3: レポートを有効化し、管理コンソールでポリシーを設定

管理対象のブラウザを登録できたら、管理コンソールでレポートを有効にしましょう。これにより、デバイスから Chrome ブラウザのプロフィールや拡張機能などの情報、端末の情報などがアップロードされます。すべての準備が整ったら、最後にポリシーを設定します。登録した Chrome ブラウザに適用したい項目を選んで、その機能の有効／無効などを選択しましょう（詳細はレッスン⑥を参照）。設定が完了すると、ポリシーが管理対象の Chrome ブラウザに自動的に配信され、各種設定がユーザーのデバイス上で有効化されます。

Chrome ブラウザ クラウド管理の管理コンソールを開いておく

1 [Chrome ブラウザ]の
[設定]をクリック

2 画面を下に
スクロール



3 [ブラウザに関するレポート]の[管理対象ブラウザに関するレポート]をクリック

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

5 画面下の[保存]をクリック



HINT!

APIでより高度な管理も 利用可能

Chrome ブラウザ クラウド管理は、登録トークンと呼ばれる一意な文字列を端末が受け取ると自動で管理対象として登録されます。登録トークンは組織構造（OU）ごとに分けて発行することができ、再発行も可能です。どの組織単位でどの登録トークンが使われたか確認したいときは[Chrome ブラウザ]の下の[トークン]から確認できます。

▼Chrome Browser Enrollment Token APIを使用する

<https://support.google.com/chrome/a/answer/9949706?hl=ja>

Point

設定まで いくつかの分岐がある

Chrome ブラウザ クラウド管理を利用するまでには、いくつかの分岐があります。最初の大きな分岐は、Google Workspace などの Google のサービスを使っているかどうかです。使っている場合は、すでに管理コンソールにアクセス可能なので、Chrome ブラウザの登録に進みます。使っていない場合は、新規に管理コンソールのセットアップが必要です。2つ目の分岐は、登録用トークンの配布方法です。組織の規模やOSの種類、既存のデバイス管理などを考慮して最適な方法でトークンを配布しましょう。

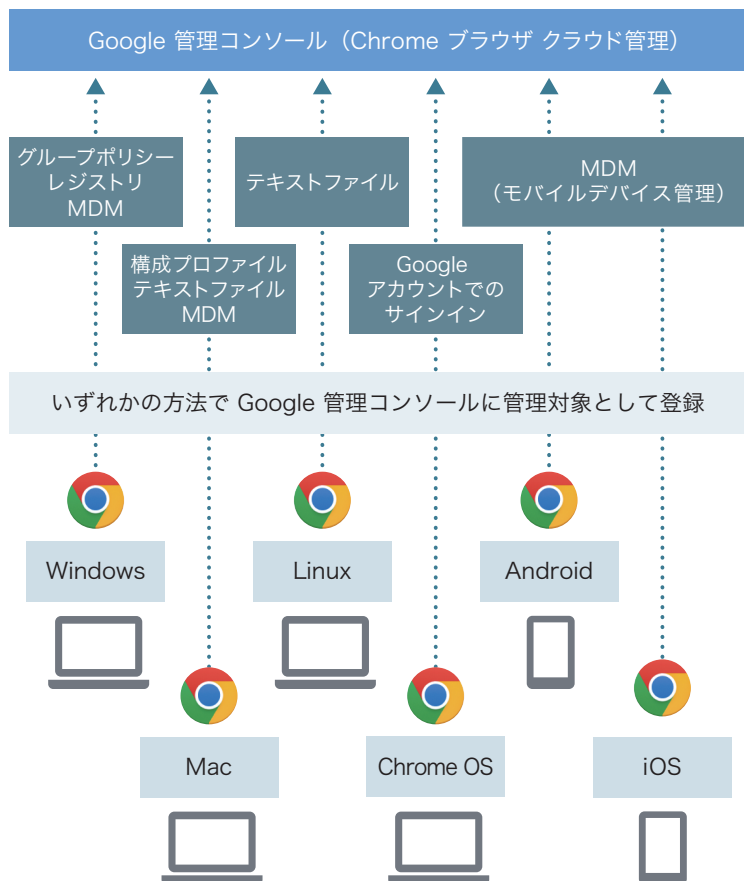
Chrome ブラウザを 管理下に置こう

登録の手順

管理対象のデバイスを登録するには

Chrome ブラウザ クラウド管理から、管理したい Chrome ブラウザを登録する流れを確認しておきましょう。最初に管理コンソールで登録トークンを発行し、そのトークンを使って管理対象のデバイス上に配布すると自動で登録されます。Windows、Mac、Linuxなど、さまざまなデバイスがある場合は、それぞれの環境に合わせた方法で登録を実行します。

●各種デバイスのブラウザ登録の流れ



各種デバイスで動作する Chrome ブラウザを
単一の管理コンソールで管理できる

管理したいデバイスの Chrome ブラウザを Chrome ブラウザ クラウド管理に登録しましょう。いくつかの方法がありますが、いずれの場合もトークンが必要です。

HINT!

企業や学校の既存の デバイス管理を活用できる

企業や学校などでは、すでにデバイスを管理するためのシステムが導入されている場合があります。Chrome ブラウザ クラウド管理へのブラウザ登録には、こうした既存のデバイス管理システムを活用できます。Windows ServerのグループポリシーやVMware Workspace ONEなどを活用することで、大規模な環境でも一括で登録作業を実行できます。

HINT!

Chrome ブラウザの インストールはどうするの？

本書では、すでにデバイスに Chrome ブラウザがインストールされていることを前提に手順を紹介しています。公式ホームページからあらかじめデバイスにインストールしておきましょう。もちろん、組織にデバイス管理の仕組みが導入済みの場合は、ネットワーク経由で Chrome ブラウザを一括展開することも可能です。

▼企業向け Chrome ブラウザを ダウンロード

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

登録トークンを生成する

1 管理対象ブラウザ画面を表示する

Chrome ブラウザ クラウド管理
の管理コンソールを開いておく

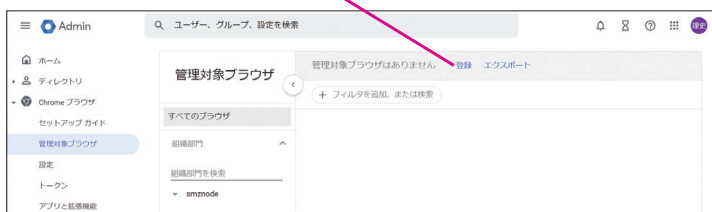
1 [Chrome ブラウザ] の [管理
対象ブラウザ] をクリック



2 デバイスの登録画面を表示する

管理対象ブラウザの
画面が表示された

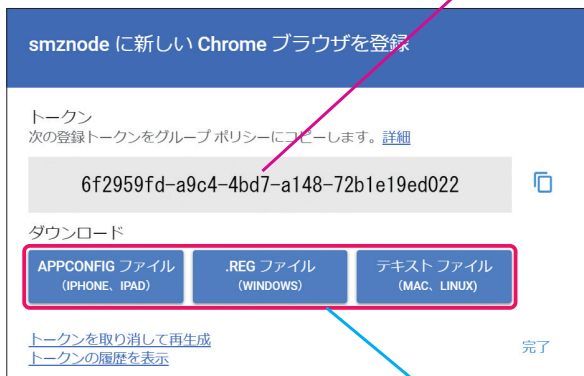
1 [登録] を
クリック



3 トークンが表示された

登録用のトークンが表示された

1 トークンをコピー



任意の方法で端末に
登録する

設定用のファイルをダウンロードして
利用することもできる

HINT!

詳細な手順はWebページを
参照

ここではデバイスの登録方法の概要
のみを紹介しています。詳細な方法
やほかの環境の登録方法は以下を参
照してください。

▼クラウド管理型の Chrome ブラウザを登録する

<https://support.google.com/chrome/a/answer/9301891>

HINT!

同時に登録可能なブラウザの
上限を撤廃

過去には、1分間に150台以上のユー
ザーが同時に Chrome ブラウザを
立ち上げた場合に、再試行待機とな
る要件がありました。しかし、現在
では登録プロセスが改善されて実質
上限がなくなったので、数万台を超
える大量展開もユーザーインパクト
なく実施可能です。

HINT!

手動登録もできる

Chrome ブラウザの登録は手動でも
可能です。小規模な環境など、デバ
イス管理ツールを利用していない場
合は、次のページで紹介するレジス
トリを利用してデバイスごとに個別
に手動設定できます。

次のページに続く

5

登録
の手
順

Windowsの場合

●方法1：グループ ポリシーを使用する

Windowsのグループポリシーを利用して登録できます。あらかじめ Chrome ポリシーテンプレートをインストール後、グループポリシーエディターで「管理用テンプレート」 - 「Google」 - 「Google Chrome」 - 「パソコンでのクラウド ポリシーの登録トークン」の「CloudManagementEnrollmentToken」に登録トークンを追加します。

●方法2：レジストリ ファイルを編集する

登録トークンをWindowsのレジストリに直接書き込みます。レジストリエディタを利用して、「HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Google¥Chrome」の「CloudManagementEnrollmentToken」に登録トークンを登録します。

●方法3：regファイルを利用する

レジストリ情報が書き込まれたファイルを使って登録トークンをレジストリに書き込みます。[.reg ファイルをダウンロード] をクリックしてダウンロードした.regファイルを実行すると、自動的に登録トークンが追加されます。

●方法4：VMware Workspace ONEを利用する

デバイス管理ソリューションの「VMware Workspace ONE」を使用して、登録トークンの生成と Chrome ブラウザの登録ができます（次ページ1つ目のHINT!を参照）。

HINT!

利用規約の画面が表示されたら

トークンの発行時に利用規約の画面が表示されることがあります。表示されたら、内容をよく読んで同意してから、作業を進めましょう。

HINT!

