



Windows 環境における Chrome ブラウザの更新方法

更新日: 2021 年 9 月

はじめに

企業で働く多くの人は、さまざまなデバイスでクラウドベースやブラウザベースのビジネスアプリを使用して日常業務を行っています。どこにいてもブラウザから会社のリソースにアクセスできるので、「仕事の効率が飛躍的に高まった」と言うクラウド利用者もいます¹。

ブラウザがミッションクリティカルなエンタープライズアプリケーションとなる一方、Windows 環境を管理する IT 担当者にとってブラウザの管理に

はいくつかの課題があります。

具体的には次のようなものです。

- 多くの企業は使用するブラウザを統一していない。
- ブラウザを最新の状態に維持してセキュリティを最適化することが難しい。

1. 「Rethink Technology In The Age Of The Cloud Worker」、Google の委託により Forrester Consulting が発行したソートリーダーシップに関する論文（2018 年 5 月）



- ブラウザによってアプリとの互換性が異なる場合がある（特に従来のブラウザと最新のブラウザ）。

Chrome ブラウザのブラウジング環境を使い慣れているユーザーが多いため、企業でも Chrome ブラウザはよく使用されています。また、企業にも対応した最新のブラウザである Chrome には自動更新モデルが採用されているため、企業の環境全体を迅速かつ安全に更新できます。

IT チームが直面している課題（特に Windows 環境の複雑性）を考慮して、Chrome には Microsoft™ Windows™ パソコン上のブラウザを管理するためのさまざまな方法があり、管理者はユーザーごとに異なる更新チャンネルを使用できます。このテクニカルペーパーでは、さまざまな更新方法について説明するとともに、企業が Chrome の管理方法を検討する際に役立つ推奨事項も記載しています。

Chrome ブラウザの更新チャンネル

chrome		Stable の 4 週間前	Stable の 8 週間前	Stable の 8 週間以上前
Extended Stable	Stable	Beta	Dev	Canary
<ul style="list-style-type: none"> • 約 2 週間ごとにマイナー リリース、8 週間ごとにメジャー リリース • Chrome テストチームによる十分なテストと承認 • 新機能をテストする時間を十分に確保可能 	<ul style="list-style-type: none"> • 約 2 週間ごとにマイナー リリース、4 週間ごとにメジャー リリース • Chrome テストチームによる十分なテストと承認 • 最も安全なチャンネル 	<ul style="list-style-type: none"> • ほぼ毎週更新 • 4 週間ごとにメジャー アップデート 	<ul style="list-style-type: none"> • 週に 1、2 回更新 • 開発中のバージョン • メジャー バージョン間の遅れがない • テスト済みだがバグを含む可能性がある 	<ul style="list-style-type: none"> • テスト段階のビルド • ビルド後すぐにリリース（毎日） • 未テスト、未使用の状態 • 不安定な可能性がある

10 年以上の間、Chrome は 6 週間ごとに新しいバージョンをリリースし、セキュリティ、安定性、スピード、シンプルさ備えたブラウザをユーザーとウェブに提供してきました。時間の経過とともにテストとリリースのプロセスが改善され、パッチのギャップも改善されました。現在では、リリース サイクルを短くして、新しい機能をより迅速に提供できるようになりました。Chrome は M94 以降、Stable チャンネルで 4 週間ごと、Extended Stable チャンネルで 8 週間ごとに新しいバージョンをリリースするようになりました。また、



Chromeには3種類（Beta、Dev、Canary）の早期アクセス更新チャンネルもあります。Stableチャンネルの環境は、[TargetChannel](#) ポリシーを使用して Stable、Extended Stable、Beta、Dev の各チャンネルに切り替えることができます、さらに、Beta、Dev、Canary の各チャンネルは、Stable チャンネルと一緒にインストールして同時に実行できます。

Stable チャンネル

Stable チャンネルは、Chrome テストチームによって十分にテストされているため、最も安全なバージョンです。脆弱性に対する重要な修正が含まれており、クラッシュなどの問題を回避するには最適です。マイナー アップデートは約 2 週間ごと、メジャー アップデートは 4 週間ごとに行われます。

推奨事項:

Beta チャンネルと Dev チャンネル（詳細は後述）を適用するユーザーを除き、組織内の全員に Stable チャンネルを適用し、ブラウザを使用するミッションクリティカルなすべてのアクティビティで Stable リリースを利用するようにします。Stable リリースでバグを見つけた場合は、crbug.com でご報告ください。

Extended Stable チャンネル

Stable チャンネルと同様に、Extended Stable チャンネルは十分にテストされており、脆弱性やその他の問題に対する重大な修正が含まれています。ただし、Extended Stable ではメジャーバージョンを 1 つおきに受信する（たとえば、Stable では 94、95、96 と更新されますが、Extended Stable では 94 から 96 に更新されます）ため、Stable チャンネルで利用できる一部のセキュリティ修正や新機能を、Extended Stable チャンネル

ではすぐに利用できない可能性があります。

メジャー アップデートは 8 週間ごと、マイナー アップデートは 2 週間ごとに行われます。

推奨事項:

