社内での
拡張機能を管理する

Chrome 拡張機能を広範囲かつ安全に管理する

目次

このガイドの目的

Chrome ブラウザには便利な拡張機能が多数あります。ユーザーはパソコンではさまざまな機能を使用している可能性があり、それが IT 管理者による拡張機能の制御や監視を困難にしていることがあります。

このガイドは、拡張機能の最適な管理方法を求めている IT 管理者を対象にしています。Chrome ブラウザ クラウド管理と Windows グループ ポリシーの両方を使って拡張機能を管理する手順をご紹介します。

このガイドは、拡張機能の管理方法に基づいて整理されています。次のように管理できます。

1. 権限に基づいて拡張機能をブロックする
2. 拡張機能がアクセスできるウェブサイトを管理する
3. Chrome ブラウザ クラウド管理または Windows グループ ポリシーで拡張機能を許可またはブロックする
4. 拡張機能をオンプレミスで自己ホストする

内容	社内での Chrome ブラウザ拡張機能の管理手順と推奨事項
主な対象読者	Microsoft® Windows® と Chrome ブラウザ クラウド管理の管理者（サポート対象: Windows、Mac、Linux）
要点	Chrome ブラウザで拡張機能を管理するためのベスト プラクティス

最終更新: 2019 年 10 月 29 日

掲載場所: https://support.google.com/chrome/a/answer/9296680

はじめに

企業はユーザーデータを保護する必要があり、拡張機能の安全性と関連性を簡単に詳しくチェックしたいと考えています。IT 管理者には、以下のことが求められます。

1. 不正な拡張機能がインストールされないようにする。
2. ユーザーに必要な拡張機能を保持する。
3. ユーザーデータや企業データへのアクセスを制限する。

このガイドでは、拡張機能を簡単に管理する方法をご紹介します。 拡張機能を管理する方法は複数ありますが、このガイドではいくつか紹介して、その中から環境に合う方法を選ぶことができるようお手伝いします。

Chrome 拡張機能の管理に関する考慮事項

ユーザーの業務には、アプリ、サイト、拡張機能へのアクセスが欠かせません。IT 管理者として行わなければならないことは、ユーザーや会社のデータを保護することです。そこで必要になってくるのが、拡張機能の管理方法を選ぶための戦略です。

主な質問事項:

- どのような規制やコンプライアンスを遵守する必要があるか？
- どのようなデバイスやウェブサイトのアクセスが、会社のセキュリティ ポリシーに違反するか？
- どのくらいのユーザーデータや企業データが、ユーザーのパソコンに保存されているか？

このような判断を行うとき、Google が提供するポリシーを使うと次のことが可能になります。

- データ保護ポリシーに基づいて拡張機能をブロックまたは許可する。
- 必要な拡張機能をユーザーのパソコンに自動的にインストールする。
- 作業に必要な最小限の権利を付与しつつ拡張機能を管理する。

これまでは、特定の拡張機能を許可またはブロックすることで管理していましたが、もっと簡単な方法があります。拡張機能が必要とする権限を使用すれば、管理することができます。許可したい権限について調べ、自分の要件を満たす拡張機能を許可またはブロックするポリシーを適用してください。

拡張機能の権限とは

拡張機能が正常に動作するために、パソコンやウェブページに変更を加える許可が必要な場合があります。こうした許可を権限と呼びます。開発者は、自分の拡張機能に必要な許可とアクセスを記載する必要があります。権限は大きく 2 つのカテゴリに分けることができ、多くの拡張機能は両方を持っています。

- サイトの権限により、ユーザーがアクセスするウェブサイトにアクセスする。
  例: ウェブページの変更、Cookie へのアクセス、タブの変更
- デバイスの権限により、ブラウザが実行されているパソコンにアクセスする。
  例: USB ポート / ストレージ / 表示画面へのアクセス

拡張機能の更新方法

拡張機能の更新は Chrome の動作中にのみ行われます。また、Chrome の起動後数分以内に行われ、その後 5 時間ごとに実行されます。

- 拡張機能の更新プロセス:
    a. インストール済みの拡張機能とバージョンのリストを含むリクエストが、Chrome によって Google のサーバーに送信される
    b. サーバーによって更新対象の拡張機能に関する指示が返される
    c. その後 Chrome によって CRX ファイルが古くなった拡張機能ごとにリクエストされ、ローカルで更新が適用される
- 拡張機能が古くなる原因:
    a. 更新のダウンロード サイズが大きい場合や、ユーザーが使用している拡張機能が多い場合、ユーザー セッションの時間が短いと更新が完了しないことがある
    b. Chrome を起動していない
    c. 拡張機能の開発者が、更新のデプロイ先クライアントの数を制限している
    d. 企業が拡張機能を自己ホストしている場合、これがアクセスの問題や設定エラーが原因になっている可能性がある
    e. 拡張機能の開発時のエラーに起因すると思われるその他の問題がある

古くなった拡張機能に関する問題を解決するには、拡張機能をアンインストールしてから再インストールします。また、chrome://extension に移動してデベロッパー モードを有効にしてから更新ボタンを押せば、手動で拡張機能を更新できます。

拡張機能の管理

ほとんどの組織におすすめできるのが、拡張機能の権限や、どのウェブサイトにアクセスできるかによって拡張機能を管理する方法です。この方法は安全で管理しやすく、またスケーラブルです。

ポリシーの設定が一度で済むため、時間の節約にもなります。長い許可リストとブロックリストを管理していた時代は終わりました。インストールしてはいけない拡張機能の短いブロックリストについては、引き続き追加できます。また、最も重要なサイトは、ランタイム ホスト ポリシーによって保護されます。この方法で組織内の拡張機能を管理する手順は次のとおりです。

1. ユーザーのパソコンにインストールされている拡張機能を確認します。
    - 方法 1（推奨）： Chrome ブラウザ クラウド管理を使用します。この機能は、追加費用なくユーザーに提供されています。拡張機能の以下の情報を確認することができます。
        - インストール済みバージョン、インストール回数、ユーザーまたは管理者のどちらでインストールされたか
        - 必要な権限
        - ステータス（有効または無効）
    - Chrome ブラウザ クラウド管理の設定手順については、こちらをご確認ください。

- コンソールを設定し、クラウド レポートを有効にしてパソコンを登録すると、**[デバイス] > [Chrome]> [アプリと拡張機能の使用状況レポート]** で、すべてのインストール済み拡張機能を確認できます
    - 拡張機能をクリックすると、その拡張機能に必要な権限に関する詳しい情報と、インストール先の例が表示されます
        - 2021 年後半～2022 年前半には、拡張機能をクリックすることで、新しい拡張機能の詳細ページが表示されるようになります（下図参照）
        - ここでは、必要な権限や情報といった拡張機能に関する詳しいインサイトを、Chrome ウェブストアの掲載情報から直接取得することができます
        - Chrome ブラウザ クラウド管理での拡張機能の管理の詳細については、こちらの YouTube 動画でご確認いただけます。
    - また、Chrome ブラウザ クラウド管理のデータ エクスポート API を使用して、登録済みブラウザからすべての拡張機能データを CSV ファイルにエクスポートすることもできます。
        - 詳しくは、手順ガイド、ブログの記事、デモ動画をご参照ください
- 方法 2: アンケート: 同僚やその上司にどのような拡張機能をよく使用しているかを聞き、ユーザーが必要としている拡張機能のリストを作成します。

2. 安全対策が必要なサイトを選びます。
    - 拡張機能によるデータの変更や読み取りをブロックする必要がある、機密性の高いウェブサイトやドメインを確認します。
        - 拡張機能の実行中に API 呼び出しをブロックすることで、こうしたサイトへのアクセスを防ぐことができます。これには、ウェブ リクエスト、クッキーの読み取り、JavaScript の埋め込み、XHR などのブロックが含まれます。

3. ユーザーにリスクをもたらす可能性がある権限を特定します。
    - 手順 1 で作成した拡張機能リストを確認します。インストールされている拡張機能と、その拡張機能に必要な権限を確認します。
        - 役立つヒント： 拡張機能の権限が不明確な場合があります。使いたい拡張機能の詳細についてはその拡張機能のベンダーにお問い合わせいただき、その拡張機能のパソコンやウェブサイトに対する影響について詳しく説明を受けてください。
    - 権限の宣言リストを確認します。このリストには、拡張機能が使用できるすべての権限が表示されます。ここで、組織で許可する権限を決定します。
        - 特定の拡張機能の権限に伴うリスクについては、権限のリスクに関するこちらのドキュメントをご確認ください。
4. 収集したデータから以下のようなリストを作成します。
    - 使いたい拡張機能： 部門、オフィスの所在地など、関連する情報に基づいて分類します。
    - 許可リスト： ブロックされるが、実行を許可する必要がある権限を持つ拡張機能。次のような例が考えられます。
        - ユーザーが必要としている拡張機能

        - ベンダーからの情報によりリスクがないと判断された拡張機能
    - ブロック リスト
        - インストールをブロックする拡張機能。
            - 実行を許可しない権限も含まれます。
        - 安全対策が必要で、拡張機能がアクセスができないウェブサイトとドメイン。
            - このブロックリストと既存のブロックリストを比較します。現在のブロックリストのポリシーを緩和できる場合があります。

5. 作成したリストを関係者と IT チームと共有し、承認を得ます。
6. ラボや組織内で小規模に試験運用して、新しいポリシーをテストします。
7. この新しいポリシーセットを従業員に段階的に展開します。
8. ユーザーからのフィードバックを確認します。
9. このプロセスを毎月、四半期、毎年繰り返し、微調整します。

これにより、許可またはブロックの権限のベースラインができます。機密性の高いウェブサイトが保護され、ユーザーエクスペリエンスが向上し、ブラウザのセキュリティが強化されます。従業員がこれまでインストールできなかった拡張機能をインストールできるようになる場合もあります。機密性の高いウェブサイトでは、管理者が望まない限りその拡張機能が動作することはありません。この方法を設定する手順については、このガイドの以下のセクションをご確認ください。

- 権限のブロックまたは許可により拡張機能を管理する
- ランタイムでホストをブロックする（機密性の高いウェブサイトの保護）
- ユーザーに対し拡張機能を自動インストールする
- 拡張機能を許可またはブロックする（必要な場合）

Chrome ブラウザ クラウド管理での拡張機能の管理の概要については、管理コンソールでの拡張機能の管理に関する YouTube 動画をご確認ください。

さまざまな拡張機能の管理ポリシーの概要

こうしたポリシーの多くについては、このドキュメントの他のセクションで詳しく説明します。ここでは、Windows のグループ ポリシーや Mac の plist を使用して拡張機能を管理するために、現在用意されているオプションをいくつかご紹介します（一部はアプリにも適用されます）。