マスタージメージに書き込んで展開することもできる

Windowsの場合、マスタージメージを使って大量展開することも可能です。Chrome ブラウザをインストールし、かつ登録キーをレジストリに書き込んだ状態でSysprepを使ってマスタージメージを作成すれば、このマスタージメージから作成したパソコンを自動的に管理対象ブラウザとして登録できます。

既存のポリシーとの併用が可能

以下の優先順位でポリシーが適用され、後から優先順位の変更も可能です。

※例：既存のグループポリシーを据え置きして、拡張機能の管理だけChromeブラウザ クラウド管理で運用

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 ブラウザ クラウド管理
（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 ブラウザ クラウド管理
（ユーザーが所属する組織単位で適用）

●優先順位を変更するポリシー

- ・ CloudPolicyOverridesPlatformPolicy
- ・ CloudUserPolicyOverridesCloudMachinePolicy



Macの場合

Macの場合、Apple プロファイル マネージャなどでプロファイル（plistファイル）を作成して登録したり、登録キーを記載したテキストファイルを配置（/Library/Google/Chrome/）したりすることで登録できます。大量展開が必要な場合は、Jamf Pro やVMware Workspace ONEなどのデバイス管理ソリューションを利用することで展開できます。

▼Jamf Pro (macOS) でブラウザを登録する

<https://support.google.com/chrome/a/answer/9771882>

Linuxの場合

Linuxの場合、登録トークンが記載されたテキストファイルを使って登録します。「CloudManagementEnrollmentToken」という登録トークンのみが記述されたファイルを「/etc/opt/chrome/policies/enrollment」に保管します。

Androidデバイスの場合

Android端末は、ポリシーをデバイスに配布するMDM（モバイルデバイスマネジメント）ソリューションが必要です。VMware Workspace ONE、MobileIron、SOTI、Intuneなど、AppConfigに対応したMDMソリューションを利用して Chrome ブラウザを登録しましょう。詳しくは以下を参照してください。

▼Android デバイスを対象に Chrome ブラウザ クラウド管理を設定する

<https://support.google.com/chrome/a/answer/11480811>

iOSデバイスの場合

iOSデバイスの場合も、AppConfigに対応したMDMソリューションが別途必要になります。Jamf、VMware Workspace ONE、Intuneなどを利用して登録しましょう。詳しくは以下を参照してください。

▼iOS を対象に Chrome ブラウザ クラウド管理を設定する

<https://support.google.com/chrome/a/answer/10377492>

HINT!

VMware Workspace ONEを利用する場合は

VMware Workspace ONEは、VMware社が提供する管理ソリューションです。組織でVMware Workspace ONEが使われている場合は、以下を参照して設定してください。

▼VMware Workspace ONE でブラウザを登録する (Windows と macOS)

<https://support.google.com/chrome/a/answer/9793780>

HINT!

登録したブラウザの削除や 再登録

登録したブラウザは、管理コンソール（次のレッスンを参照）から削除することができます。また、削除後、もう一度、このレッスンの方を実行することで再登録することができます。また、部署単位などでグループ分けしてブラウザを管理している場合は、登録後に所属するグループを移動することもできます。

Point

組織に合った方法で 登録しよう

Chrome ブラウザ クラウド管理に Chrome ブラウザを登録する方法はいろいろあります。どの方法を使うかは、現在の組織で、どのようなデバイスを利用しているか、どのようにデバイスを管理しているかによって変わります。現在の組織の状況をよく確認して、適した方法で登録しましょう。

管理画面を確認しよう

管理画面のメニューと使い方

管理コンソール

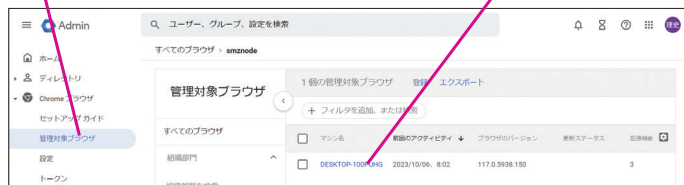
Chrome ブラウザ クラウド管理の管理画面は、Google 管理コンソールの [Chrome ブラウザ] にある [管理対象ブラウザ] からアクセスできます。以下のアドレスから Google 管理コンソールにアクセスし、管理者ユーザーでサインインしましょう。

▼Google 管理 コンソール

<https://admin.google.com/>

Chrome ブラウザ クラウド管理の管理コンソールを開いておく

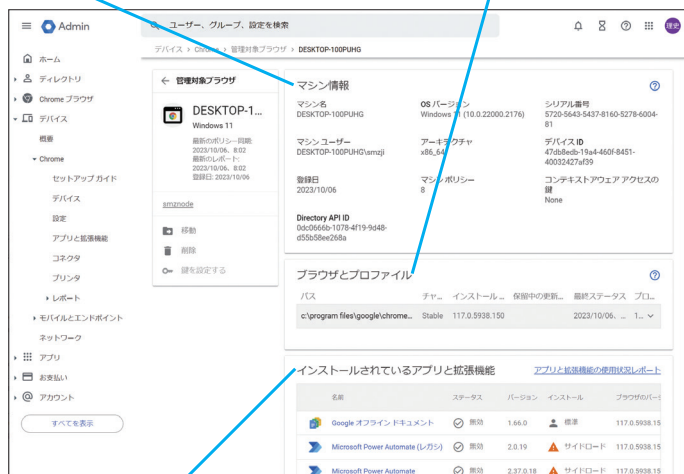
1 [管理対象ブラウザ]をクリック 2 登録されたマシンをクリック



管理対象のブラウザやマシンの詳細な情報が表示された

◆マシン情報
OSのバージョンなどを確認できる

◆ブラウザとプロフィール
Chrome ブラウザのバージョンを確認できる



◆インストールされているアプリと拡張機能
Chrome ブラウザにインストールされているアプリや拡張機能を確認できる

管理対象の Chrome ブラウザを登録できたら、管理コンソールからデバイス上の Chrome ブラウザを管理できます。管理コンソールの使い方を見ましょう。

HINT!

Google Workspace の場合は

Google Workspace など、Google のサービスをすでに利用している場合は、Gmail など既存のサービスにサインイン後、アプリの一覧から [管理]を選択することでも管理コンソールにアクセスできます。

HINT!

どこからでも管理できる

管理コンソールは、クラウド上で提供されているため、インターネットに接続できるデバイスであれば、どこからでもブラウザを使ってアクセスできます。テレワークなどで社外にいる場合でも管理が可能です。

HINT!

レポートを有効にしておこう

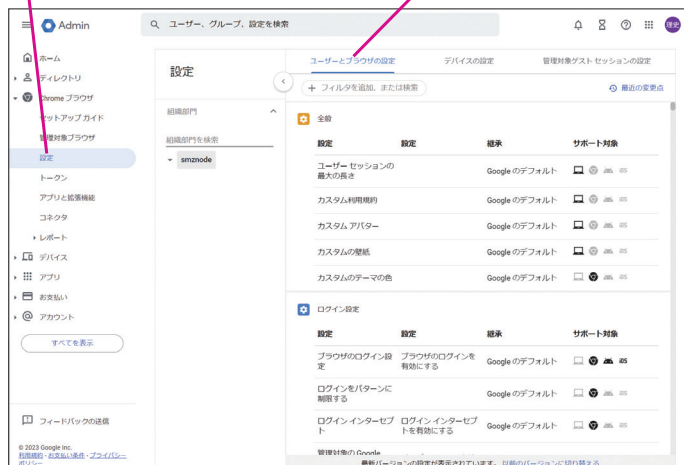
デバイス上の管理対象の Chrome の情報を収集するには、管理コンソールでレポートを有効にする必要があります。15ページで紹介している方法でレポートを有効にしておきましょう。

Chrome 管理画面

Chrome ブラウザ クラウド管理の画面を見てみましょう。Chrome ブラウザの管理は [Chrome ブラウザ] にまとめられています。[設定] や [アプリと拡張機能] や [コネクタ] などのメニューをクリックすることで、それぞれの管理画面にアクセスできます。Chrome ブラウザのポリシーを設定するには、[設定] の [ユーザーとブラウザの設定] を利用します。

1 [Chrome ブラウザ] の [設定] をクリック

2 [ユーザーとブラウザの設定] タブをクリック



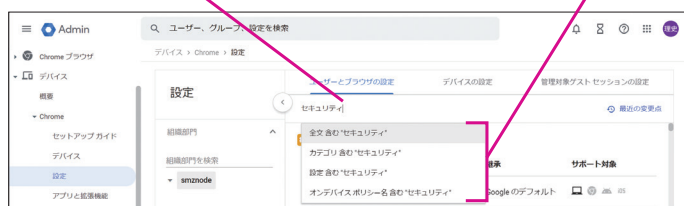
設定可能なポリシーの一覧が表示された

管理項目を検索するには

Chrome ブラウザ クラウド管理には、たくさんの管理項目が用意されています。目的の管理項目が見つからないときは、フィルタを追加して項目を絞り込むといいでしょう。キーワードを入力すると、対象とする範囲が表示されます。標準では全文を対象に絞り込みが実施されますが、カテゴリなど特定の部分のみを対象に絞り込むこともできます。

1 検索したいキーワードを入力

2 カテゴリなど、特定の部分のみを対象に絞り込む



「セキュリティ」を含むカテゴリや設定だけに絞り込むことができる

HINT!

どんな設定ができるの？

ポリシーでどのような設定をするかは、組織のセキュリティやガバナンスの方針によって異なります。Chrome ブラウザ クラウド管理の画面では、Chrome ブラウザ向けに以下のようなカテゴリのポリシーを適用できます。

●主なカテゴリ

- ・ログイン設定
- ・モバイル
- ・アプリと拡張機能
- ・セキュリティ
- ・セッションの設定
- ・ネットワーク
- ・起動
- ・コンテンツ
- ・ユーザーエクスペリエンス
- ・アドレスバーの検索プロバイダ
- ・以前のサイトの互換性
- ・ブラウザに関するレポート
- ・Chrome のセーフ ブラウジング
- ・Chrome Enterprise コネクタ
- ・Chrome の更新
- ・Chrome のバリエーション

Point

組織内の Chrome ブラウザをまとめて管理できる

Chrome ブラウザ クラウド管理を利用すると、組織内に存在する Chrome ブラウザの現在の状況を簡単に把握できます。どのバージョンがどれくらいあり、どのように使われているのかを判断できるので、セキュリティ対策などの方針を決める際の参考になります。もちろん、Chrome ブラウザの設定を一括で変更することもできるので、組織のルールに従った使い方をユーザーに強制できます。セキュリティ被害につながりそうな使い方を禁止することで、安全性を高めることができるので、ぜひ活用してみましょう。

Chrome ブラウザのセキュリティを強化するには

Chrome ブラウザのセキュリティ

安全にインターネット上のリソースを活用する

「インターネット上のさまざまなサービスを積極的に活用したいが、セキュリティが心配……」と考えている管理者も多いことでしょう。このため、まずは Chrome ブラウザのセキュリティ機能をしっかりと有効化しておくことが大切です。安全ではない可能性があるサイトを警告する「セーフ ブラウジング」を強化したり、パスワードの再利用を禁止したり、危険なファイルのダウンロードを禁止したりしておきましょう。また、セキュリティセンターで危険なログを確認することも重要です。



実際に Chrome ブラウザ クラウド管理を使って、Chrome ブラウザを管理してみましょう。まずは、安全に Web ページを閲覧するための設定を紹介します。

HINT!

設定項目を一通り確認してみよう

Chrome ブラウザ クラウド管理には、たくさんのポリシーが用意されています。まずは、どのようなポリシーがあるのか、全体をざっと眺めておくといいでしょう。もちろん、すべての設定を使う必要はありません。組織に合った項目だけを選んで設定しましょう。

HINT!

