chrome enterprise

スタートガイド: Chrome ブラウザ エンタープライズ拡張機能管理

はじめに

Chrome ブラウザでは数千もの拡張機能を利用でき、それらの多くは、時間の節約、ビジネス ワークフローの改善、作業の効率化に効果
を発揮します。拡張機能は、RAM の使用率の最適化、ブラウザの高速化、文法の訂正など、仕事の生産性を向上させるために作られてい
ます。ただし、適切に管理されなければ、企業環境にリスクや脆弱性をもたらす可能性がある点に注意することも重要です。そのため、
企業の IT チームでは、ユーザーの生産性のニー
ズと、企業のセキュリティのニーズのバランスを取る必要があります。

拡張機能を管理するうえで、企業の IT チームは次の 3 点を優先的に行います。

1. ユーザーデータと企業データを保護する
2. 不正な拡張機能のインストールを防止する
3. 生産性と効率性を向上させるために必要な拡張機能にユーザーがアクセスできるようにする

新しいものも既存のものも含めて、多くの拡張機能には絶えず更新が行われています。そのため、管理者はベスト プラクティスに従ってユーザーの Chrome 拡張機能をモニタリング、管理、保護することが重要です。

この技術資料では、ニーズに合った方法を選択できるように、拡張機能のさまざまな管理オプションについて説明しています。

考慮すべき基準

拡張機能の管理を開始する前に、まず拡張機能を評価、承認するために組織で考慮すべき要素を 特定する必要があります。これには、次の質問が役に立ちます。

- 組織で遵守する必要があるセキュリティ関連の規制やコンプライアンスにはどのようなものがありますか？
- ユーザーのデバイスには、どのようなユーザーデータと企業データが保存されていますか？
- 拡張機能がリクエストする権限で、データ セキュリティ ポリシーに違反する可能性がある権限は何ですか？

回答が明確になったら、拡張機能の管理オプションの検討に進みましょう。

従来のアプローチ:

長い間、ブラウザの拡張機能を管理する唯一の方法は、拡張機能をひとつずつ手動で評価し、許可リストとブロックリストを作成して、ユーザーのデバイスにインストールできる拡張機能とインストールできない拡張機能を指定するやり方でした。企業によっては現在でもこのアプローチを採用しています。

Google 管理コンソールでは、管理者は拡張機能を次のように管理できます。

- ブロックするものを除くすべての拡張機能を許可する
- 許可するものを除くすべての拡張機能をブロックする
- 拡張機能を個別にブロックまたは許可する
- 1 つ以上の拡張機能を自動インストールする

Microsoft[1] のグループ ポリシーでは、テンプレートを使用することで、同様の保護を特定のグループや組織全体に適用できます。たとえば、次のようなことが可能です。

- ブロックするものを除くすべての拡張機能を許可する
- 単一の拡張機能をブロックまたは許可する
- 拡張機能を自動インストールする

ある程度まではこれらのアプローチで対応することもできますが、限界があります。また、手動の対応であるため、多くの労力も必要になります。

人間による確認が必要になると、ユーザーと管理者の生産性の低下につながる可能性があります。また、セキュリティの観点から最も留意すべき点は、すでに許可リストに含まれている拡張機能が審査されていない組織に売られたり、そのような組織によって更新されたりする可能性があるということです。

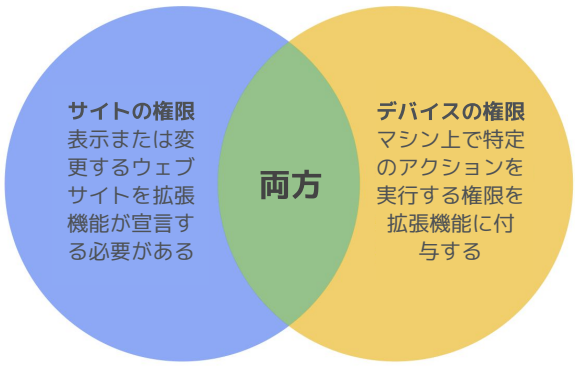
[1] Microsoft®、Windows®、Internet Explorer® は、米国およびその他の国における Microsoft Corporation の登録商標です。