- 拡張機能のインストールの許可リスト: ユーザー環境へのインストールを承認した拡張機能の一覧です。
- 拡張機能のインストールのブロックリスト: インストールを許可しない拡張機能の一覧です。すでにインストールされている拡張機能は無効になります。ユーザーがその拡張機能をインストールしようとすると、ブロックされます。また、Chrome ウェブストアでは [Chrome に追加] ボタンが赤く表示される新機能があり、拡張機能のインストールが許可されていないことがユーザーに通知されます。
- 拡張機能の自動インストール リスト: ユーザーのパソコンに拡張機能が自動インストールされます。ユーザーが拡張機能を無効にしたりアンインストールしたりすることはできません。この設定は、拡張機能のブロックリストのポリシーより優先されます。
- 外部の拡張機能のブロック: この設定により、外部ソースからの拡張機能のインストールがブロックされます。たとえば、アプリケーションをインストールすることでレジストリ経由で Chrome に拡張機能が追加される場合、この設定によりその拡張機能の読み込みが拒否されます。
- 許可されている拡張機能のタイプ: ここでは、インストールを許可する拡張機能とアプリのタイプのリストを作成できます。サポートされている値は、拡張機能、テーマ、ユーザー スクリプト、ホステッド アプリケーション、従来のパッケージ アプリケーション、プラットフォーム アプリケーションです。
    - 許可するものをすべてこのリストに含める必要があります。リストに含まれないものはインストールされません。
    - さまざまなタイプに関する詳細については、こちらの Chrome ウェブストアの拡張機能とアプリに関するページをご確認ください。
- 拡張機能のインストール元: 以前は、.crx ファイルのリンクをクリックすると警告がいくつか表示された後、Chrome により拡張機能のインストールを確認するメッセージが表示されました。この機能は、Chrome 21 以降、セキュリティ上の理由により削除されました。
    - このポリシーでは、このポリシーで指定する特定の URL に対して、その古いインストール機能を取得することができます。このポリシーで使用できる、こちらの URL の一致パターンに関するページをご確認ください。

- 拡張機能の設定: このポリシーはさまざまな機能を提供しており、JSON スクリプトを作成する必要があります。また、1 行の文字列形式にしなければなりません。
    - この設定は複雑になることがあるため、詳しくは、このドキュメントのさまざまなセクションで説明します。
        - Chrome ブラウザ クラウド管理には、JSON を記述しなくてもほぼすべての機能が含まれているほか、インストール済みの拡張機能も監査できます。この Chrome ブラウザ クラウド管理の使用を検討することをおすすめします。

包括的な命名規則に対する Google の取り組みに関する注記。以下のポリシーはサポートが終了しており、Chrome 97 で削除される予定です。したがって、それまでに新しいポリシーに切り替えてください。

- ExtensionInstallWhitelist は ExtensionInstallAllowlist に変更されます
- ExtensionInstallBlacklist は ExtensionInstallBlocklist に変更されます

権限に基づいて拡張機能をブロックする

ユーザーにインストールを許可する拡張機能は、権限を使用してコントロールできます。インストールされている拡張機能でも、その権限がブロックされていれば無効になります。権限がブロックされている拡張機能をインストールしようとしても、インストールできません。

Chrome ブラウザ クラウド管理で権限によって拡張機能を管理する

（Windows、Mac、Linux）

許可されていない権限を必要とする拡張機能をブロックできます。たとえば、拡張機能による USB デバイスへの接続をブロックしたり、Cookie へのアクセスを防いだりできます。

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ]** を選択します。
2. 拡張機能を許可するユーザーの組織部門を選択します。
3. [その他の設定] 歯車アイコン をクリックします 

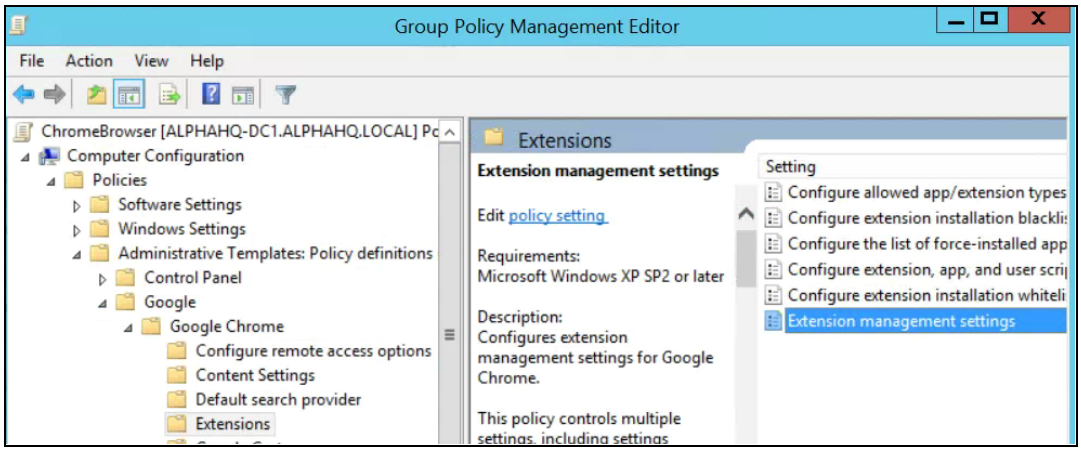
4. **[権限と URL]** セクションで、ブロックまたは許可する権限をそれぞれオンにします。

a. また、[ユーザーとブラウザ] タブで個別の拡張機能をクリックし、[権限と URL アクセス] > [このアプリまたは拡張機能のために権限をカスタマイズする] で、権限を使用して管理することもできます。
    i. 注: これは、該当の拡張機能に適用されているグローバル ポリシーよりも優先されます。
    ii. 各権限の詳細については、こちらの権限のリストをご確認ください。
5. [保存] をクリックします。

グループ ポリシーで権限によって拡張機能を管理する

(Windows のみ)

1. Microsoft 管理コンソールで、グループ ポリシー オブジェクトにアクセスします。
2. [編集] を右クリックします。
3. グループ ポリシー管理エディタで、**[ポリシー] > [管理用テンプレート] > [Google Chrome] > [拡張機能] > [拡張機能の管理設定]** を選択します。



拡張機能の管理設定のパス

4. ポリシーを有効にして、許可またはブロックする権限を入力し、1 つの JSON 文字列に圧縮します。

この JSON データの例に従って、形式を指定します(この例では、USB を使用する必要があるすべての拡張機能がブロックされます)。

```
{
        "*": {
                "blocked_permissions": ["usb"]
        }
}
```

コンパクト JSON データ:

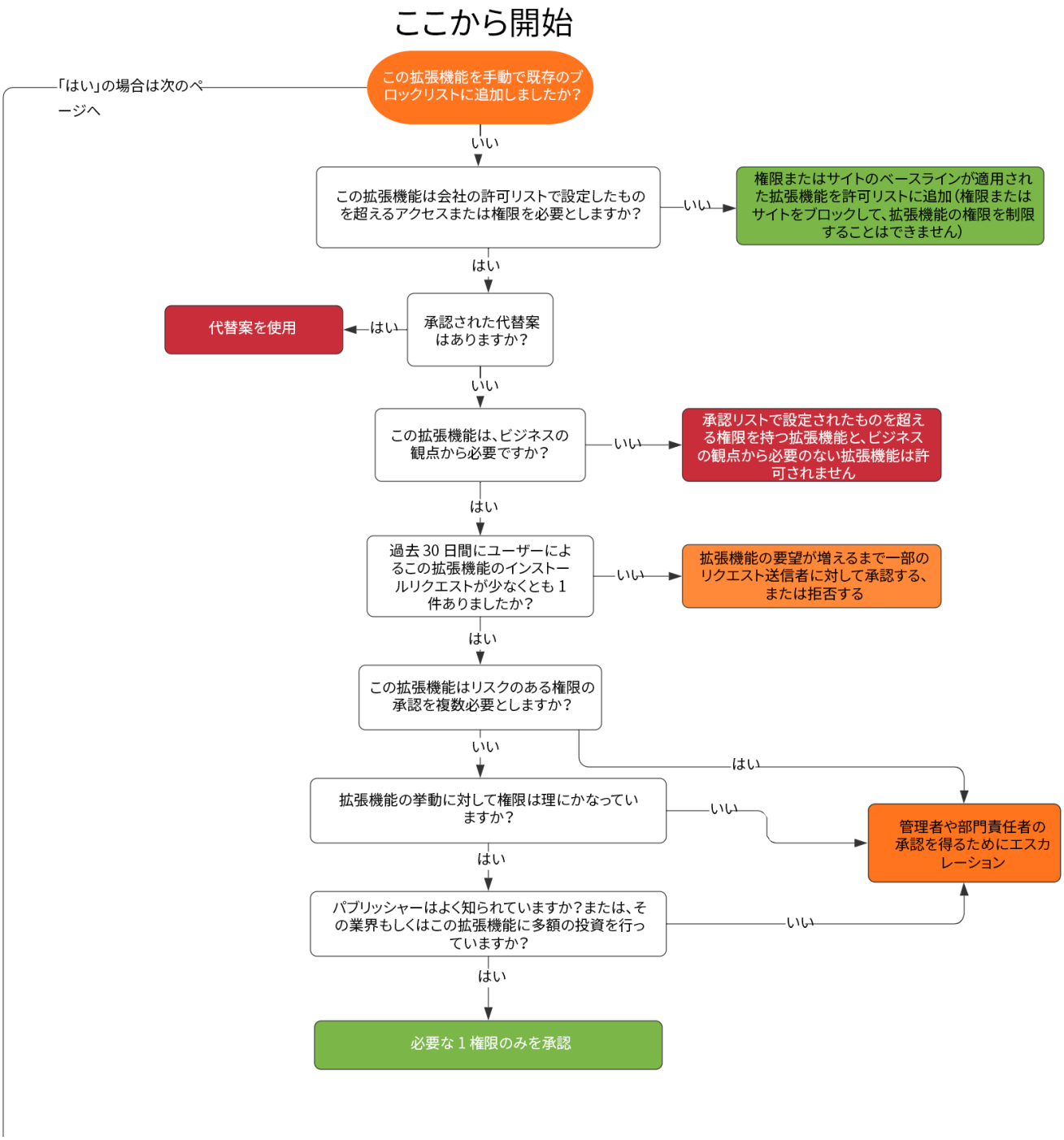
```
{"*":{"blocked_permissions":["usb"]}}
```