カテゴリ分けされている

設定項目はカテゴリごとに分類されています。セキュリティ関連の項目は、主に「セキュリティ」や「セーフブラウジング」などの項目に分類されています。まずは、これらの項目を確認してみましょう。

HINT!

セーフ ブラウジングの保護強化機能とは

Chrome ブラウザに搭載されているセーフ ブラウジング機能では、「保護強化機能」「標準保護機能」「保護なし」の3つのレベルを選択できます。最上位の「保護強化機能」では、最新情報を元にしたリアルタイムのチェックや、AIによる予測を元に危険なサイトやファイル、拡張機能を検知できます。10分おきにドメインを変更するなど、既知のデータベースからの検知を逃れようとする悪意のあるサイトも検知可能です。

セーフブラウジングの設定をしよう

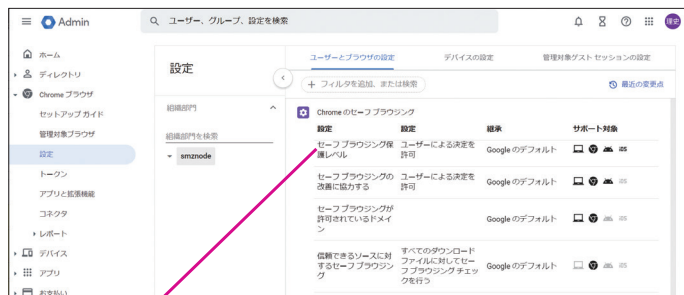
セーフ ブラウジングは、マルウェアなどの不正なソフトウェアやフィッシング詐欺などの可能性があるサイトなど、安全ではない可能性があるサイトについて警告する機能です。標準で有効化しておきましょう。ここでは標準モードで有効化しましたが、よりセキュリティを強化できる強化モードで有効化することもできます。このほか、[Chrome のセーフ ブラウジング]のカテゴリでは、許可するドメインを登録したり、ダウンロードされるファイルの危険性を警告したりすることもできます。

1 セーフ ブラウジングの各種設定ポリシーを表示する

[Chrome のセーフ ブラウジング]のカテゴリを表示しておく

セーフ ブラウジングに関するさまざまな設定が用意されている

ここでは[セーフ ブラウジング保護レベル]を設定する



1 [セーフ ブラウジング保護レベル]をクリック

2 セーフ ブラウジングの保護レベルを指定する

ここではセーフ ブラウジングを標準モードで有効に設定する

1 [設定]で[セーフ ブラウジングを標準モードで有効にする]を選択



2 [保存]をクリック

HINT!

ダウンロードを制限するには

[ダウンロードの制限]を利用すると、ユーザーによるファイルのダウンロードを制限できます。すべてのファイルを全面的にブロックすることもできますし、不正なファイルや危険性のあるファイルだけをブロックすることもできます。環境に応じて設定を選択しましょう。

HINT!

許可するドメインを登録できる

セーフ ブラウジングによって、組織内のWebサイトなどでも警告が表示されるようになってしまった場合は、組織のドメインを許可するドメインに登録しておくといでしょう。[セーフ ブラウジングが許可されているドメイン]のポリシーに組織のドメインを登録しておくことで、セーフ ブラウジングでの警告を回避できます。

HINT!

広告をブロックする

Web サイトによっては、煩わしいと感じられるほどに、たくさんの広告が表示されることがあります。広告をブロックしたい場合は、[Chrome のセーフ ブラウジング]の[煩わしい広告を含むサイト]の構成で、広告をブロックすることもできます。

次のページに続く

セキュリティ関連の設定を強化しよう

インターネット上には、ポップアップ表示やコマンドラインフラグ（コマンドオプション）などの手法を悪用する不正なサイトもあります。こうした危険から身を守るには、[セキュリティ] カテゴリや [コンテンツ] カテゴリの設定を活用しましょう。パスワードの不正使用に関するアラートを常に表示するようにしたり、ポップアップを禁止したりできます。

1 パスワードに関するアラート表示を設定する

パスワードに関するアラートを常に表示するように設定する

[セキュリティ]の[不正使用されたパスワードに関するアラート]の項目を表示しておく



1 [不正使用されたパスワードに関するアラートを非表示にすることを拒否]を選択

2 [保存]をクリック

2 ポップアップのブロックを設定する

すべてのポップアップをブロックする設定にする

[コンテンツ]の[ポップアップ]の項目を表示しておく



1 [すべてのポップアップをブロックする]を選択

2 [保存]をクリック

HINT!

セーフサーチの設定もできる

[コンテンツ]カテゴリの「セーフサーチと制限付きモード」を利用すると、成人向けサイトなどを検索結果から除外できます。教育機関などで未成年が Chrome ブラウザを利用する場合は有効にしておくことをおすすめします。

HINT!

ポップアップを許可するには

組織内のサイトなどでポップアップを許可したい場合は、手順2の画面で [これらのサイトのポップアップを許可する] の欄に許可したいサイトを登録しておきましょう。

HINT!

特定の URL をブロックするには

[コンテンツ] カテゴリにある [URL のブロック] を利用すると、特定の URL のサイトへのアクセスをブロックできます。利用を禁止したいサイトや確実に危険であることがわかっていてるサイトなどは、この方法でブロックするといいいでしょう。

Chrome ブラウザには、インターネット上に存在するさまざまな危険から端末を保護するための機能が搭載されています。しかし、こうした機能も「有効」になっていないと意味がありません。[セキュリティセンター] や各種ログを活用して、設定ミスやユーザーの行動などの状況を定期的にチェックしましょう。

運用ニーズに沿って Chrome ブラウザの更新を管理するには

Chrome ブラウザの更新管理

ユーザー作業の中断やバージョン固定などの悩みを解決

組織にたくさんの端末がある場合、ブラウザの更新を管理するのは大変です。業務中の更新によってユーザーの作業が中断されたら困るうえ、特定のバージョンでないと困る業務などもあり、「更新」と言っても、さまざまな点に気を配る必要があります。Chrome ブラウザ クラウド管理では、こうした更新の悩みも解決できます。Chrome ブラウザの自動更新機能を制御して、スケジュールを調整したり、バージョンを指定したり、キャッシュによってネットワークの混雑を避けたりと、組織のニーズに合わせて更新を制御できます。



ブラウザを安全に使うにはソフトウェアの更新を適切なタイミングで、素早く適用することが大切です。ニーズに合わせて更新を制御する方法を見てみましょう。

HINT!

標準では自動更新される

Chrome ブラウザは標準で自動更新が有効になっています。これにより、特に更新を意識しなくても、脆弱性や不具合などに迅速に対応できるうえ、新機能もいち早く利用できます。現在のバージョンは、Chrome ブラウザの [設定] の [Chrome について] で確認できます。モバイルデバイスの場合は、MDMからのバージョンアップまたは、ユーザー自身でのバージョンアップが必要です。

HINT!

更新内容や更新履歴を確認するには

Chrome ブラウザの更新内容や過去の更新履歴は、ヘルプ センターに掲載されています。ヘルプセンターで「リリースノート」と検索すると、最新版の更新内容が記載されたリリースノートを確認できます。また、「以前のリリースノート」で過去の更新履歴を確認できます。

▼Chrome Enterprise and Education ヘルプ センター

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

ニーズに沿ったタイミングで自動更新を配信しよう

Webシステムの対応が最新の更新に対応していない場合に、Chrome の自動更新のバージョンをピン留めして、対応が完了したタイミングで自動更新を取りに行くようにタイミングを制御することが可能です。例えば、[目的のバージョンのプレフィックス]を利用すると特定バージョン以降の自動更新を防ぎ、現在のバージョンでピン留めできます。また、問題が後から発覚した場合にも、[目的のバージョンにロールバック]を利用することで、すでに更新済みの場合も以前のバージョンに戻すことができます。

1 更新の設定画面を表示する

[Chrome の更新] カテゴリを表示しておく

Chrome ブラウザの更新に関するさまざまな項目を設定できる



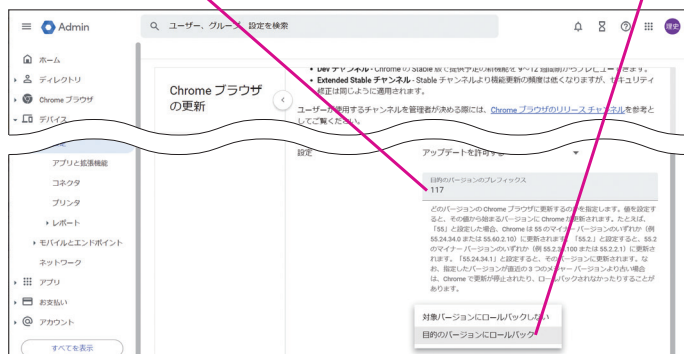
ここではバージョンを固定する

1 [Chrome ブラウザの更新] をクリック

2 目的のバージョンにピン留めする

1 利用したいバージョンを指定

2 [目的のバージョンにロールバック]を選択



3 画面下の[保存]をクリック

HINT!

組織内で使われているバージョンを把握するには

組織内で使われている Chrome ブラウザのバージョンを把握したいときは、[レポート]の[バージョン]でデバイスごとのバージョンを一覧表示できます。

HINT!

バージョンを制御するには

特定バージョンの Chrome ブラウザを利用する方法としては、手動でインストーラーファイルを配信する方法もあります。ただし、管理工数が増大することと、最新のセキュリティアップデートが配信されないためお勧めできません。運用効率化と安全性を高めるために、基本的には自動更新を設定しつつ、新しいバージョンに切り替えるタイミングを制御する方法を検討しましょう。

HINT!

部門単位で管理できる

管理コンソールの[ディレクトリ]にある[組織部門]を利用すると、組織の部門ごとに、更新方法などを個別に管理できます。部門ごとにバージョンを使い分けたいときなどに活用するといでしょう。

次のページに続く

ユーザーの利便性を考慮して更新スケジュールを決めよう

Chrome ブラウザの更新は、重要なセキュリティ関連の更新が含まれていることもあるため、なるべく早く適用するのが理想です。しかし、業務のピーク時間などに更新が実行されると、ユーザーの作業が中断されてしまうこともあります。こうした事態を避けるには、[自動更新のチェックを停止する]という設定を活用しましょう。指定した時刻から一定時間、一時的に自動更新のチェックを停止できます。また、[自動更新のチェック間隔]で更新をチェックするタイミングを遅らせることもできます。

1 自動更新のチェック時間を設定する

自動更新を一時的に停止する時間を構成する

[自動更新のチェックを停止する]の設定画面を開いておく

1 自動更新のチェックを停止する開始時間を設定



2 自動更新のチェックを停止する時間(分)を設定

3 画面下の[保存]をクリック

2 自動更新のチェック間隔を設定する

自動更新をチェックする間隔を調整する

[自動更新のチェック間隔]の設定画面を開いておく

1 更新をチェックする間隔(分)を設定



2 [保存]をクリック

HINT!