最新のアプローチ: 権限による 拡張機能の管理

効率性、拡張性、安全性に優れた方法で企業向け拡張機能を管理するために、Chrome では権限別に拡張機能を管理することもできます。権限別に拡張機能を管理すると、IT チームは企業データを危険にさらすことなく、必要な拡張機能をユーザーに提供できます。この方法は Google の IT チームが採用しているもので、他の企業にも推奨されます。

権限が与えられた拡張機能は、ウェブサイトやデバイスに変更を加えられるようになります。拡張機能が適切に動作するためには、特定の権限が必要になることが多々あります。

拡張機能の権限には、主に「サイトの権限」と「デバイスの権限」の 2 つのカテゴリがあります。多くの拡張機能では、これらを両方使用します。



サイトの権限の例には、拡張機能による画像のブロックを許可する、拡張機能によるサイトの拡大/縮小の制御を許可する、といったものがあります。デバイスの権限の例には、USB ポートへのアクセス、画面の表示、プログラムの操作などがあります。

リスクをさらに軽減するには、次のポリシーを使用して拡張機能を管理することを検討します。

- **権限のブロックまたは許可:** すでに許可リストに含まれている拡張機能が新しい権限で更新されることを防止したり、インストール後に要件を満たさなくなった拡張機能を無効にしたりできます。
- **実行時のホストのブロック:**拡張機能を実行できるサイトを指定できます。
- **拡張機能の自動インストール:**生産性向上に必要なツールを使用できるように、ユーザーのマシンに拡張機能を一律にインストールできます。
- **許可リスト / ブロックリスト:** 必要に応じて使用します。

この Chrome 拡張機能の管理方法は、安全性と管理性に優れており、大規模な組織向けにスケーリングすることもできます。また、不正な拡張機能からユーザーを保護できるうえ、過度に長い許可リストとブロックリストの管理、更新の確認、拡張機能ごとの個別の検証などが不要になるため、IT 担当者の時間を節約できます。このように、ユーザーと管理者の双方にメリットがあります。

使用方法: 権限別に拡張機能を管理する

企業向け拡張機能を権限別に管理するには、次の手順を踏みます。

1. ユーザーがすでにインストールしている拡張機能のリストを作成する（Chrome ブラウザ クラウド管理のレポート機能を使用するか、エンドユーザーに対してアンケートを実施する）
2. 保護が必要なウェブサイトやホストを特定し、潜在的なリスクがあるために制限が必要な権限を判断する
3. 収集した全データのマスターリストを作成し、同意を得る必要がある重要な関係者と共有する
4. テスト環境で新しいポリシーをテストする、または小規模の試験運用グループを編成して新しいポリシーセットを段階的に従業員にリリースする
5. ユーザーからのフィードバックを確認する
6. プロセスを繰り返し実施して調整する（毎月、毎四半期、毎年など、組織に適した期間で実施する）

1 度ポリシーを設定するだけで、許可された権限のベースラインが設定されるため、機密情報を含む企業サイトを保護できます。企業の安全性が自動的に強化されるだけでなく、ユーザー環境も向上します。

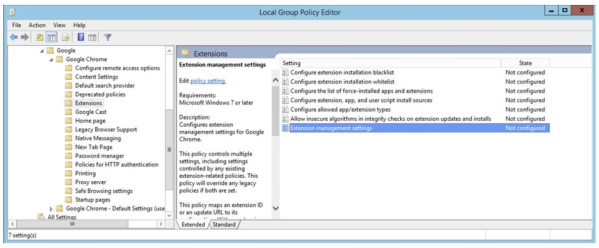
機密情報を含む企業サイトでは実行できないものの、以前は許可されなかった拡張機能を従業員がインストールできる場合もあります。