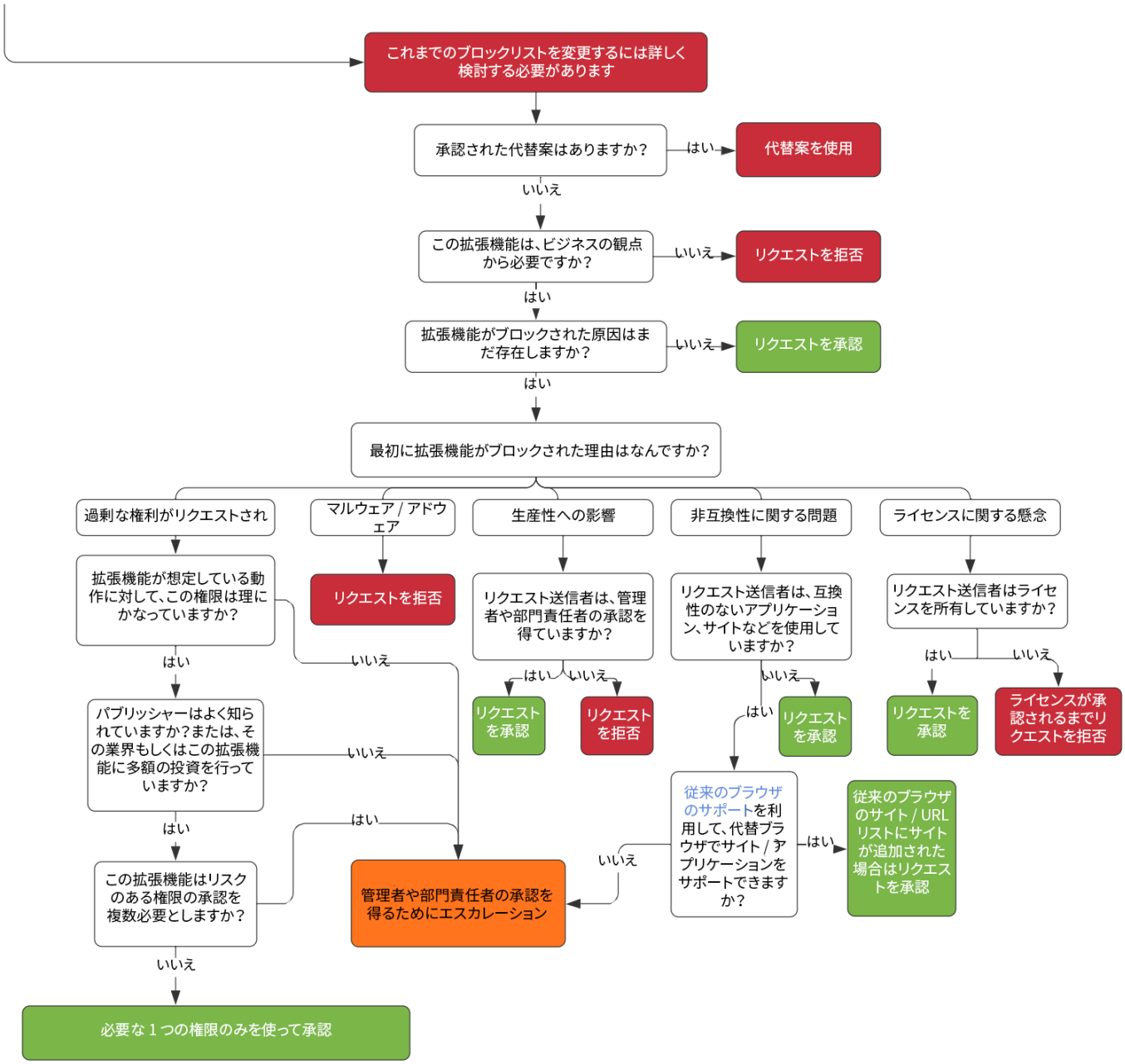
役立つヒント:

- その権限を使用しているすべての拡張機能をブロックするには、拡張機能 ID にアスタリスクを使用します（上記を参照）。
- JSON で複数の権限をブロックできます。以下の例では、すべての拡張機能について、power、printerProvider、serial、usb がブロックされます。
    - {"*":{"blocked_permissions":["power","printerProvider","serial","usb"]}}
- 1 つの拡張機能 ID を指定すると、ポリシーはその拡張機能にのみ適用されます。上の例では、* を拡張機能 ID に置き換えてください。 複数をブロックできますが、JSON 文字列内でそれぞれのエントリに分ける必要があります。
    - 拡張機能 ID を見つける手順については、このヘルプ記事の手順 3 をご確認ください。

リスクの高い権限を必要とする拡張機能を対象に例外プロセスを作成する

リスクが高いため企業の環境では実行できないと判断した権限が必要となる可能性のある拡張機能が、ビジネスで求められることがあります。例外的なワークフローがどのようなものかを説明するために、ここでは、使用したい拡張機能に、現在ブロックされている拡張機能が必要な場合のワークフローの例を示します。





- このフローは 1 つの例にすぎません。それぞれの企業に独自のワークフローや変更管理プロセスがあることに注意してください。

拡張機能の設定ポリシーで拡張機能を管理する

Windows には、拡張機能を管理する方法が複数用意されています。一般的には、拡張機能の設定ポリシーを使用して、JSON 文字列または Windows レジストリで複数のポリシーを設定します。
役立つヒント: このポリシーは、Mac、Chrome OS、Linux でサポートされています。ポリシーページには、こうした他のプラットフォームの値の例が記載されています。

このポリシーによって、拡張機能を最初にインストールするときのダウンロード元である更新 URL や、ブロックされている（実行が許可されていない）権限などの設定をコントロールすることができます。詳細については、Extension settings full description をご確認ください。また、ヘルプ記事ExtensionSettings ポリシーを設定するとアプリと拡張機能のポリシーもご確認してください。

すべての拡張機能の管理設定にこのポリシー使用するか、個別のポリシーを使用するかを決めることができます。

- ランタイムで許可またはブロックされているホストの設定（特定のウェブサイトで拡張機能をブロック）は、拡張機能の設定ポリシー内で GPO を介してのみ設定することができます。
    - また、Chrome ブラウザ クラウド管理からも設定できます。
- 拡張機能の設定ポリシーによって、グループ ポリシーの他の場所にある以下のようなポリシーが上書きされる場合があることに注意してください。
    - ExtensionAllowedTypes
    - ExtensionInstallAllowlist
    - ExtensionInstallForcelist
    - ExtensionInstallSources
    - ExtensionInstallBlocklist

拡張機能の設定ポリシーは、次の 2 つのいずれかの方法で設定されます。

- Windows レジストリ
- Windows グループ ポリシー エディタの JSON 文字列

ヒント:

- JSON 文字列の形式を適切に設定することは容易ではありません。ポリシーを実装する前に、JSON チェッカーを使用してください。
- JSON 形式の適切な設定が難しい場合は、レジストリ キーを使うこともできます。この方法を使用すると、対象パソコンの Chrome によって chrome://policy 内で JSON に変換されます。
    - この JSON をコピーすれば、拡張機能の設定ポリシーを使用して GPO 経由で適用できます。
    - この方法は、Chrome ブラウザ クラウド管理から拡張機能の設定を行い、JSON 出力をコピーすることによっても行うことができます。

Windows レジストリを使用して拡張機能ポリシーを設定する

ExtensionSettings ポリシーは、次のレジストリに書き込む必要があります。
`HKLM\Software\Policies\Google\Chrome\ExtensionSettings\`

- HKLM ではなく HKCU を使用できます。同等のパスを GPO を使用して設定できます。
- キーは、ユーザーのパソコンで選択した方法を使用して作成できます。

Chrome の場合、すべての設定が次のキーの下で開始されます。
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\`

作成する次のキーは、ポリシーのスコープを対象としています。1 つの拡張機能に適用する場合は、キーの名前を拡張機能 ID にします。すべての拡張機能に適用する場合は、キーの名前をアスタリスクにします。たとえば、Google Hangouts 拡張機能にのみ適用する設定の場合は、次の場所を使用します。
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd`

すべての拡張機能に適用する設定については、次の場所を使用します。
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*`

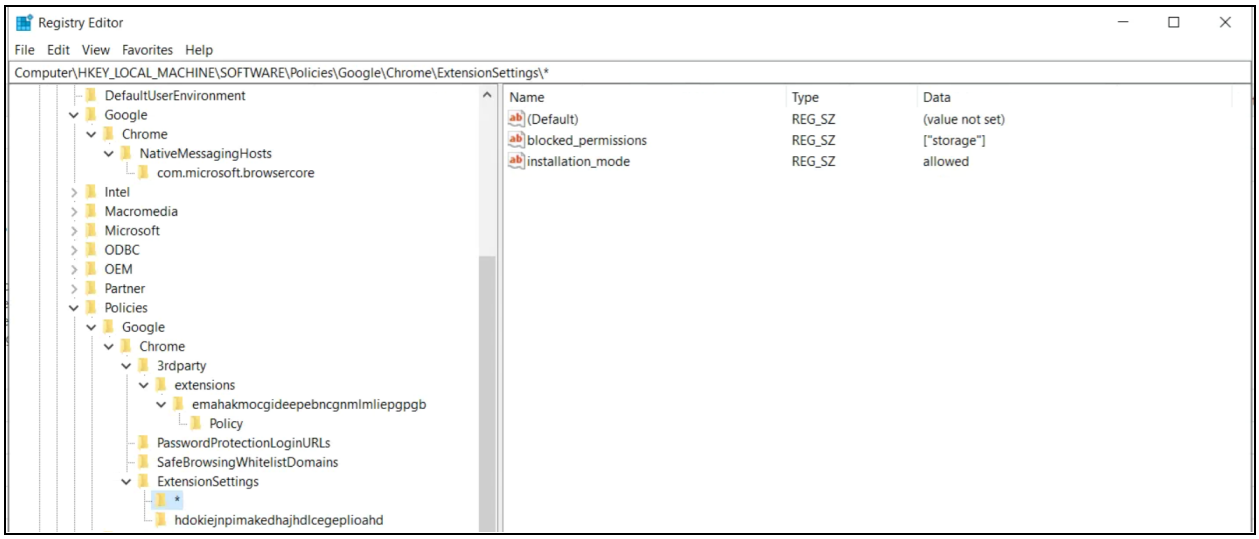
設定が違えば、必要な形式も異なります。つまり、設定が文字列なのか、文字列の配列なのかによって形式は異なります。配列の値には `["value"]` が必要です。文字列の値は、[" "] を付けずに入力できます。どの設定が配列でどの設定が文字列かを、次に示します。

- Installation_mode = 文字列
- update_url = 文字列
- blocked_permissions = 文字列の配列
- allowed_permissions = 文字列の配列
- minimum_version_required = 文字列
- runtime_blocked_hosts = 文字列の配列
- runtime_allowed_hosts = 文字列の配列
- blocked_install_message = 文字列

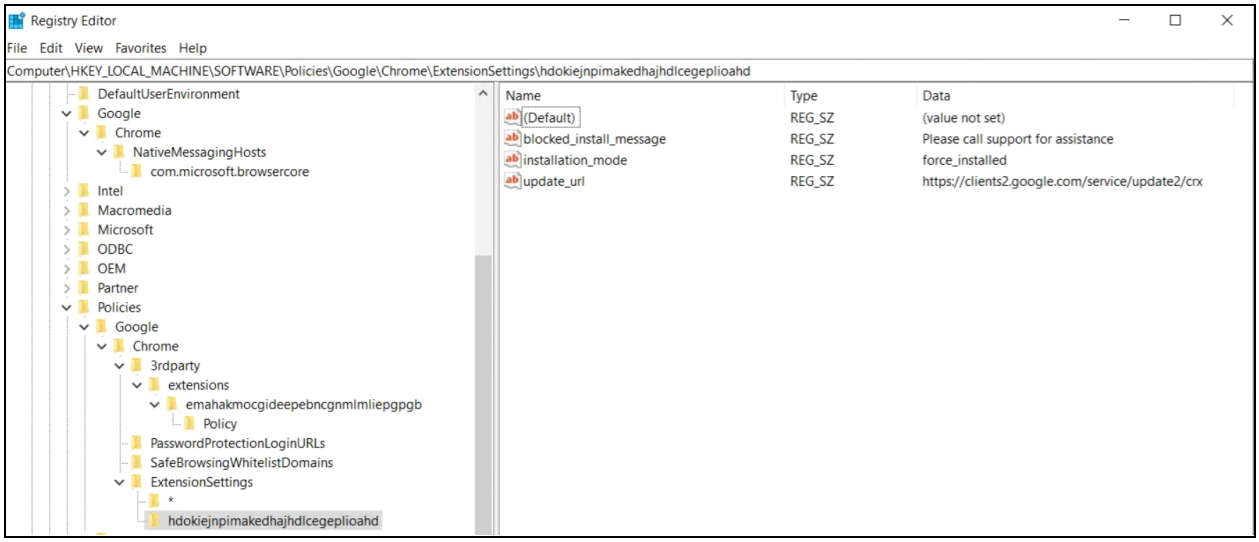
（ブロックされている権限のように）複数の値を 1 つの文字列で設定する構文の例を、次に示します。