組織部門ごとにスケジュール調整が可能

[自動更新のチェック間隔]を利用すると、更新ポリシーを組織部門ごとに個別に構成できます。例えば、営業部門は初日に更新チェックを実施し、財務部門は2日目に更新チェックを実施するといったように、自動更新のチェック間隔を組織部門ごとに変更することで、更新のタイミングを分散し、ネットワークの負荷を軽減することなどができます。

HINT!

どれくらいの間隔で更新されるの？

Chrome ブラウザの更新は、概ねフルアップデートが4週間ごと、セキュリティ修正やソフトウェア更新のマイナーアップデートが1週間ごととなっています。ただし、緊急のセキュリティ更新が配布される場合もあるため、なるべく短い間隔で更新をチェックの方が安心です。なお、大規模な更新のリリース日程を知りたい場合は、以下のサイトが参考になるでしょう。

▼Chrome Platform Status

<https://chromestatus.com/roadmap>

HINT!

レガシー テクノロジー レポートによる サポート終了技術の検知

管理コンソールの [レガシー テクノロジー レポート] を利用すると、サードパーティ CookieやTLS 1.0/1.1などのサポートが終了する技術を利用しているWebサイトを検知し、レポートを生成できます。これにより、組織内の古いWebサーバーを検知し、どの技術を置き換えればいいのかを事前に検討できます。

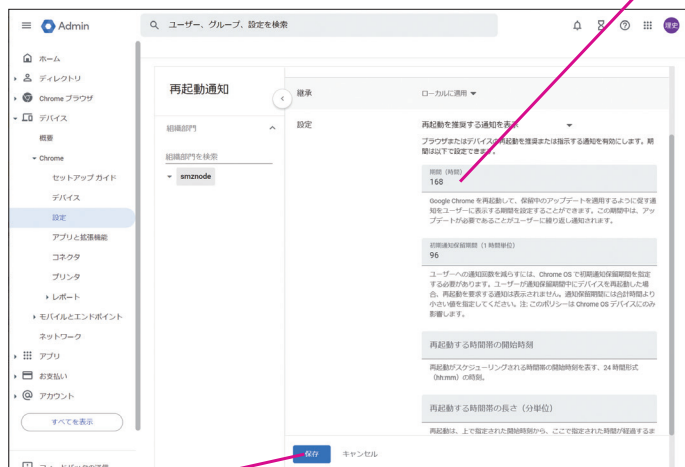
再起動通知を設定するには

Chrome ブラウザの更新を適用するにはアプリの再起動が必要です。確実に更新を適用してもらうためには、[再起動通知] を有効にして、ユーザーに通知を表示するといいでしょ。忘れずに更新を適用してもらうことができます。

再起動の通知に関する設定を変更する

[再起動通知] の設定画面を開いておく

1 再起動通知を表示する間隔などを設定



2 画面下の[保存]をクリック

HINT!

自動的に再起動することはできるの？

[再起動通知] で [一定期間が経過したら自動的に再起動する] を選択すると、再起動する必要があることを示すメッセージが繰り返し表示されます。ユーザーは通知を閉じることができますが、再起動するまで何度も通知を表示できます。

HINT!

通知の表示時間を設定するには

[再起動通知] を表示する時間を設定したいときは、[再起動を推奨する通知を表示] を選択することで、通知を表示する期間や再起動する時間帯などを細かく設定できます。

キャッシュを活用してネットワーク帯域を削減しよう

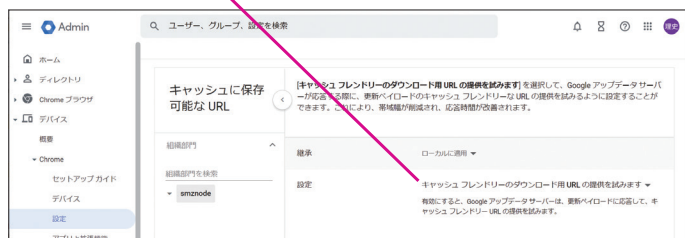
組織で管理しているデバイスの数が多い場合、たくさんのデバイスが一斉に Chrome ブラウザを更新しようとする、ネットワークが混雑してしまう場合があります。そこで利用したいのが、[キャッシュに保存可能な URL] という設定です。この設定を有効にしておくと、帯域幅を削減したり、応答時間を改善したりできます。

更新のキャッシュを設定する

[キャッシュに保存可能な URL] の設定画面を開いておく

1 [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

2 画面下の[保存]をクリック



Point

利便性を損なわないように注意しよう

更新の設定をするときは、事前にユーザーの利用状況を確認しておくことが大切です。現在、使われているバージョンは何なのか？ 更新しても業務に支障はないのか？ 更新を避けるべき業務のピーク時間は何時なのか？ といったことを検討しておきましょう。セキュリティだけを考慮せず、きちんとユーザーの利便性を損なわないように計画することが大切です。

利便性と管理の両ニーズを満たす 拡張機能の運用をするには

拡張機能の管理

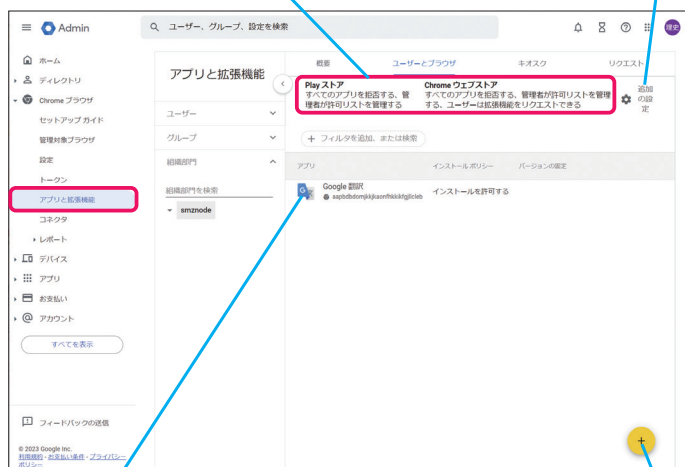
便利だが自由に使われたら困る拡張機能

Chrome ブラウザには、作業効率が向上したり、外部の Web サービスの利用が簡単になったりする多様な拡張機能が提供されています。拡張機能は、ユーザーにとっては便利ですが、管理者にとっては利用状況を把握したり、利用を制御したりするのが難しいもののひとつとなります。ユーザーがある程度自由に拡張機能を使えるようにしつつ、不適切な拡張機能が使われないように管理しましょう。拡張機能を管理するには、まず「許可/ブロックモード」を選択します。すべてのアプリを許可して管理者が拒否リストを管理するのか、すべてを拒否した状態で管理者が許可リストを管理するのかを選択し、各リストに拡張機能を登録しましょう。

1 「Chrome ブラウザ」の「アプリと拡張機能」をクリック

ここでは、すべて拒否で管理者が許可リストを管理し、かつユーザーにリクエストを許可する設定にしている

「追加の設定」をクリックして「許可/ブロックモード」を変更できる



管理者が許可したアプリが、ここに一覧表示される

「+」をクリックすると、ユーザーにインストールを許可するアプリを追加できる

ブラウザの拡張機能を管理しましょう。適切な拡張機能のみを使えるようにすることで、組織全体の拡張機能の利用状況を把握し、利用の可否を制御できます。

HINT!

リスクを確認するには

組織でどの拡張機能の利用を許可すればいいのかを判断したいときは、リスク評価を確認するといでしょう。[アプリの詳細] 画面を開くことで、サードパーティによって提供されたリスク評価スコアやリクエストされた権限などを確認できます。

リクエストの一覧でスコアを確認したいアプリを開き、詳細情報を表示する

サードパーティによって評価されたスコアを確認できる



リクエストされた権限を確認できる

HINT!

拡張機能を権限で ブロックするには

特定の権限を要求する拡張機能をブロックしたいときは、手順1の「追加の設定」の「権限で拡張機能をブロック」でブロックしたい権限を指定します。指定した権限を要求する拡張機能をまとめてブロックできます。

「アプリと拡張機能」の「追加の設定」から権限で拡張機能をブロックできる



ユーザーからのリクエストでインストール可否を決められる

ユーザーからの拡張機能のインストール リクエストをワークフローとして組むことも可能です。組織で利用したい拡張機能を把握し、リスクを監査したうえで管理者承認の元、拡張機能をユーザーに展開できます。ユーザーからのリクエストは、Chrome ブラウザ クラウド管理の [アプリと拡張機能] の [リクエスト] 画面に表示されるので、管理者が拡張機能の内容を確認して許可/拒否を判断できます。

●ユーザーの画面

ユーザーは許可されていない拡張機能をインストールする際にリクエストが必要になる

1 [リクエスト]をクリック



●管理者の画面

管理コンソールの [Chrome ブラウザ] にある [アプリと拡張機能] から [リクエスト]を開く

ユーザーからのリクエストが表示され、インストールの可否を設定できる



外部拡張機能のインストールをブロックできる

拡張機能は、Chrome ウェブストアだけでなく、外部のインストールソースからも導入することができます。ただし、こうした外部拡張機能を許可してしまうことはセキュリティリスクにつながる可能性もあります。外部からのインストールを拒否したい場合は、[外部拡張機能のインストールをブロックする] を選択しておきましょう。

ここでは外部拡張機能のインストールをブロックする

[アプリと拡張機能] の [追加の設定] から設定画面を開いておく

1 [外部拡張機能のインストールをブロックする]を選択



HINT!

拡張機能のリクエストを許可するには

拡張機能のリクエストを許可するには、ユーザーの設定や権限の設定などが必要です。以下のドキュメントで手順が紹介されていますので、参考にしながら設定しましょう。

▼拡張機能のワークフロー：ユーザーに拡張機能のリクエストを許可する

<https://support.google.com/chrome/a/answer/10405494>

HINT!

ポリシーの設定状況を確認するには

管理対象のブラウザにポリシーが適用されているかどうかを確認したいときは、対象となる端末で Chrome ブラウザを起動し、アドレス欄に「chrome://policy」と入力します。ポリシーの一覧で設定を確認できるほか、ポリシーを再読み込みすることなどができます。

Point

バランスよく管理しよう

組織全体を安全に管理するためには、ある程度、厳しいルールを定めることは必要です。ただし、拡張機能のようなユーザーの利便性に大きく影響する機能は厳しく管理しすぎると、組織の生産性が低下することにもなりかねません。ユーザーの視点も忘れずにバランスよくルールを決めて管理することが大切です。

求められるセキュアな エンタープライズブラウザ

安全なブラウザの利用

組織で使用するブラウザには、高度な安全性が必須です。ユーザーがどこで、どのような使い方をしたとしても、情報を保護できるセキュアな環境を整えましょう。

ブラウザがセキュリティのフロントラインに

どこでも手軽に使えるブラウザが業務の中心になってきたことで、ユーザーのセキュリティの意識が薄れてきたと感じることはありませんか？ 例えば、自宅のパソコンに社外秘の資料をダウンロードしたり、個人のパソコンを持ち込んで作業したり、機密情報をうっかりWebサービスに貼り付けたりすることも珍しくありません。また、話題の生成AIサービスに入力した機密情報が、意図せず学習されてしまう懸念もあります。さまざまな利用環境においても組織の情報を守るためには、情報を保護する機能を備えたセキュアなエンタープライズブラウザが不可欠です。

できる Chrome ブラウザ 企業向け導入と運用管理



HINT!