権限の設定

許可する権限と許可しない権限を指定するだけで、ユーザーがインストールできる拡張機能を簡単に制御できます。

Google 管理コンソール

Windows、Chrome OS、Mac[2]、Linux 環境では、Google 管理コンソールを使用してこれらを制御できます。セキュリティ ポリシーに違反するアクセス権や権限を必要とする拡張機能はインストールされません。たとえば、ユーザーの USB デバイスにアクセスする拡張機能や、Cookie の読み取りを妨げる拡張機能をブロックできます。インストール済みであっても、ブロックされている権限を必要とする拡張機能は、実行されません。拡張機能は削除されるのではなく、無効になります。



グループ ポリシー

Windows で拡張機能を管理する場合、拡張機能設定ポリシーを使用する方法も一般的です。グループ ポリシー管理エディタでは、JSON 文字列または Windows レジストリを使用して、複数のポリシーを 1 か所で設定できます。拡張機能設定ポリシーでは、インストール モード、

[2] Mac および macOS は、米国およびその他の国における Apple Inc. の登録商標です。

更新 URL、ブロックする権限、インストール元、許可するタイプ、ブロックするインストール、
ランタイムがブロックおよび許可するホストなどを制御できます。拡張機能の管理設定をすべてここで行うことも、他の個別のポリシーでこれらを制御することもできます。ここでの設定には、Windows グループ ポリシー エディタで Windows レジストリまたは JSON 文字列が使用されます。

その他の考慮事項

企業によっては、拡張機能をダウンロードするための独自のサイトを用意する場合があります。Google では、この方法はおすすめしていません。Chrome ウェブストアよりも安全性が低くなる可
能性があるためです。Chrome ウェブストアでは、自動および手動のコードスキャンを利用できる
ため、悪意のあるコードがユーザーに送信されることを防止できます。

Chrome ブラウザ クラウド管理は新しいコンソールであり、Windows、Mac、Linux マシンの Chrome ブラウザの設定をすべて 1 か所で管理できます。このコンソールでは環境内の Chrome ブラウザの状態を詳しく把握できます。たとえば、次のような情報を簡単に確認できます。

- 企業が所有するすべてのデスクトップ パソコンやノートパソコンにデプロイされている Chrome Browser の現在のバージョン（デスクトップ パソコンやノートパソコンの種類を問わない）
- 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

また、コンソールからボタンをクリックするだけで、すべてのマシンに対して不審な拡張機能をブロックすることもできます。

Google のやり方と同じ Chrome 拡張機能の管理

Google では、30 万台以上のエンドポイントに対して、許可リストとブロックリストを使用した従来型の拡張機能管理を数年間実施してきました。その結果、Google の IT チームは、企業の IT およびセキュリティのニーズと従業員の生産性とのバランスが取れた、より手間のかからない方法が必要だと考えました。権限別に拡張機能を管理するという Google IT チームのソリューションは、スケーラブルかつ安全で、オーバーヘッドを大幅に削減できます。

他の企業でも、Google のように許可リストとブロックリストを使用する方法から、この技術資料で説明されている、より安全な方法に切り替えることができます。企業に求められるセキュリティを確保しながら、安全かつ生産性向上につながる拡張機能のインストールをユーザーに許可できます。

権限別の拡張機能管理を今すぐ開始しましょう。

Chrome ブラウザ拡張機能の管理についてより深く理解するために、**次のリソースもご確認ください。**

社内での拡張機能の管理ガイドを読む
Google Cloud Next '19 のブレイクアウト セッション: Google Cloud の技術で企業向け拡張機能を管理する仕組みを視聴する
Chrome ブラウザ クラウド管理のオプションを確認する
企業向けの Chrome ブラウザのダウンロードを確認する
Chrome ブラウザ エンタープライズ サポートの詳細を確認する
Chrome ブラウザのポリシーリストを確認する
Chrome ブラウザ エンタープライズのヘルプ センターと Chrome ブラウザのヘルプ フォーラムを参照する