- [“power”,”printerProvider”,”serial”,”usb”]

レジストリ内でキーの表示例:



デフォルト(*)のスコープキーとその値



個別のスコープとその値

ここでは、レジストリで設定されたキーは、ブラウザ内の chrome://policy にあるポリシーを使用して、JSON に変換されています。

Windows グループ ポリシー エディタで JSON 文字列を使用して設定する

GPO を使って拡張機能の設定ポリシーを使用する手順では、Chrome ポリシー用 ADM/ADMX がすでにインポートされていることが前提となっています。

その他の OS プラットフォームについては、Mac | Linux | Chrome OS をご確認ください

1. GPO 管理エディタで、[Google Chrome] > [拡張機能] > [拡張機能の管理設定ポリシー] を選択します。
2. ポリシーを有効にし、そのポリシーのコンパクト JavaScript Object Notation（JSON）データをテキスト ボックスに 1 行（改行なし）で入力します。
   ポリシーを検証し、1 行に縮めるには（JSON データの例は次項を参照）、サードパーティ製 JSON 圧縮ツールを使用します。

拡張機能の設定ポリシー用に JSON の形式を適切に設定する：
この方法を使用するには、このポリシーの 2 つの部分、つまりデフォルトのスコープと個別のスコープを理解する必要があります。デフォルトのスコープは、すべての拡張機能に適用されます。個別のスコープは、指定した拡張機能にのみ適用されます。

デフォルトのスコープは、アスタリスク（*）で特定されます。この例では、デフォルトのスコープと 1 つの個別の拡張機能スコープが定義されています。

```
{
   “*”: {},
   “nckgahadagoaajjgafhacjanaoiihapd”: {}
}
```

拡張機能は、1 つのスコープからのみ設定を取得します。その拡張機能に個別のスコープがある場合は、その設定が適用されます。個別の拡張機能スコープが存在しない場合は、デフォルトのスコープが使用されます。

次の JSON の例では、.example.com で実行されないようにすべての拡張機能をブロックし、USB 権限を必要とする拡張機能もすべてブロックしています。

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

コンパクト JSON データ:

```
{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}
```

拡張機能のインストールを管理するためのサンプル値を含む参照例

- allowed（デフォルト）
  ユーザーは、Chrome ウェブストアから拡張機能をインストールできます。
  JSON の例:
  `{ "*": {"installation_mode": "allowed" }}`

- "blocked"
  ユーザーは、Chrome ウェブストアから拡張機能をインストールできません。
  JSON の例:
  `{ "*": {"installation_mode": "blocked" }}`

- "blocked_install_message"
  インストールがブロックされたときに表示するカスタム メッセージを指定できます。
  JSON の例 - blocked_install_message:
  `{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}`

- “force_installed”
  - 拡張機能はユーザー操作なしで自動インストールされます。
  - ユーザーが拡張機能を無効にしたり削除したりすることはできません。

  `{ "*": {"installation_mode": "force_installed" }}`

- "normal_installed"
  拡張機能は、ユーザー操作なしで自動インストールされますが、ユーザーはその拡張機能を無効にすることができます。
  `{ "*": {"installation_mode": "normal_installed" }}`

- “removed”
  （Chrome バージョン 75 以降）ユーザーは拡張機能をインストールできません。ユーザーがすでにその拡張機能をインストールしていた場合は、Chrome ブラウザによって削除されます。
  `{ "*": {"installation_mode": "removed" }}`

- “toolbar_pin”

  拡張機能アイコンをツールバーに固定するかどうかを指定します。次のように設定できます。
  force_pinned - 拡張機能アイコンはツールバーに固定され、常に表示されます。ユーザーは拡張機能メニューでこのアイコンを非表示にすることはできません。
  default_unpinned - 拡張機能メニューに拡張機能アイコンは表示されなくなりますが、ユーザーはこのアイコンをツールバーに固定できます。
  この項目を設定しない場合、デフォルトは default_unpinned の動作になります。
  `{ "*": {"toolbar_pin": "forced_pinned" }}`

拡張機能によって installation_mode 機能が使用されている場合は、拡張機能のインストール元を示す「update_url」フィールドも定義する必要があります。

- ダウンロードする拡張機能が Chrome ウェブストアでホストされている場合は、「https://clients2.google.com/service/update2/crx」を使用します。

- 拡張機能を独自のサーバーでホストしている場合は、Chrome がパッケージ化された拡張機能（.crx ファイル）をダウンロードする URL を指定します。
  JSON の例 - update_url を含む force_installed 拡張機能:
  `{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url": "https://clients2.google.com/service/update2/crx"}}`
- Chrome 89 以降は、override_update_url 設定を使用して、update_url フィールドの URL または ExtensionInstallForcelist ポリシーで指定された更新 URL が、以降の拡張機能の更新において Chrome で使用されるように指定することもできます。
  - このポリシーを未設定のままにするか false に設定した場合は、拡張機能のマニフェストで指定した URL を使用して更新が行われます。

拡張機能がウェブページを変更できないようにする

この設定により、拡張機能は最も機密性の高いウェブサイトのデータの変更や読み取りを行えなくなります。
このポリシーは、拡張機能による以下の処理をブロックします。

- ウェブサイトへのスクリプトの挿入
- Cookie の読み取り
- ウェブリクエストの変更

この設定では、ユーザーによる拡張機能のインストールや削除を禁止することはできません。指定したウェブサイトが拡張機能によって変更されることを防ぐだけです。

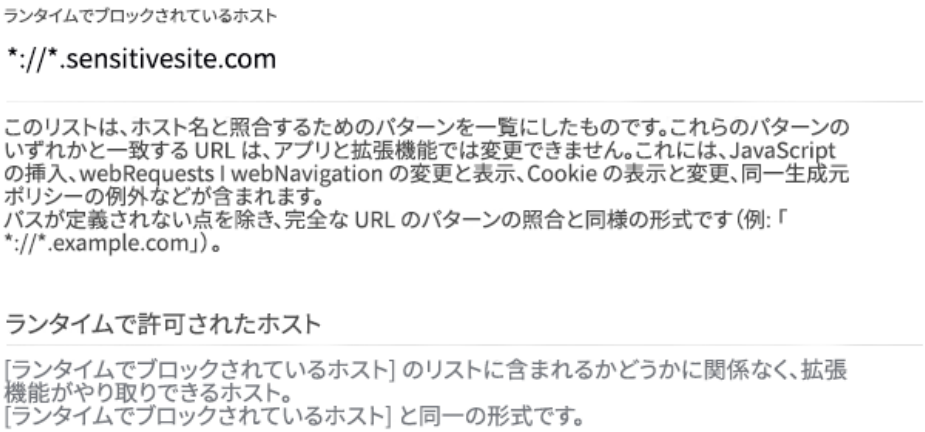
この機能の設定は 2 つあります。

- **runtime_blocked_hosts** - 拡張機能と、これらのホストとのやり取りがブロックされます。
- **runtime_allowed_hosts** - runtime_blocked_hosts で定義されている場合でも、拡張機能は、このリストのホストとはやり取りできます。

役立つヒント: runtime_blocked_hosts と runtime_allowed_hosts の各インスタンスでは、最大 100 個のホストパターンを定義できます。この数を超えると、ポリシーは無効になります。

Chrome ブラウザ クラウド管理
ランタイム ホストによるブロックは、GPO よりも Chrome ブラウザ クラウド管理で行う方が簡単です。JSON を必要とせず、ブロックする URL を拡張機能の設定に入力するだけの簡単な作業です。これを設定するには、ブラウザのデバイスを Chrome ブラウザ クラウド管理に登録する必要があります。この機能には、追加費用はかかりません。登録の手順については、こちらをご確認ください。

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ]** を選択します。
2. 拡張機能を許可するユーザーの組織部門を選択します。
3. [追加の設定] 歯車アイコン をクリックします。
4. 拡張機能を実行させたくない機密性の高いウェブサイトの URL を、[ランタイムでブロックされているホスト] に入力します。構文の情報については、ブロックまたは許可されている URL の構文に関するページをご確認ください
   a. 複数の URL を入力するには、1 つの URL を入力したら Enter キーを押し、新しい URL を入力します。
   b. 個別の拡張機能をクリックし、[権限と URL アクセス] で、許可されているホストとブロックされているホストを設定することもできます。
      i. 注: これは、該当の拡張機能に適用されているグローバル ポリシーよりも優先されます。
      ii. また、[ランタイムでブロックされているホスト] の URL に対する例外処理のための [ランタイムで許可されたホスト] もあります。
5. [保存] をクリックします。



[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] > [追加の設定] のランタイム ホストの項目
GPO

ここでは、Windows パソコンでこの GPO を管理する手順について説明します。その他のプラットフォームについては、Mac | Linux をご確認ください

拡張機能の設定ポリシーでは、以下の設定によってウェブサイトやドメインの変更をブロック（または許可）することができます。

- Runtime_blocked_hosts
  選択したウェブサイトでの拡張機能によるデータの変更や読み取りをブロックします。

- Runtime_allowed_hosts
  選択したウェブサイトでの拡張機能によるデータの変更や読み取りを許可します。

いずれのポリシーでも、JSON 文字列でサイトを指定するには次の形式を使用します。

```
[http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
```

注: [hostname|*] および [eTLD|*] セクションは必須ですが、[subdomain|*] セクションはオプションです。

有効なホストパターンと一致パターンの例:

有効なホストパターン	一致する	一致しない
://.example.*	http://example.com https://test.example.co.uk	https://example.google.com http://example.google.co.uk
http://example.*	http://example.com http://example.ly	https://example.com http://test.example.com
http://example.com	http://example.com	https://example.com http://test.example.co.uk
://	すべての URL	

次の JSON 文字列のサンプルは、1 つの拡張機能について、アクセスをブロックしています。この文字列は、1 つの拡張機能による特定のサイトの拡張を防ぎます。

```
{
	"aapbdbdomjkkjkaonfhkkikfgjllcleb": {
		"runtime_blocked_hosts": ["*://*.importantwebsite"]
	}
}
```

コンパクト JSON データ:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

次のサンプルは、すべての拡張機能について、複数のサイトをブロックしています。

```
{
   "*": {"runtime_blocked_hosts": [ "*://*.importantwebsite.com",
"*://*.importantwebsite2.com" ]
   }
```

コンパクト JSON データ:

```
{"*":{"runtime_blocked_hosts":["*://*.importantwebsite.com","*://*.importantweb
site2.com"]}}
```

拡張機能が複数ある場合は、ブロックするアプリ ID ごとにそれぞれを独立したエントリに分けます。次の例は、2 つの拡張機能が同じドメインで実行されないようにする方法を示しています。

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      },
      "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