クリティカルな業務に使われるブラウザ

Google のレポートによると、ナレッジワーカーは業務の71%の時間をブラウザに費やしています。また、組織の業務に欠かせない機密性の高いアプリの約半数（48%）がブラウザベースであると報告されており、その傾向はますます増加するでしょう。大切な組織の情報を守るには、ブラウザにエンタープライズレベルのセキュリティ機能を実装する必要があります。

▼Optimize Security and Productivity, Starting with the Browser: Insights from New Report

<https://cloud.google.com/blog/products/chrome-enterprise/optimize-security-and-productivity-starting-with-the-browser-insights-from-new-report>

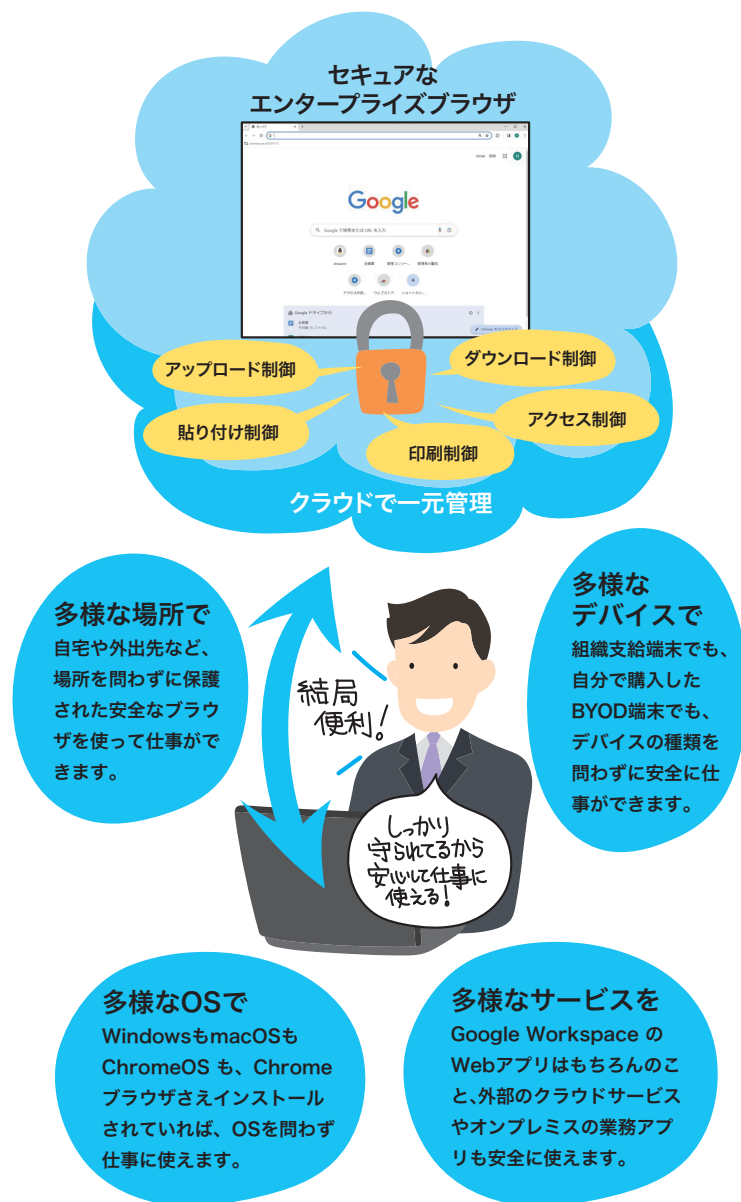
HINT!

「禁止」と伝えるだけでは効果がない

ルールとして、機密情報の扱いを教育したり、社外での勤務の注意事項を設けたりしている組織も多いことでしょう。しかし、単に禁止事項や注意事項を伝えるだけでは万全な対策とはいえません。また、操作ミスを含むさまざまなリスクを防ぐため、情報漏洩や危険な行動を自動で検知し防止するシステムの導入が重要です。

Webアプリやクラウドサービスを安全に使うには

組織の情報を保護するには、ブラウザのセキュリティ設定を強化し、組織全体で統一されたルールを適用できる管理のしくみが必要です。リスクを避けるためのルールを設定し、危険な行為をブロック／警告できるようにしましょう。ネットワークやOSの依存性がなく、いつでも、どこでも、安全にWebアプリやクラウドサービスを利用可能にすることで、使えるデバイスの種類や場所が自由になり、結果的にユーザーの利便性向上にもつながります。



HINT!

組織内やVPN接続だから安心とは限らない

「オフィスのLANにつないでいるから安心」「自宅からでもVPN接続なら業務データに危険はない」。かつてのセキュリティ対策は、こうした一定の境界でルールを分ける方式が主流でした。しかし、働く場所、使うデバイス、利用するサービスが多様化した現代では安全な環境と危険な環境を区別する境界があいまいで、従来のようなセキュリティ対策だけでは情報を安全に扱うことが難しい状況です。誰が、いつ、どこから、どのアプリで、どのような操作をしても保護される新しいセキュリティの考え方が必要です。

HINT!

働き方が多様でも利用制限があっては意味がない

リモートワークなどで、働く場所や時間が自由になっても、セキュリティ対策によって、利用できる業務アプリが制限されたり、煩雑な設定や操作が要求されたりしては意味がありません。高いセキュリティと利便性を両立させることが大切です。

Point

組織のセキュリティ課題をブラウザ管理で解決しよう

組織の情報を保護するには、業務アプリの基盤となっているブラウザを「セキュアなエンタープライズブラウザ」として構成することが重要です。組織のデータを保護したり、アクセス先を制限したりと、組織のセキュリティ方式に合わせたルールがブラウザに適用されるように一元管理しましょう。どこでも、どのデバイスでも安全に仕事ができれば、組織にもユーザーにもメリットが生まれます。

セキュアなエンタープライズブラウザを使うには

Chrome Enterprise Premium

セキュアなエンタープライズブラウザを構成する方法を見てみましょう。「Chrome Enterprise Premium」を利用することで高度なセキュリティ対策が可能です。

Chrome ブラウザ クラウド管理+ Chrome Enterprise Premium

Chrome ブラウザをより安全に利用するには、これまでに紹介した Chrome Enterprise Core にて活用している「Chrome ブラウザ クラウド管理」に加えて、「Chrome Enterprise Premium」を利用することをおすすめします。Chrome Enterprise Premium を利用することで、デバイスや場所を問わず、Webアプリのアクセスやデータを保護したり、アクセスできるURLを制限したり、環境に合わせて動作を制限したりすることが可能です。

Chrome ブラウザ
クラウド管理

目的：設定・更新管理
対象：組織のデバイス
費用：無料

+

Chrome Enterprise
Premium

目的：データ損失防止
対象：デバイスや場所を
問わず
費用：有料

=



セキュアな
エンタープライズ
ブラウザ

●Chrome Enterprise Core (Chrome ブラウザ クラウド管理) と Chrome Enterprise Premium の比較

URLカテゴリフィルタリング		
Webサービスのデータ損失防止 (DLP)		
-保護ルールに基づくセンシティブデータのスキャン・監査		
-コピー & ペースト・ダウンロード・アップロード制御		
-コンテキスト別の保護ルール		
リアルタイムマルウェアスキャン		
コンテキストウェアアクセス (Private Web App)		
コンテキストウェアアクセス (SAML/ SaaS)		
ブラウザ上のセキュリティログ、SIEM連携		
レポート (リスクのあるブラウザ、更新、拡張機能、レガシー Web サイト検出、等)		
拡張機能の監査と制御 (許可、ブッシュ、ブロック、等)		
更新管理 (スケジュール制御、バージョン制御等)		
300を超えるブラウザの制御ポリシー (マルチOS対応)		
-セキュリティ (URLブロック、シャドー IT制御、アイト ライムアウト、等)		
-ユーザーエクスペリエンス (ブックマーク配信、言語設定、アカウント制御、等)		
-データ (キャッシュ・クッキー自動消去、Chrome Sync、ローミング、等)		
-従来のブラウザサポート (特定のサイトで開くブラウザを指定)		

Chrome Enterprise Core Chrome Enterprise Premium

HINT!

Chrome Enterprise Premium って何？

Chrome Enterprise Premium は、ユーザーやデバイスの状態に基づいて、利用できるリソースを細かく制御できるセキュリティサービスです。例えば、認証されたユーザーだけに Web アプリを許可したり、デバイスの場所や状態に応じて使えるクラウドサービスを制限したりできます。アクセス後も、データ保護により Web アプリの検疫が可能です。Google のサービスだけでなく、一般的なクラウドサービスや社内のサーバーへのアクセスも制御できます。Chrome Enterprise Premium の管理方法はこれまで解説した Chrome ブラウザ クラウド管理と大きな違いはなく、組織の Chrome ブラウザに適用したいポリシーやルールを設定するだけです。デバイスへのソフトウェアのインストールや設定なども必要ありません。

HINT!

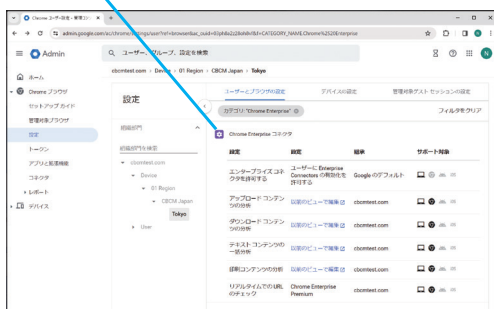
Chrome Enterprise Premium を使うには

Chrome Enterprise Premium の利用にはライセンスが必要です。ユーザーごとに割り当てる必要があるので、営業担当者経由で問い合わせてみましょう。有効化するには、「ライセンスの割り当て」→「Endpoint Verification 拡張機能の配布」→「Chrome Enterprise コネクタの設定」→「ルールの設定」という流れで設定します。詳しくはレッスン 18 で解説します。

接続先として Chrome Enterprise Premium を設定

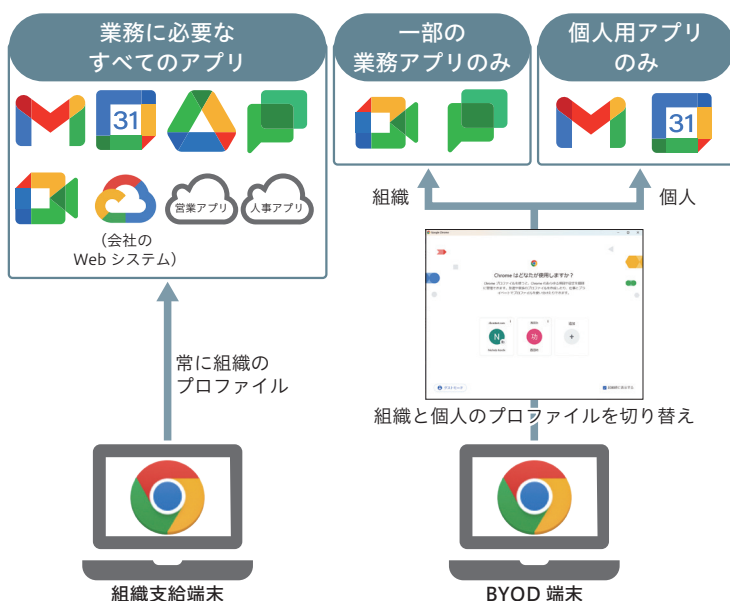
Chrome Enterprise Premium の設定や管理に特別なしくみは必要ありません。これまでに紹介した管理機能と同様に、Google 管理コンソールから設定や管理ができます。詳しくはレッスン⑩を参照してください。

Chrome Enterprise コネクタで接続先を Chrome Enterprise Premium に設定する



Chrome ブラウザにサインインすることで適用される

Chrome Enterprise Premium のライセンスが割り当てられたユーザーは、Chrome ブラウザに組織のアカウントでログインすることで自動的にルールが適用されます。利用するデバイスやログインするプロファイルによって、適用するルールの使い分けが可能です。例えば、個人のプロファイルの場合は個人用アプリのみに制限し、組織のプロファイルのときだけ業務アプリにアクセスできるように設定できます。



HINT!

会社独自のWebアプリのアクセス制御も可能

Chrome Enterprise Premium を利用することで、Google 管理コンソールから、クラウドやオンプレミス（自社の運用環境）上にホストされた会社独自のWebアプリにアクセス制御の対象とすることができます。そうすることで、安全に社内アプリに接続できるようになります。

HINT!

組織支給端末とBYOD端末を区別できる

Chrome Enterprise Premium には、条件によって細かくデバイスを制御できる「コンテキスト アウェアアクセス」という機能が利用できます。コンテキスト アウェアアクセスは、接続中のIPアドレスやデバイスの種類、OSなどを判断して、Webアプリへのアクセスを制御できる機能です。例えば、組織支給端末のみ、すべての業務アプリにアクセス可能にし、個人が持ち込んだBYOD端末では一部の業務アプリのみのアクセスに制限できます。

Point

Chrome ブラウザに高度なセキュリティを追加

Chrome Enterprise Premium を利用すると、Chrome ブラウザ管理に、データ保護機能（DLP：データ損失防止）やURLカテゴリフィルタ、コンテキスト アウェアアクセスといった高度なセキュリティ機能を追加できます。デバイスや場所を問わず、Chrome ブラウザで情報漏洩対策やアクセス制御ができるので、組織の安全性を高めるのに役立つでしょう。

どんなリスクを防げるの？

Chrome Enterprise Premium の機能

データ保護やURLフィルタリングを実現

Chrome Enterprise Premium は、データ保護（アップロード時、ダウンロード時、テキスト貼り付け時、印刷時）やカテゴリごとのアクセス制御を実現します。具体的には、Chrome ブラウザを通じてやり取りするデータやアクセスするWebサイトを監視し、あらかじめ定められたルールと照らし合わせ、ブロックや警告などの対処が可能です。



Chrome Enterprise Premium を利用することで、具体的にどのようなリスクを防げるのでしょうか？ 組織の業務を想定したシーンで確認してみましょう。

HINT!

機能の制限範囲は選択して設定できる

どのような動作を制限するかは、組織のニーズや方針によって選択できます。例えば、ファイルのアップロードのみを制限したり、段階的に機能を有効化したりと、自由に構成できます。

HINT!

複雑なルールも設定可能

Chrome Enterprise Premium のルールは柔軟な設定が可能です。単純に「社外秘」という言葉が含まれている場合だけブロックすることもできれば、「社外秘」または「Confidential」が含まれる場合など、複数の条件をANDやORで組み合わせ設定できます。

HINT!

対象の設定も簡単

ルールには、「事前定義されたデータの種類と一致する」という項目が用意されており、メールアドレスや銀行口座番号、パスワードなどの認証情報、履歴書などのドキュメントなどを簡単に分析対象に設定できます。また、複数の単語を登録した単語リストや正規表現なども設定できます。

在宅勤務や外出先でも組織のファイルを保護したい

Chrome Enterprise Premium を利用すると、ファイルのアップロード／ダウンロード操作を保護できます。例えば、在宅勤務中に個人のパソコンにファイルをダウンロードして作業しようとしても、ファイルに機密情報や個人情報が含まれる場合は操作を禁止できます。同様に、事前のルールに従ってファイルのアップロード操作も禁止できます。Google Drive だけではなく、外部のクラウドストレージサービス等すべてのWebアプリに対し、カテゴリに準じて制御可能です。

●ダウンロードコンテンツの分析



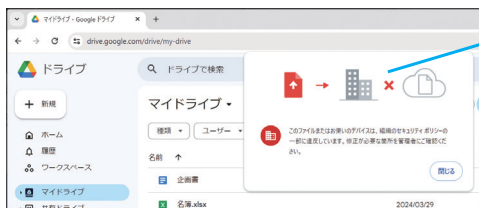
ダウンロードがブロックされる

例えば…

- ・「社外秘」や「Confidential」という文字が含まれるファイル
- ・特定の製品名やプロジェクト名が含まれるファイル



●アップロードコンテンツの分析



アップロードがブロックされる

例えば…

- ・クレジットカード番号やマイナンバーなどが含まれるファイル
- ・認証情報やシークレットが含まれるファイル



HINT!

画像内のテキストも認識可能

Chrome Enterprise Premium では、ファイル内に貼り付けられた画像も分析できます。画像内に禁止された言葉が含まれる場合は、同様にダウンロードやアップロードをブロックできます。

HINT!

Evidence Locker も設定可能

Evidence Locker (証拠監査) 機能を用いることで、設定したデータ損失防止 (DLP) のルール、およびブラウザの管理状態に基づいて、ブラウザ上でやり取りされる機密情報の監査から Google Cloud Storage 上に証拠を残して詳しい解析を実行できます。

HINT!

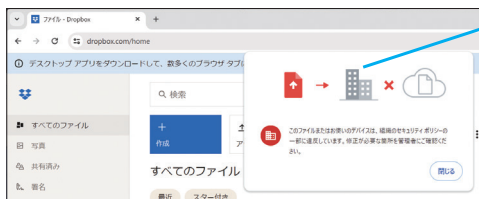
組織におすすめのルールを参照できる

Google 管理コンソールの [セキュリティ] にある [アクセスとデータ管理] から [データ保護] を開くと、外部共有されているファイルや組織のおすすめのルールを参照できます。ルールの設定に困ったら、参照してみるといいでしょう。

次のページに続く

目の届かない外部でのファイル共有を禁止したい

取引先などとのファイル共有に Google 以外のストレージサービスを利用することも珍しくありません。Chrome Enterprise Premium では、Google 以外のサービスを利用したアップロード／ダウンロード操作も監視できます。あらかじめ設定したルールに違反するファイルがアップロード／ダウンロードされそうになると、動作をブロックできます。



外部サイトでもファイルのアップロードがブロックされる

例えば…

- ・外部のクラウドストレージサービスへの保存
- ・Web会議やチャットへのファイル投稿



勤務中についつい個人的な調べもの

勤務中のWebサービスの利用を制限したい場合にも Chrome Enterprise Premium が役立ちます。あらかじめ禁止したいWebサイトやクラウドサービスのカテゴリを設定しておくことで、ショッピングサイトやゲームサイトなどのアクセスを制限できます。



特定サイトへのアクセスをブロックできる

例えば…

- ・業務中のショッピングサイト利用
- ・ゲームや動画の禁止



HINT!

オンプレミスの業務アプリは？

HTTPまたはHTTPSベースのオンプレミスアプリへの接続を Chrome Enterprise Premium で管理したい場合は、「Identity-Aware Proxy (IAP) コネクタ」をデプロイする必要があります。詳しくは、以下のドキュメントを参照してください。

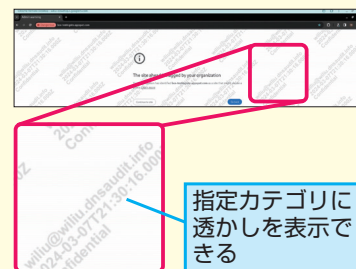
▼オンプレミス アプリでのIAPの有効化

<https://cloud.google.com/iap/docs/enabling-on-prem-howto?hl=ja>

HINT!

Watermarkも設定できる

指定したURLカテゴリ（生成AIやSNS等）に、利用者の情報や日時、指定したメッセージを透かしとして表示させることが可能です。機密情報であることの明確化によって画面内の情報の公開・共有をしないように注意喚起できます。また、ログを取得することでデータの監査が可能になりガバナンスを強化することができます。



指定カテゴリに透かしを表示できる

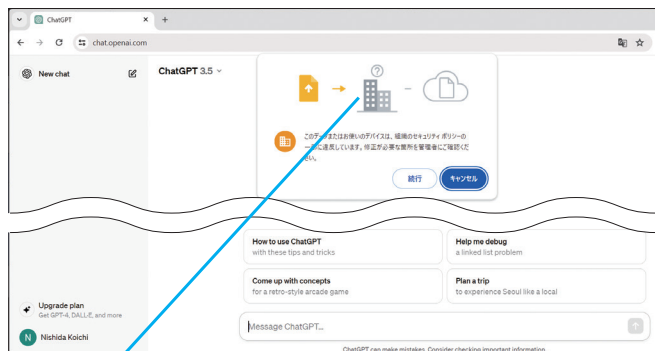
HINT!

URL指定とカテゴリ指定ができる

URLフィルタリングでは、URLを直接指定する方法と、カテゴリを指定する方法があります。複数のWebサイトを制限したい場合は「ショッピング」や「ゲーム」などのカテゴリを、特定のサイトを制限したい場合はURLを指定しましょう。

調べもので機密情報をうっかり

検索サイトやAIチャット、SNSなどで、意図せず、クリップボードに残っていた文字列が貼り付けられて、驚いた経験はありませんか？ Chrome Enterprise Premium を利用すれば、貼り付け操作を検知して、機密情報などルールに違反する情報が貼り付けられること自体をブロック、および監査、警告することができます。



「貼り付け」操作を検知して、特定情報の投稿をブロックできる

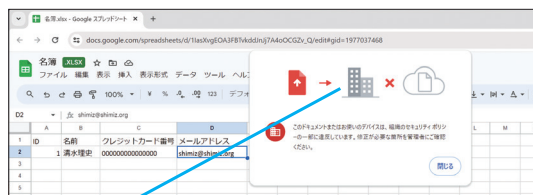
例えば…

- ・AIチャットで機密情報を相談
- ・コピーしたまま忘れていた情報をSNSにうっかり投稿



印刷物からの情報漏洩を防ぎたい

デジタルが中心の現代でも、まだ紙の印刷物のニーズは少なくありません。うっかり社外秘の情報を印刷してしまうことなどを防ぎたいなら、Chrome Enterprise Premium の利用がおすすめです。ルールに反した文書の印刷を未然にブロック、および監査、警告することができます。



印刷しようとするブロックされる

例えば…

- ・印刷して外部に持ち出し
- ・気付かずにうっかり印刷



HINT!