コンパクト JSON データ:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn":
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

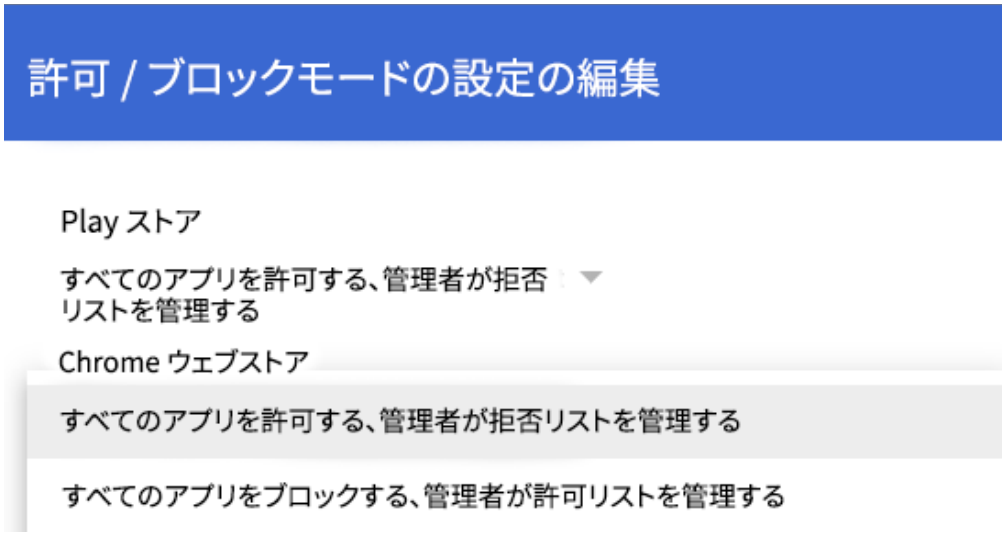
Google 管理コンソールで拡張機能を許可またはブロックする

管理者は、許可リストとブロックリストを作成することで、ユーザーがインストールできる拡張機能を管理します。ユーザーによる任意のアプリや拡張機能のインストールを許可できます。すべてのユーザーまたは特定の従業員がアプリをブロックまたは許可するように、ポリシーを設定することができます。

次の手順は、管理者が管理コンソールでの設定変更に慣れていることを前提としています。

一部の拡張機能をブロックし、それ以外のすべての拡張機能を許可する

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] > [追加の設定]** を選択します。
2. 左側で、拡張機能を許可する組織部門を選択します。
3. 下にスクロールして Chrome ウェブストアの [許可 / ブロックモード] に移動し、[編集] をクリックして、**[すべてのアプリを許可する、管理者が拒否リストを管理する]** オプションを選択します。

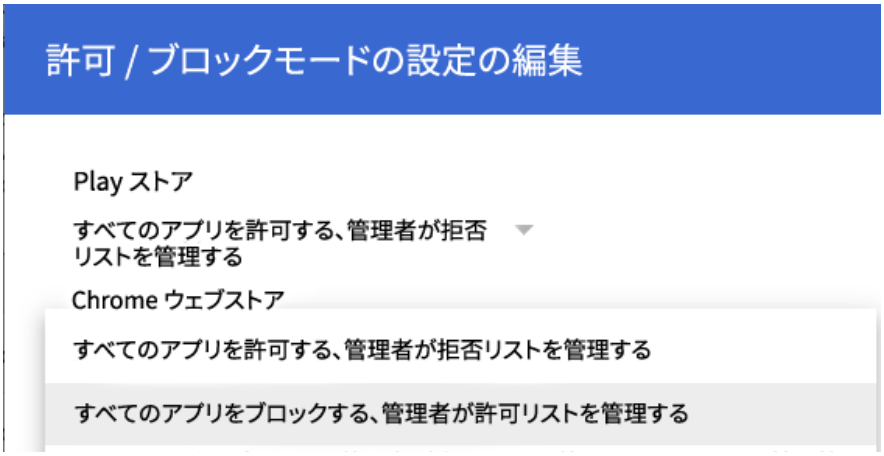


許可 / ブロックモードの設定

4. [保存] をクリックします。
5. [ユーザーとブラウザ] タブをクリックして、前のページに戻ります。
6. 右下の黄色のプラス記号をクリックして、ブロックする各拡張機能を追加します。
7. その拡張機能をコンソールに追加する方法を選択します（[Chrome ウェブストアから追加]、[拡張機能を ID で追加]、[URL で追加]）。
8. 拡張機能の横のプルダウンで [ブロック] を選択します。
9. [保存] をクリックします。

一部の拡張機能を許可し、それ以外のすべての拡張機能をブロックする

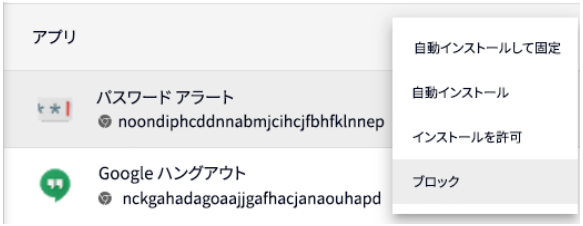
1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] > [追加の設定]** を選択します。
2. 左側で、拡張機能をブロックする組織部門を選択します。
3. 下にスクロールして [Chrome ウェブストア] の [許可 / ブロックモード] に移動し、**[すべてのアプリをブロックする、管理者が許可リストを管理する]** オプションを選択します。



4. [保存] をクリックします。
5. [ユーザーとブラウザ] タブをクリックして、前のページに戻ります。
6. 右下の黄色のプラス記号をクリックして、許可する各拡張機能を追加します。
7. その拡張機能をコンソールに追加する方法を選択します（[Chrome ウェブストアから追加]、[拡張機能を ID で追加]、[URLで追加]）。
8. 拡張機能の横のプルダウンで [インストールを許可] を選択します。
   a. [自動インストールする] を選択して、ユーザーのパソコンに拡張機能を自動インストールすることもできます。
9. [保存] をクリックします。

1 つの拡張機能をブロックまたは許可する

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ]** を選択します。
2. 許可またはブロックする拡張機能の組織部門を選択します。
   - 注: 組織部門の設定は親組織部門から継承されますが、サブ組織部門ごとに上書きすることができます。
3. ブロックまたは許可する拡張機能を選択するか、それを追加します（前のセクションの手順 6 と 7 を参照）。
4. インストール ポリシー列で、[ブロック]、[自動インストール]、または [インストールを許可] を選択します。

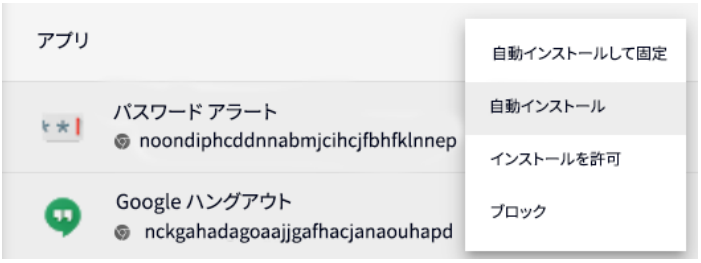


5. [保存] をクリックします。

拡張機能の自動インストール

ユーザーに拡張機能が必要であることがわかっている場合は、そのユーザーのためにインストールすることができます。拡張機能を自動インストールすると、実行に必要なすべての権限が付与されます。また、ユーザーがこれを削除することはできず、通知なくインストールされます。拡張機能を自動インストール リストから削除すると、その拡張機能はユーザーのパソコンから削除されます。

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ]** を選択します。
2. 拡張機能の自動インストール先組織部門を選択します。
3. 自動インストールする既存の拡張機能を選択するか、それを追加します。
   a. インストールする拡張機能を追加するには、右下の黄色のプラス記号をクリックします。
   b. その拡張機能をコンソールに追加する方法を選択します ([Chrome ウェブストアから追加]、[拡張機能を ID で追加]、[URLで追加])。
4. 自動インストールする拡張機能を選択し、インストール ポリシー列で、プルダウン メニューから [自動インストール] を選択します。



5. [保存] をクリックします。

ユーザーに表示される、管理者選択の拡張機能のカスタム Chrome ウェブストア コレクションを作成することができます。この設定では、ユーザーは企業の認証情報を使用して、Google ID にログインする必要があります。

- この設定は、管理コンソールの [デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] > [その他の設定] > [Chrome ウェブストアのホームページ] > [Chrome ウェブストア コレクションを使用する] にあります

- その後、すべての拡張機能をこのページに表示するか、[ユーザーとブラウザ] セクションで個別の拡張機能をクリックし、[Chrome ウェブストアのコレクションに追加する] を選択できます。

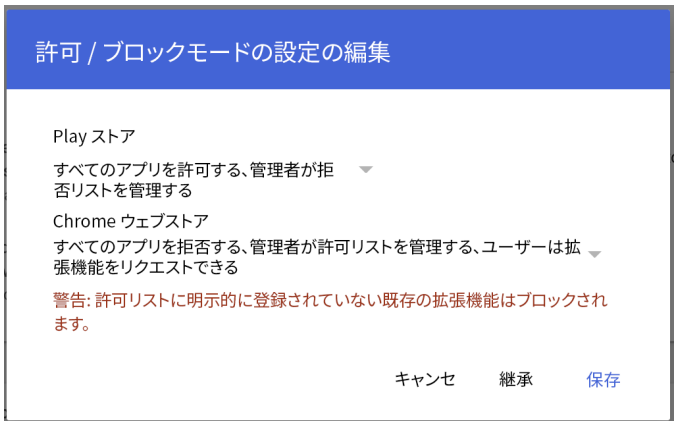
ユーザーが拡張機能をリクエストできるようにする: 拡張機能ワークフロー

管理者は Google 管理コンソールを使用して、Chrome ウェブストアでの拡張機能のリクエストをユーザーに許可できます。さらに、ユーザーがリクエストした拡張機能を許可、ブロック、自動インストールできます。

Chrome ウェブストアのリクエスト ダイアログの例

この機能は、許可 / ブロックリストとして動作します。この機能をオンにすると、すべての拡張機能がデフォルトでブロックされます。問題が発生しないように、次のプロセスを踏むことをおすすめします。

1. Chrome ブラウザ クラウド管理で拡張機能のデータ エクスポート レポートを使用して、ユーザーが現在使用している拡張機能を確認します。
    - 詳しくは、データ エクスポート API の設定に関する YouTube 動画をご確認ください。
2. 手順 1 で収集したデータに基づいて、重要な拡張機能（GPOまたは管理コンソール）のリストを作成します。
3. **[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ] > [その他の設定]** > [許可 / ブロックモード] で、拡張機能ワークフロー機能をオンにして、編集ボタンを押します。
4. Chrome ウェブストアで、プルダウン メニューから **[すべてのアプリを拒否する、管理者が許可リストを管理する、ユーザーは拡張機能をリクエストできる]** を選択します。



管理コンソールで拡張機能ワークフローを有効にする

- はじめに、エンドユーザーに問題が発生しないように、テスト環境になっている組織部門の一部のユーザーとデバイスに設定を適用し、フィードバックを収集することをおすすめします。準備ができたら、組織全体に設定を適用することができます。