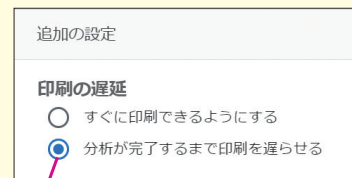
貼り付け先を指定できる

コンテンツの貼り付け操作の検知では、貼り付ける先のWebサイトやクラウドサービスをURLやカテゴリで指定できます。このため、「生成AI」や「掲示板」「チャット」など、特定のカテゴリやWebサイトへの貼り付け操作を禁止および監査、警告することができます。

HINT!

印刷を禁止するときは

印刷を禁止するときは、コネクタの追加の設定が必要です。[Chrome Enterprise コネクタ] の [印刷コンテンツの分析] の設定にある [追加の設定] で、[印刷の遅延] の [分析が完了するまで印刷を遅らせる] を選択しておきましょう。



1 [分析が完了するまで印刷を遅らせる]を選択

Point

いろいろなシーンで役立つ

Chrome Enterprise Premium は、組織の日常的な業務に潜む危険から、大切なデータを保護するのに役立ちます。ファイルのアップロードやダウンロード、テキストの貼り付け、印刷を検知し、あらかじめ指定したルールに従って自動的に制御（ブロック、警告、監査）できます。というわけで、情報漏洩につながるリスクを低くできるでしょう。

エンタープライズブラウザを設定・管理するには

Chrome Enterprise Premium の設定とリスクの可視化

Chrome Enterprise Premium の設定や管理方法を見てみましょう。特別な管理ツールは不要で、Google 管理コンソールから簡単に設定や状況確認ができます。

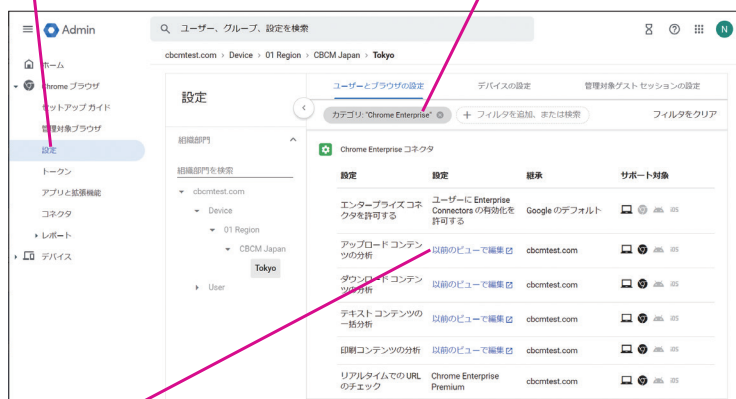
Enterprise コネクタを有効にする

Chrome Enterprise Premium のデータの保護機能を利用するには、Chrome ブラウザでやり取りするデータを Chrome Enterprise Premium に送信して分析する必要があります。Chrome ブラウザの [Enterprise コネクタ] ポリシーにある各項目の接続先として [Chrome Enterprise Premium] を設定しておきましょう。

1 右のURLにアクセス **◆管理コンソール**
https://admin.google.com

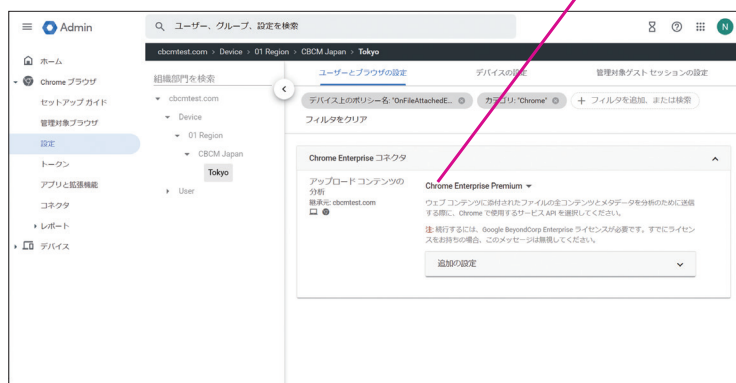
2 [Chromeブラウザ]の[設定]をクリック

3 [Chrome Enterpriseコネクタ]でフィルタを設定



4 設定したい項目をクリック

5 接続先として[Chrome Enterprise Premium]を選択



HINT!

ライセンスを割り当てておこう

Chrome Enterprise Premium を利用するには、ユーザーごとにライセンスが必要です。Google 管理コンソールの [お支払い] にある [サブスクリプション] で、Chrome Enterprise Premium に管理対象のユーザーを割り当てておきましょう。

HINT!

条件や動作の変更には追加の設定が必要な場合もある

Enterprise コネクタの各項目で Chrome Enterprise Premium を接続先に設定する際、[追加の設定] で分析の動作や条件を変更できます。例えば、分析が完了するまで対象の動作(アップロードやダウンロード、印刷)を遅らせたり、警告メッセージを変更したりできます。



ルールを設定する

Enterprise コネクタの設定ができれば「ルール」を設定します。ルールは、どのアプリを、どんな条件のときに、どう制限するかを決めるものです。例えば、ファイルのアップロードやダウンロードを制限するときに、どのような文字列が含まれる場合にブロックするのかが設定します。

1 [ルール] をクリック

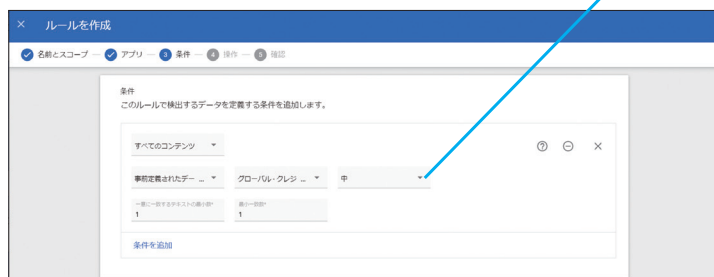
2 [ルールを作成] - [データの保護] の順にクリック



登録済みのルールが表示された

画面の指示に従って、適用する範囲、対象のアプリ、条件、操作を設定する

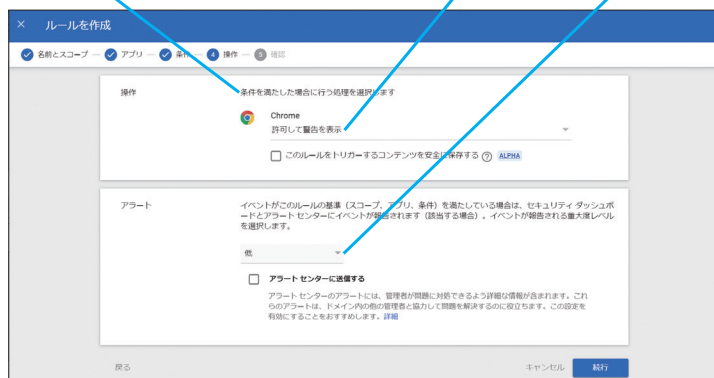
何をどのような条件で制限するのかが設定する



条件に合った場合にどうするのかを設定する

ブロックしたり、警告を表示したりできる

アラートのレベルを選択できる



HINT!

ルールの設定例

例えば、「社外秘」という文字列が含まれるファイルのダウンロードを禁止した場合は、各項目を次のように設定します。

●アプリ：

[Chrome]の[ファイルをダウンロードしました]を選択

●条件：

[すべてのコンテンツ]の[次の単語を含む]で「社外秘」を設定

●操作：

[ブロック]を選択

●アラート：

[高]を選択

13

Chrome Enterprise Premium の設定とリスクの可視化

HINT!

操作は3種類ある

条件に合った場合に実行される「操作」は、「ブロック」「許可して警告する」「監査のみ」の3種類から選べます。完全に禁止したい操作は「ブロック」、禁止していないもののリスクが高い操作は「許可して警告する」、間接的にリスクにつながる可能性がある操作は「監査のみ（ログに記録される）」を選択するといでしょう。

次のページに続く

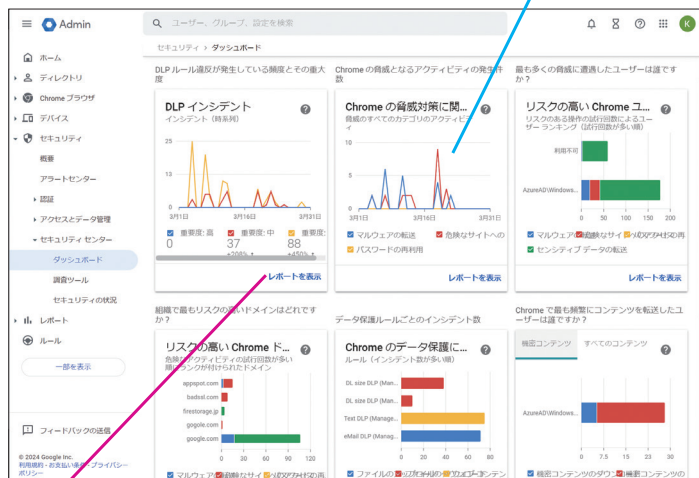
リスクの状況を確認するには

Chrome Enterprise Premium の保護状況は、[セキュリティセンター] の [ダッシュボード] で確認できます。ルールに合致したインシデントのレポートを [DLPインシデント] から確認してみましょう。このほか、ダッシュボードでは、リスクの高い操作が多いユーザーやリスクの高いドメインなども把握できます。

管理コンソールで、[セキュリティ] の [セキュリティセンター] にある [ダッシュボード] を表示する

セキュリティの統計情報が表示される

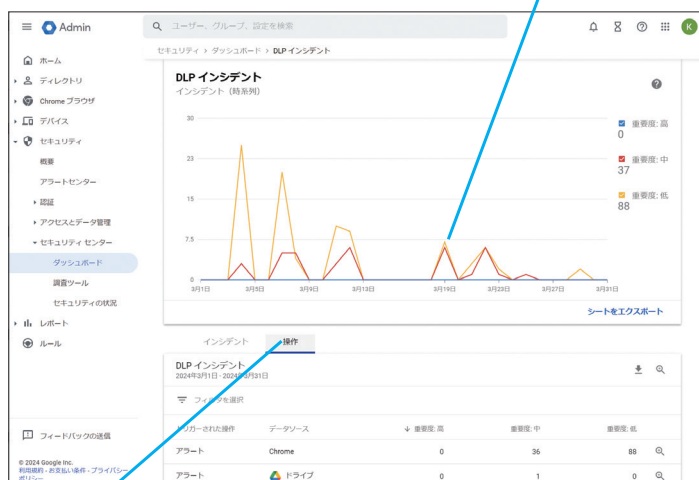
カテゴリごとに発生頻度などがグラフとして表示される



1 [DLPインシデント]の[レポートを表示]をクリック

DLP（データ保護）のレポートが表示される

設定したルールに抵触した件数が日付ごとに表示される



[操作]タブでは、ダウンロードなど操作ごとの件数を確認できる

HINT!

ダッシュボードをカスタマイズできる

ダッシュボード画面の右上に表示されているアイコンをクリックすると、ダッシュボードをカスタマイズできます。ウィジェットを追加したり、表示される位置を変更したりできます。把握したい情報に合わせてカスタマイズしておきましょう。

HINT!

どんなリスクを確認できるの？

ダッシュボードでは、Chrome ブラウザ上での悪意のあるファイルの転送や不正なアクセス、パスワードの再利用、機密情報の転送といったリスクが発生しているユーザーやドメインを確認できます。また、どのような機密情報が、どのサイトで多くやり取りされているかも可視化できます。

HINT!

さらに調査が必要な場合は

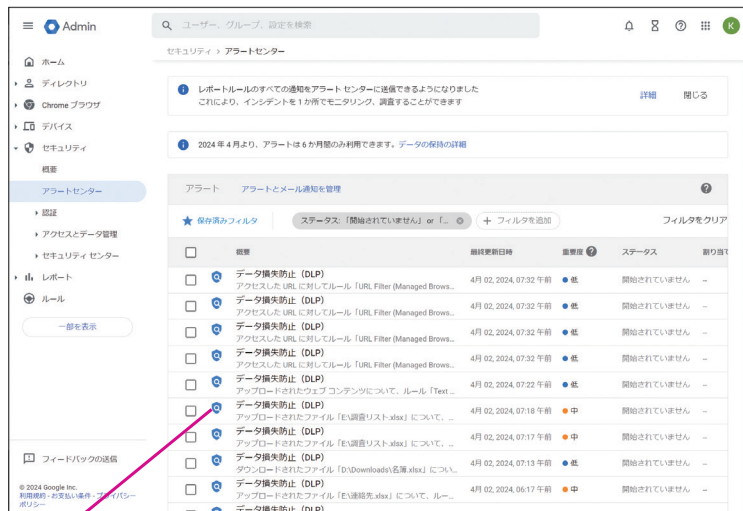
このページの下で、インシデントの右端に表示されているループのアイコンをクリックすると、調査ツールを起動できます。日付や重要度などでフィルタリングして特定のインシデントを探したり、各インシデントのログから詳しく状況を確認したりできます。

アラートを確認する

ルールで設定したアラートは「アラートセンター」で確認できます。どのアプリに対して、どのような操作が行われたのかが日時ごとに表示されます。ユーザーや重要度でフィルタできるので、特定のインシデントを調査したいときに役立ちます。

管理コンソールで、「セキュリティ」の「アラートセンター」を表示する

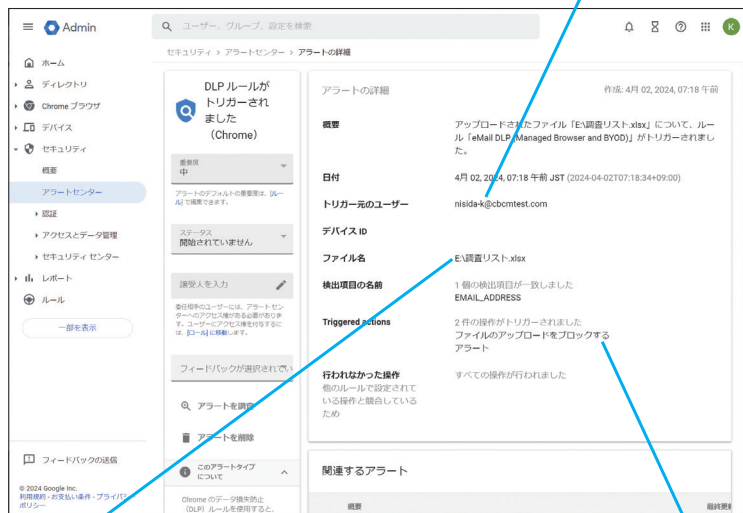
ルールで設定したアラートが一覧表示される



1 詳細を確認したいアラートをクリック

アラートの詳細が表示された

◆ルールに合致したユーザー



◆ルールに合致したファイル

◆合致した操作

HINT!

メール通知を設定するには

アラートの通知をメールで受け取ることもできます。アラートのリストの上部に表示されている「アラートとメール通知を管理」をクリックして、「ルール」の画面から通知したいルールの「アラート」設定を開き、「メール通知を送信する」を設定しましょう。

Point

組織のセキュリティ状況を可視化できる

Chrome Enterprise Premium は、ユーザーによるリスクのある操作を未然に防げる機能です。組織に合わせたルールを柔軟に構成できるので、利用環境に合わせて活用しましょう。また、リスクを防ぐだけでなく、組織の利用状況を可視化することもできます。どのアプリで、誰が、どのような情報を、どう扱っているかを把握できるので、組織のルールを見直したり、リスクに対する啓蒙活動をする際の参考にしたりできるでしょう。

付録 Chrome ブラウザ企業向けサポートオプション

組織で Chrome ブラウザの導入や、Chrome Enterprise Core・Chrome Enterprise Premium の導入を検討しているときは、有償サポートの利用も検討するといいいでしょう。導入や利用方法などについて、専門家に電話やオンラインでの問い合わせができます。有償サポートの加入方法は以下の2通りがあります。

●Google のサービス購入条件を満たすお客様向け

すでに Google Workspace などのサービス条件を満たす形で利用している場合は、現在の契約だけで Chrome ブラウザに関するサポートを受けることができます。以下のようなライセンスを一定数以上契約している場合が対象です（このケースの場合は特徴として100ライセンスを保有していれば、無制限のユーザーの Chrome ブラウザをサポート可能です）。

- ・ Google Workspace：最低100ライセンス
※有償ライセンスの購入が条件
- ・ Chrome Enterprise Upgrade (CEU)：
最低100ライセンス
※年間ライセンスはライセンスの購入が条件
- ※永続ライセンスはライセンスの購入に加えて登録済みデバイスとしてアップデートを受けていることが条件
- ・ Google Cloud Enhanced | Premium
サポート

●Chrome ブラウザエンタープライズサポートの購入

上記条件を満たしていない場合は、Chrome ブラウザを利用するユーザー数分のライセンスにてサポートを購入することができます。最低1,000ライセンスからとなるため中規模以上の環境となりますが、年間一定の金額で Chrome ブラウザおよび Chrome ブラウザ クラウド管理の利用方法などを電話、もしくはオンラインで問い合わせることができます。

●Chrome ブラウザ企業向けサポートの対象範囲

Chrome ブラウザ企業向けサポートの対象範囲は、以下の通りです。

- ・ Chrome ブラウザ クラウド管理
- ・ Windowsのグループポリシー テンプレート
- ・ Chrome ブラウザの MSI インストーラー
- ・ 従来のブラウザ設定ポリシー
(Internet Explorerとの切り替え)
- ・ 第三者のソフトウェアやサイトに起因しないブラウザの問題
- ・ 最新のstable、beta、devバージョンのサポート
- ・ すべてのOSに対するサポート

▼企業向けの Chrome ブラウザのサポートサービスや Chrome ブラウザ クラウド管理に関する問い合わせはこちら

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



▼Chrome ブラウザ 操作手順 解説動画

レッスン④以降の内容の具体的な手順を解説付きで公開しています。

https://www.youtube.com/watch?v=IFG0Xkd88GM&list=PL_M98aVzfljqP3bdixnKeYMDzLmVCCnNN&index=4



■著者

清水理史（しみず まさし）mshimizu@shimiz.org

1971年東京都出身のフリーライター。雑誌やWeb媒体を中心にOSやネットワーク、ブロードバンド関連の記事を数多く執筆。「INTERNET Watch」にて「イニシャルB」を連載中。主な著書に『できるWindows 11』『できるWindows 11 パーフェクトブック 困った! & 便利ワザ大全』『できるZoom ビデオ会議やオンライン授業、ウェビナーが使いこなせる本 最新改訂版』『できるChromebook 新しいGoogleのパソコンを使いこなす本』『できるUiPath StudioX はじめての業務RPA』『できるはんこレス入門 PDFと電子署名の基本が身に付く本』『できるfit ドコモiPhone SE 第3世代 基本+活用ワザ』などがある。

「できる Chrome ブラウザ 企業向け導入と運用管理」（以下、本書）は、Google LLCから株式会社インプレスが委託を受けて制作した特別版です。本書は無償で提供されるものであり、本書の使用または使用不能により生じたお客様の損害に対して、著者、Google LLCならびに株式会社インプレスは一切の責任を負いかねます。また、本書に関するお問い合わせはお受けしておりません。あらかじめご了承ください。

できる Chrome ブラウザ 企業向け導入と運用管理

- Chrome Enterprise Core / Chrome Enterprise Premium 活用編 -

編集 ————— できるシリーズ編集部
執筆 ————— 清水理史
シリーズロゴデザイン — 山岡デザイン事務所
カバーデザイン ————— 横川信之
本文イメージイラスト — 原田 香
DTP制作 ————— 株式会社トップスタジオ

2024年5月 初版発行

発行 株式会社インプレス
〒101-0051
東京都千代田区神田神保町一丁目105番地

Copyright © 2024 Masashi Shimizu and Impress Corporation. All rights reserved.

本書の内容はすべて、著作権法によって保護されています。著者および発行者の許可を得ず、転載、複写、複製等の利用はできません。

「できるサポート」では、本書に関するお問い合わせにはお答えしておりません。あらかじめご了承ください。

できる Chrome ブラウザ 企業向け導入と運用管理

Chrome Enterprise Core / Chrome Enterprise Premium

活用編

非売品

「できるシリーズ」は、画面で見せる入門書の元祖です。

見開き完結のレッスンを基本とし、レッスン1から順を追って

進めていくことで、楽しみながらパソコンの操作を学べます。

また、レッスンを進めるにしたがって、必要な知識が身に付く構成に

なっています。できるシリーズなら、はじめての人でも安心です。

- オールカラーの紙面でわかりやすく解説
- レッスン単位でステップアップ学習できる
- 各レッスンごとに重要ポイントを掲載
- 関連知識をヒント形式で解説