5. 承認と拒否のリクエストは、**[デバイス] > [Chrome] > [アプリと拡張機能] > [リクエスト]** で管理されます。
6. 確認する拡張機能のリクエストの行をクリックします。
7. ここで拡張機能の詳細を確認し、プルダウン メニューからインストール ポリシーを選択できます。
   - 自動インストール - 拡張機能は通知なくインストールされ、削除できません
   - インストールを許可 - ユーザーが拡張機能をインストールできるようにします
   - ブロック - ユーザーが拡張機能をインストールできないようにします。拡張機能をインストールしたユーザーから、その拡張機能を削除します

この機能の詳細については、ヘルプセンターの拡張機能のワークフローに関する記事、またはこちらの拡張機能のワークフローに関する YouTube 動画でご確認ください。

グループ ポリシーで拡張機能を許可またはブロックする

開始する前に： 以下の手順は、ユーザー用に Chrome がすでに管理されていることを前提としています。Windows に Chrome をデプロイする方法については、Chrome ブラウザ デプロイ ガイド（Windows）をご確認してください。Mac® へのデプロイとポリシー管理については、Mac で Chrome ブラウザを設定するをご確認ください。

Windows の場合、2 種類のポリシー テンプレート（ADM テンプレートと ADMX テンプレート）があります。ご利用のネットワークで使用できるタイプをご確認ください。テンプレートには、Chrome の設定に使用できるレジストリ キーと、指定できる値が記載されています。Chrome の動作は、これらのレジストリ キーの設定値を参照して決定されます。

1. Chrome ポリシーのテンプレートをダウンロードします。
   Windows 用テンプレートと、すべてのオペレーティング システムに共通のポリシーに関するドキュメントは、こちらのリンクから入手できます
2. ダウンロードした ADM テンプレートまたは ADMX テンプレートを開きます。
   a. **[スタート] > [ファイル名を指定して実行]** を選択し、「**gpedit.msc**」を実行します。
   b. **[ローカル コンピュータ ポリシー] > [コンピュータの構成] > [管理用テンプレート]** を選択します。
   c. [管理用テンプレート] を右クリックし、[テンプレートの追加と削除] を選択します。

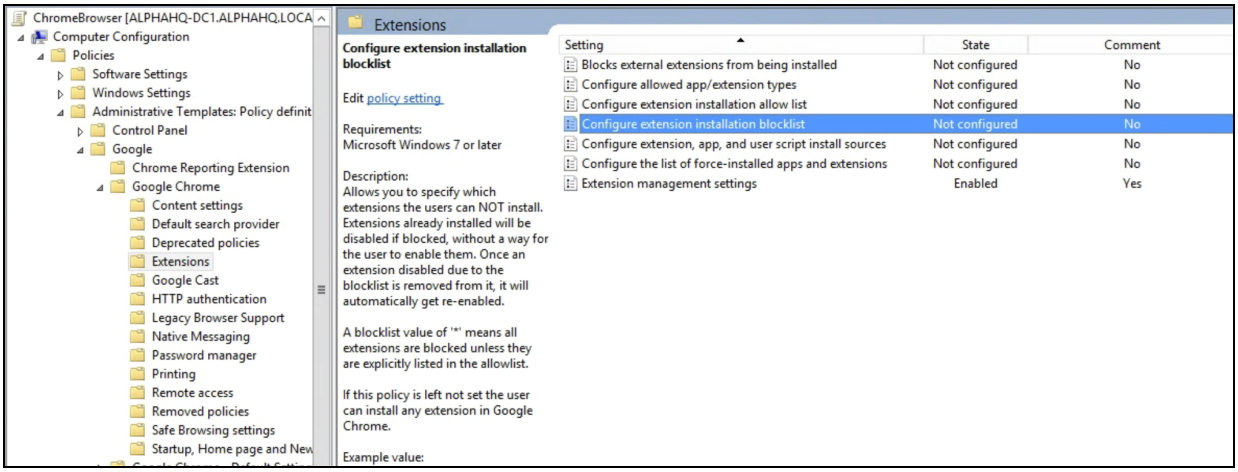
d. ダイアログで chrome.adm テンプレートを追加します。

その後、その場所にまだない場合は、[管理用テンプレート] の下に Google または Google Chrome フォルダが表示されます。

- Windows 7 または Windows 10 に ADM テンプレートを追加する場合は、[従来の管理用テンプレート] > [Google] > [Google Chrome] の下に表示されます。

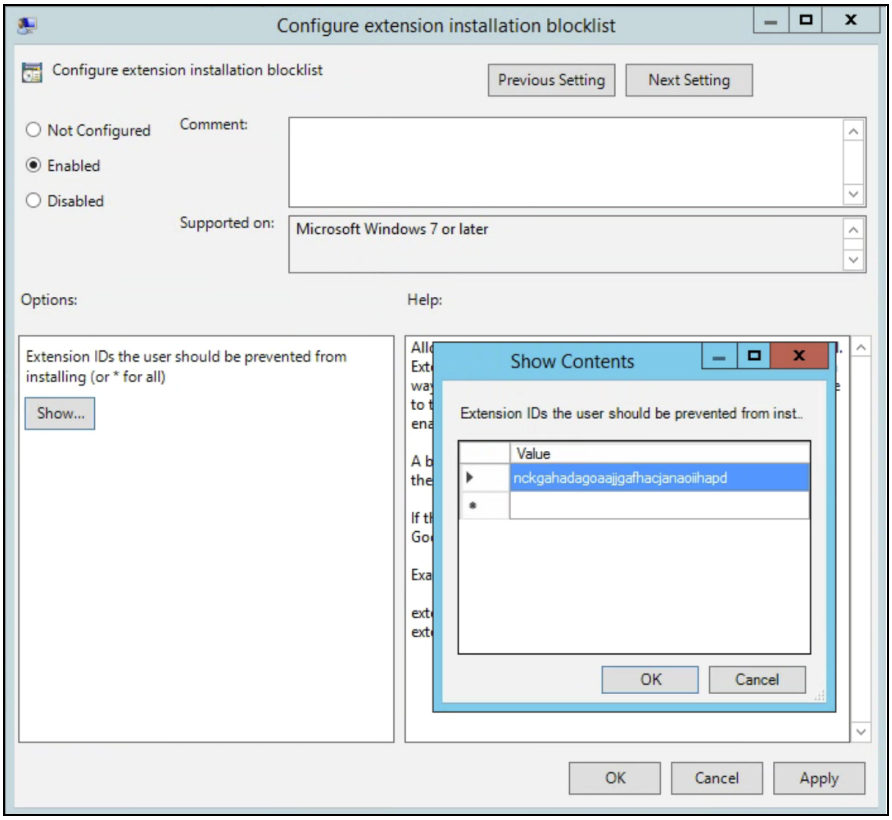
一部の拡張機能をブロックし、それ以外のすべての拡張機能を許可する

1. 追加したテンプレートを、グループ ポリシー エディタで開きます。
2. [Google] > [Google Chrome] > [拡張機能] > [拡張機能インストールの拒否リストを設定する] に移動します。



拡張機能の管理ポリシーへのパス

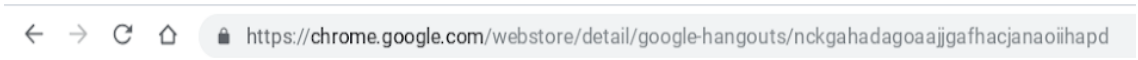
2. 設定で [有効] を選択します。
3. [表示] をクリックします。
4. ブロックする拡張機能のアプリ ID を入力します。



拡張機能インストールのブロックリストを設定する

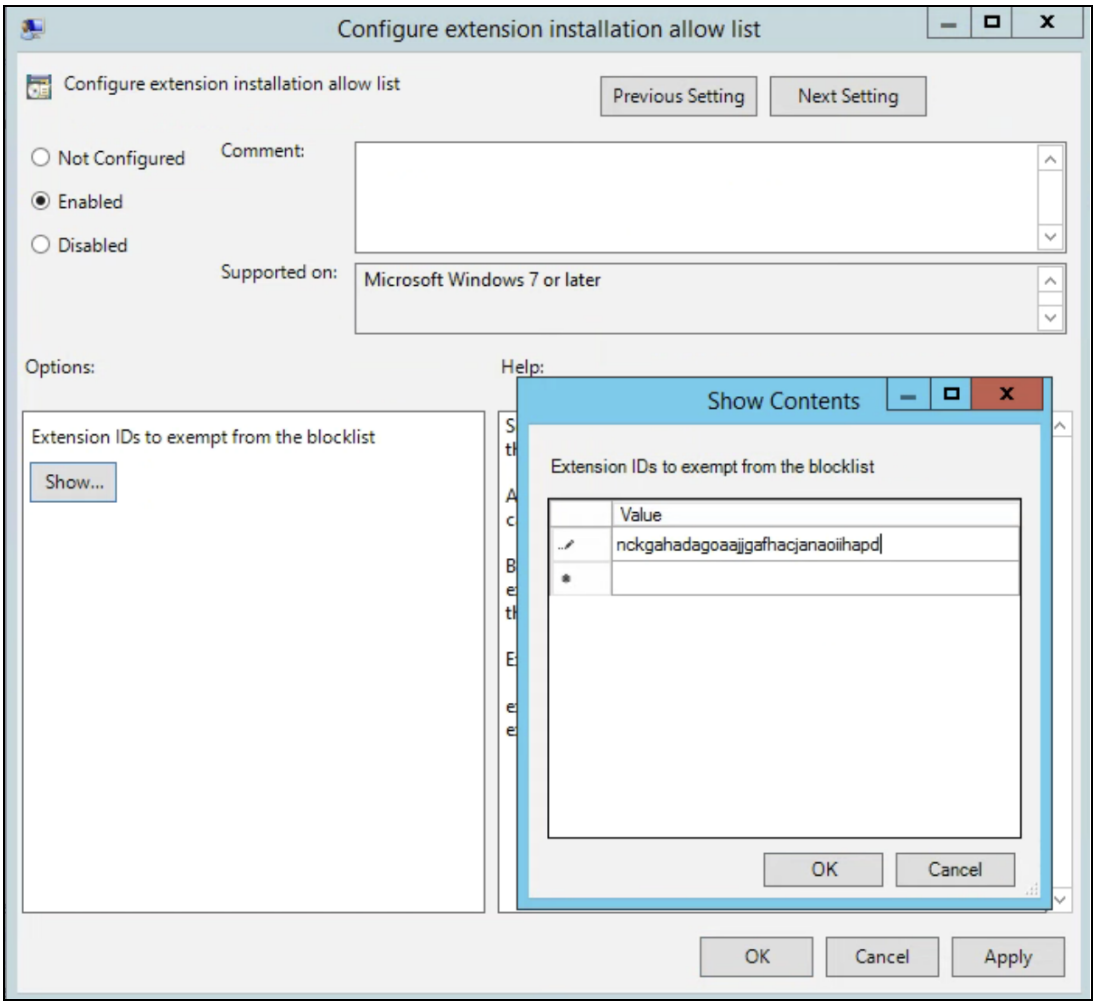
注:

- 拡張機能のアプリ ID が見つからない場合は、Chrome ウェブストアで確認します。拡張機能のアプリ ID は、Chrome アドレスバーに表示されている URL の末尾に示されます。



google-hangouts/ の後ろに配置されているアプリ ID の例

- ポリシーに「*」と入力すると、すべての拡張機能がインストールされなくなります。これは、拡張機能インストールの許可リストの設定ポリシーで使用できます。この方法を使用すると、特定の拡張機能のみをユーザーがインストールできるようにして、それ以外の拡張機能はすべてブロックできます。
- ユーザーのパソコンにすでにインストールされている拡張機能を、拒否リストに追加できます。これにより拡張機能が無効になり、ユーザー側では再度有効にすることができなくなります。アンインストールはされません。無効になるだけです。



拡張機能インストールの許可リストを設定する

1 つの拡張機能をブロックまたは許可する

1 つの拡張機能をブロックするには、その拡張機能のアプリ ID を、拡張機能インストールのブロックリストの設定ポリシーに追加します。それ以外の拡張機能はすべて、インストールが許可されます。

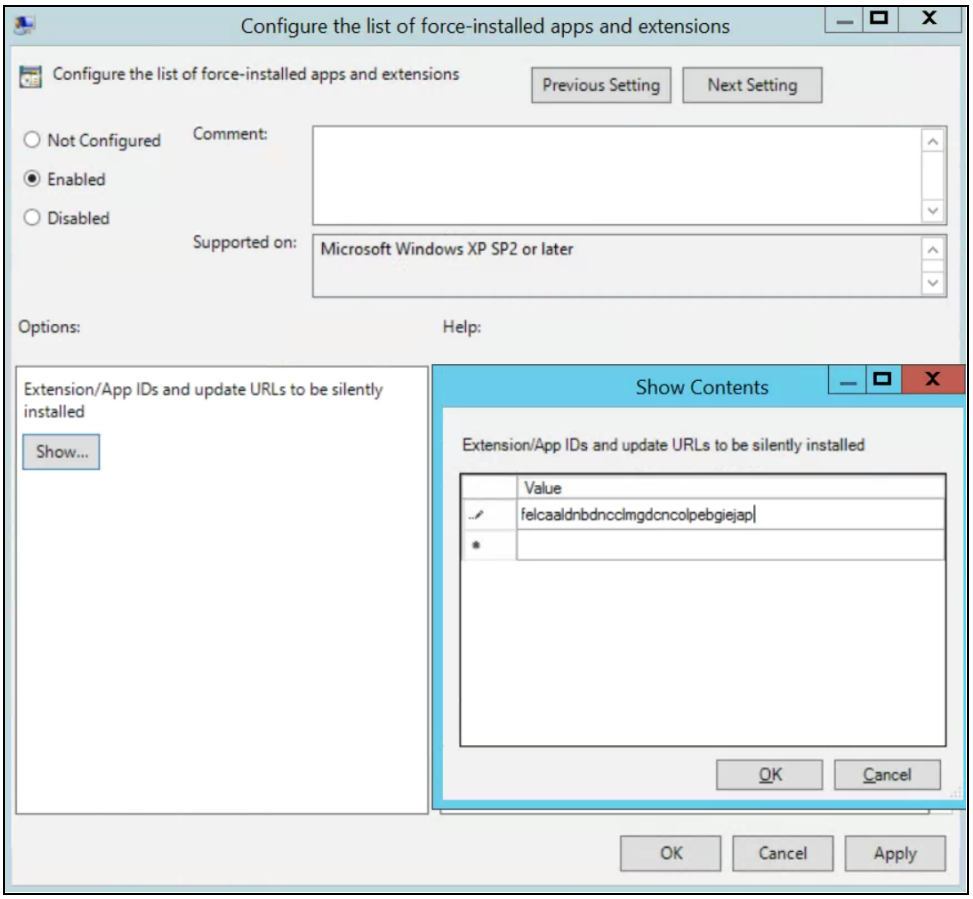
1 つの拡張機能を許可するには:

1. 拡張機能インストールのブロックリストの設定ポリシーのコンテンツ セクションに、「*」と入力します。これにより、リストに含まれる拡張機能はすべて、インストールがブロックされます。
2. 許可された拡張機能のアプリ ID を、拡張機能インストールの許可リストの設定ポリシーに追加します。

拡張機能を自動インストールする

1. グループ ポリシー エディタで、[Google] > [Google Chrome] > [拡張機能] > [自動インストールするアプリと拡張機能のリストの設定] に移動します。
2. [有効] を選択します。
3. [表示] をクリックします。
4. 自動インストールする拡張機能のアプリ ID を入力します。

拡張機能は通知なしでインストールされます。ユーザー操作は必要ありません。ユーザーは、拡張機能をアンインストールすることも無効にすることもできなくなります。この設定は、有効になっている可能性のあるブロックリスト ポリシーよりも優先されます。



自動インストールするアプリと拡張機能のリストを設定する

ポリシーの検証

ポリシーが有効であること、また意図したとおりに動作することを確認するには、そのポリシーをテストパソコンに適用します。テストパソコンでの手順は次のとおりです。

1. chrome://policy に移動します
2. [ポリシーを再読み込み] ボタンをクリックします
3. ページの右上隅のポリシーフィルタで「ExtensionSettings」と入力し、このポリシーのみを表示します。
4. [値が設定されていないポリシーを表示する] チェックボックスをオンにします
5. ポリシーの [ステータス] が [OK] になっていることを確認します
6. [値を表示] をクリックしてポリシーを展開し、空白でないことを確認します
7. これで有効なポリシーがあることを確認できました

独自の拡張機能の自己ホスティング

Chrome ウェブストアは拡張機能をホストしており、多くのセキュリティ機能を提供しています。

- 自動コードスキャンや手動コードスキャンなどの機能。
    - 悪意のあるコードがユーザーに送信されることを防ぎます。

しかし、Chrome ウェブストアとは別に、独自のサーバーで拡張機能をホストするオプションもあります。ここでは、この方法の長所と短所をご紹介します。

長所:

- 独自の拡張機能のホスティングには、Chrome ウェブストアのルールや要件が適用されません。
    - このため、拡張機能に対する監視が緩く、利用規約違反によって拡張機能が削除されるリスクを抑えることができます。

短所:

- 自己ホスティングではより多くの設定作業が必要です。また、拡張機能ファイル用に独自のファイル サーバーをホストしなければなりません。
- 拡張機能のセキュリティの検証と更新には手間がかかります。Chrome ウェブストアではこれが自動的に実施されます。

このセクションでは、拡張機能を自己ホストする方法を説明します。Chrome ウェブストアを使わずに拡張機能をパッケージ化し、ホストする方法のほか、こうした拡張機能をデバイスやユーザーにデプロイする方法についてもご紹介します。

拡張機能の自己ホスティングの代替案

拡張機能の公開オプション

自己ホスティングの代わりに、Chrome ウェブストアで内部の拡張機能を非公開として指定することをご検討ください。拡張機能には、一般公開、非公開、限定公開の 3 つの公開オプションがあります。次の表は、それぞれの長所と短所を詳しく示しています。

	Chrome ウェブストアの検索に表示されるか？	ログインが必要？	Chrome ブラウザ クラウド管理対応？
一般公開	はい	いいえ	はい
非公開	いいえ	はい	はい
限定公開	いいえ	いいえ - ユーザーがインストールするにはリンクが必要	はい

詳細については、こちらのブログをご確認ください。このブログでは、拡張機能を自己ホストせずに、一般に公開することなく公開する方法をご紹介しています。

- 管理コンソールで拡張機能を管理している場合、[Chrome ウェブストアのアクセス許可] 設定で、非公開の拡張機能がユーザーに表示されるように設定する必要があることに注意してください。
    - この設定は、管理コンソールの [デバイス] > [Chrome] > [アプリと拡張機能] > [追加の設定] > [Chrome ウェブストアのアクセス許可] にあります。ここで、Chrome ウェブストアで自分のドメインに限定された非公開アプリを、他のユーザーが公開できるように設定します。

管理コンソールで拡張機能を特定のバージョンに固定する

Google 管理コンソールに、拡張機能の管理オプションがいくつか新しく追加されました。まず、管理コンソールで直接、拡張機能のバージョンを固定できるようになりました。これにより、特定のバージョンの拡張機能を必要とする企業での安定性がより高まります。古いバージョンの拡張機能に固定することはおすすめしません。古いバージョンへの固定は、最新の機能とセキュリティ アップデートを確保するための一時的な措置としてご利用ください。この機能は、自動インストールされた拡張機能にのみ利用できます。詳細については、こちらのヘルプセンターの記事をご確認ください。

1. 管理コンソールで、**[デバイス] > [Chrome] > [アプリと拡張機能] > [ユーザーとブラウザ]** を選択します。
2. 固定する拡張機能がある組織部門を選択します。
3. バージョンによって管理する既存の拡張機能を選択（または新しい拡張機能を追加）し、[バージョンの固定] 列で固定するバージョンをプルダウン メニューから選択して [保存] を押します。
    a. アプリや拡張機能を固定すると、セキュリティ アップデートや互換性アップデートなどのアップデートを取得できなくなることに注意してください。
    b. また、設定時に Chrome ウェブストアに存在する、最新バージョンの拡張機能にのみ固定することができます。
    c. 自己ホスト型アプリや拡張機能を固定し、管理コンソールで URL を更新することもできます。こちらのヘルプセンターの自己ホスト型アプリの固定に関するセクションをご確認ください。

管理コンソールでのバージョン固定

自己ホスティング拡張機能の要件

拡張機能をホストするには、拡張機能とそのマニフェスト ファイルのための独自のウェブ ホスティング サービスが必要になります。このホスティング場所では、認証を要求すべきではありません。この場所には、デバイスがどこで使

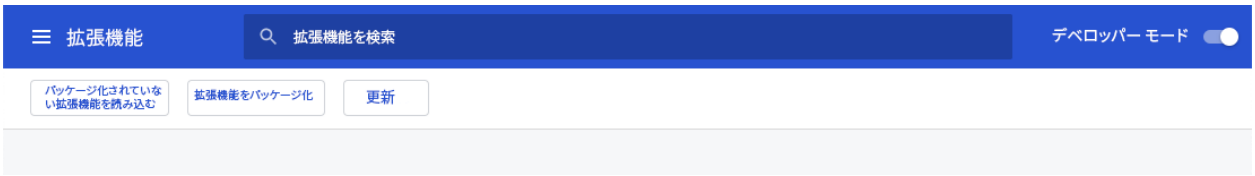
用されていても、そこからアクセスできなければなりません。社内のリポジトリでファイルをホストする場合は、この点に注意してください。

この手順は、すでに拡張機能が作成済みで、XML ファイルの使用経験があることを前提としています。また、グループ ポリシーと Windows レジストリの使用に関する知識も必要です。この手順は、自分で開発していないサードパーティの拡張機能には適用されません。サードパーティの拡張機能を自己ホストするには、拡張機能のベンダーに直接ご相談ください。

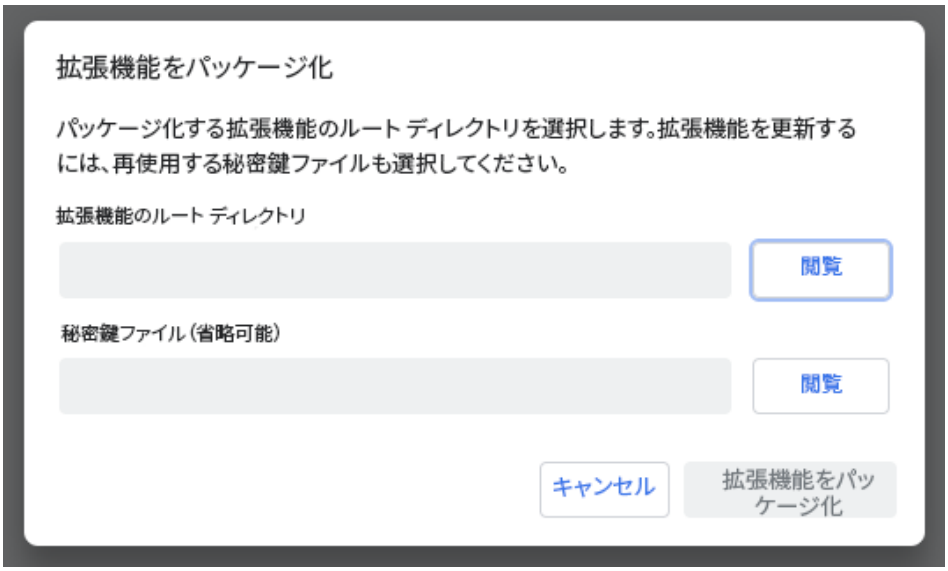
拡張機能のパッケージ化

拡張機能はまず、CRX ファイルにパッケージ化する必要があります。拡張機能が CRX ファイルとしてパッケージ化されていない場合の手順は以下のとおりです。

1. Chrome のアドレスバーを使用して **chrome://extensions** にアクセスし、[デベロッパー モード] のチェックボックスをオンにします。



2. デベロッパー モードで、[拡張機能をパッケージ化] をクリックして CRX ファイルを作成します。



3. ソースがあるディレクトリを選択します。これにより CRX ファイルと PEM ファイルが作成されます。
役立つヒント: PEM ファイルは安全に保管してください。これは拡張機能の鍵であり、今後更新の際に必要となります。

4. CRX を拡張機能ウィンドウにドラッグし、読み込まれることを確認します。
    a. Windows と Mac では、この拡張機能はデフォルトで無効になります。Linux では無効になりません。
5. 拡張機能をテストして、ID フィールドとバージョン番号をメモします。
これらは今後重要になってきます。

6. CRX ファイルをホスト場所に配置します。ユーザーやデバイスは、この場所からそのファイルをダウンロードします。
    - ファイルのアップロード先の URL をメモします。
    - これはマニフェスト XML ファイルにとって重要になります。

7. アプリ / 拡張機能の ID、ダウンロード URL、バージョンを使ってマニフェスト XML ファイルを作成するには、以下の 3 つのフィールドを定義します。
    - **appid**（手順 5 でメモした拡張機能 ID）
    - **codebase**（手順 3 の CRX ファイルのダウンロード場所）
    - **version**（アプリ / 拡張機能のバージョン。手順 5 でメモしたバージョンと一致する必要があります）

   XML マニフェスト ファイルの例:

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='abcdefghijklmnopqrstuvwxyz123456
'>
    <updatecheck codebase='https://example.com/chrome/helloworld.crx'
version='1.0' />
  </app>
</gupdate>
```

8. 完成した XML ファイルを、ユーザーやデバイスがアクセスできる場所にアップロードして、URL をメモします。ユーザーやデバイスは、この場所からファイルをダウンロードできます。

拡張機能のホスト

拡張機能の .crx ファイルをホストするサーバーでは、ユーザーがリンクをクリックして拡張機能をインストールできるように、適切な HTTP ヘッダーが使用されていなければなりません。
次のいずれかが該当する場合、Google Chrome によって、ファイルがインストール可能であると見なされます。

- ファイルのコンテンツ タイプが application/x-chrome-extension である
- ファイルのサフィックスが .crx で、以下の両方が当てはまる:
    - ファイルとともに HTTP ヘッダー X-Content-Type-Options: nosniff が提供されていない
    - ファイルとともに以下のいずれかのコンテンツ タイプが提供されている
        - 空の文字列
        - "text/plain"
        - "application/octet-stream"
        - "unknown/unknown"
        - "application/unknown"
        - "*/*"

インストール可能なファイルを認識できない理由として最もよくあるのが、サーバーによる X-Content-Type-Options: nosniff ヘッダーの送信です。2 番目に多い理由は、サーバーによる未知のコンテンツ タイプ、つまり前のリストにないコンテンツ タイプの送信です。HTTP ヘッダーの問題を修正するには、サーバーの設定を変更するか、別のサーバーで .crx ファイルをホストしてみます。

拡張機能へのアップデートの公開

拡張機能に必要な変更を行い、テストしたことを確認します。アップデートを公開する手順は次のとおりです。

1. 拡張機能のマニフェスト JSON ファイル内のバージョン番号を、より大きな値に変更します。
   例:
   `"version": "versionString"`
   If the `"version":"1.0"`, then you can update to `"version":"1.1"` or any number higher than `"1.0"`.
2. XML ファイルの `<updatecheck>` の `"version"` を更新して、前の手順でマニフェスト ファイルに入力した番号と一致させます。
   別の例:
   ```
   <updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx'
   version='1.1' />
   ```

3. 新しい変更点を含む CRX ファイルを再作成します。
    a. Chrome アドレスバーを使用して **chrome://extensions** にアクセスします。
    b. [デベロッパー モード] のチェックボックスをオンにします。

4. [拡張機能のパッケージ化] をクリックし、ソースがあるディレクトリを選択して CRX ファイルを作成します。注: PEM ファイルについては、CRX ファイルが初めて作成されたときに生成、保存されたものと同じファイルを使用してください。
5. CRX を拡張機能ウィンドウにドラッグし、読み込まれることを確認します。
6. 拡張機能をテストします。
7. 古い CRX ファイルと XML ファイルを、新しいファイルに置き換えます。
    a. これは、ユーザーやデバイスによるファイルの以前のダウンロード元と同じホスト場所にある必要があります。

この変更は、次のポリシー同期サイクル中に反映されます。

参照 URL:

- 自動更新
- 更新 URL
- 更新マニフェスト

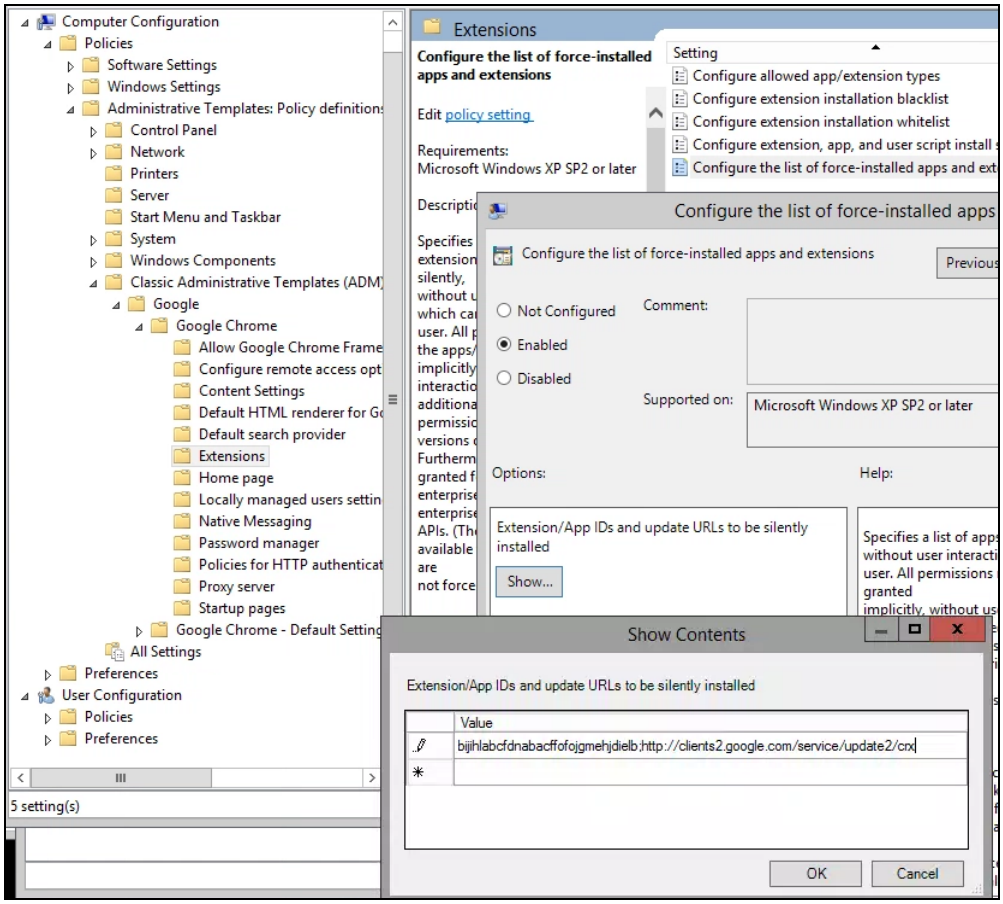
非公開でホストされている拡張機能の配布

グループ ポリシー内: 現在、自己ホスト型拡張機能の配布は、グループ ポリシーによってのみサポートされています。[自動インストールされたアプリと拡張機能のリストを設定する] というポリシーを使用して、ユーザーのデバイスに拡張機能を自動インストールすることができます。

(Chrome ウェブストアにない) 非公開でホストされているアプリについては、次のような文字列を使用します。

```
pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml
```

URL は、内部アプリの `update.xml` に対して指定されます。公開用の `clients2.google.com` URL ではありません。



[自動インストールされたアプリと拡張機能のリストを設定する] GPOポリシー（コンテンツを表示）

その後、ポリシーは、選択したユーザーかパソコン、またはその両方に適用できます。ポリシーが適用されるまでに時間がかかることがありますが、ユーザーのパソコンで「gpupdate」を実行すると早めることができます。

Chrome ブラウザ クラウド管理を使用して拡張機能を管理する

Windows、Mac、Linux パソコンの Chrome ブラウザをまとめて管理し、ご利用の環境における Chrome ブラウザの状態を詳細に把握することができます。Chrome ブラウザ クラウド管理により、Chrome ブラウザの設定を最適な方法で管理できます。このコンソールへのアクセスには追加費用はかかりません。Google 管理コンソールに言及しているこのドキュメントのすべてのセクションに、Chrome のこの機能を使用してアクセスできます。 このコンソールを使用すると、以下に関するインサイトを得ることができます。

- フリート全体にデプロイされている現在の Chromeブラウザのバージョン
- 各ブラウザにインストールされている拡張機能
- 各ブラウザに適用されているポリシー
- Chrome ブラウザ クラウド管理における拡張機能の管理の詳細については、こちらの動画をご確認ください

補足資料

組織内での Chrome ブラウザの管理に役立つリソースをご紹介します。

- Chrome ブラウザ クラウド管理のランディング ページ
- Chrome ブラウザ エンタープライズ バンドル
- Chrome のポリシーリスト
- Chrome Enterprise リリースノート
- Chrome ブラウザ更新管理の戦略
- Chrome Enterprise ヘルプセンター
- Chrome をデフォルトのブラウザに設定する（Windows 10）
- Chrome insider のブログシリーズ
- Manifest V3 への Chrome 拡張機能の移行