各リリース間の期間を長く確保する必要がある一部の組織では、Extended Stable チャンネルを使用します。バージョン更新のサイクルが長くなることで、管理者はユーザーの Chrome を一定期間同じバージョンに維持できるため、場合によっては特定のバージョンに固定する必要がなくなります。更新の設定は簡単で、ポリシーを一度設定するだけで済みます。

Beta チャンネル

Beta チャンネルでは、リスクを最小限に抑えながら、Stable チャンネルで次回リリースされる内容を確認できます。Google は、Chrome リリースのバグトラッカー (crbug.com) で報告された Beta チャンネルに関する問題を積極的に調査しています。Beta チャンネルではマイナー アップデートが約1週間ごと、メジャー アップデートが4週間ごとに行われ、Stable チャンネルに先行して新しい機能がリリースされます。

すべての機能が全ユーザーに適しているわけではありません。Beta チャンネルを使用することで、組織全体に計画的に展開できるほか、ポリシーを使用して特定の機能を制御する方法を検討できます。テストデバイスで問題が見つければ、問題を報告するための期間を確保できます。次回の Stable リリースまでに Google で問題が解決されない場合は、すべてのユーザーに展開する前にその更新をブロックできます。

推奨事項:

組織全体の約 5% のユーザー (IT スタッフ、デベロッパー スタッフ、ビジネス ユーザーなど) を Beta チャンネルに割り当てます。また、複数の種類のハードウェアを使用している場合は、各ハードウェアのユーザーの約 5% に Beta チャンネルに割り当てることをおすすめします。これにより、

複数グループのユーザーと複数種類のハードウェアでテストする期間を 4 週間確保できます。

Beta チャンネルを適用する方法は 2 つあります。1 つは、Beta と Stable を両方インストールし、ユーザーが自分の判断でどちらを実行するか選択できるようにする方法です。Beta で問題が見つかったら、問題を報告して Stable に切り替えることができます。もう 1 つは、TargetChannel ポリシーを使用してブラウザを Beta に設定する方法です。ユーザーが問題を見つけた場合はユーザー自身で報告できますが、重大な問題が見つかった場合は、管理者が TargetChannel ポリシー設定を変更して Stable に切り替える必要があります。

Dev チャンネル

Dev チャンネルを使用することで、今後リリースされる更新と機能を把握できます。Dev チャンネルでリリースされたバージョンは、8 週間後に Stable チャンネルでリリースされます。Chrome の早期リリースであるため、Beta や Stable のようには安定していません。IT スタッフやデベロッパー スタッフはこのチャンネルを使って、組織で利用しているアプリとシステムが今後の更新と機能変更に対応しているかどうかを確認できます。更新は週に 1 回または 2 回行われます。メジャーバージョン間の遅れがないので、Google が保有するすべてのコードを入手できます。Dev チャンネルのビルドはテスト済みですが、バグを見つけた場合



は Chrome リリースのバグリスト (crbug.com) にご報告ください。

推奨事項:

少数の IT スタッフと一部のデベロッパーを Dev チャンネルに割り当てることをおすすめします。Dev チャンネルのユーザーは、Beta、Stable、Extended Stable チャンネルのユーザーに新しいバージョンが展開される前に、環境に影響を及ぼす可能性がある変更を発見して報告できます。ほとんどの問題は Stable チャンネルでリリースされる前に Google 側で修正されますが、特定の環境のみに影響を及ぼすような特殊なケースについては把握できないこともあるため、一部の IT スタッフとデベロッパー スタッフを Dev チャンネルに割り当てておけば、Beta または Stable チャンネルでリリースされる前に、環境に影響を及ぼす可能性がある変更をすばやく特定して報告できます。Dev チャンネルは安定していない可能性があるため、TargetChannel を使用して Chrome インスタンスを Dev チャンネルのみに指定するのではなく、Stable チャンネルと並行して使用できるようにすることをおすすめします。

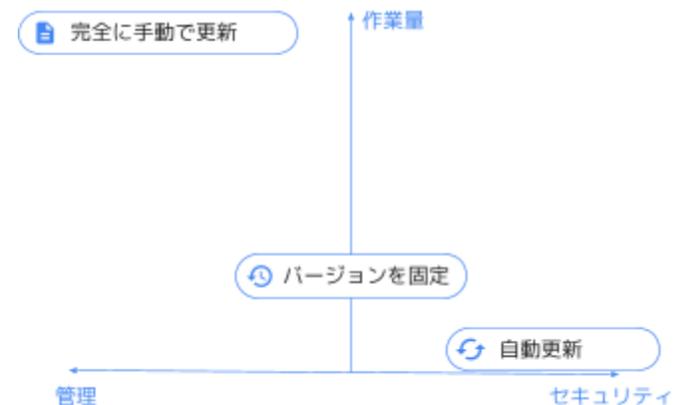
Canary チャンネル

Canary チャンネルのビルドは、未テスト、未使用のまま毎日リリースされます。Canary チャンネルでリリースされたバージョンは、8 週間以上経過してから Stable チャンネルでリリースされます。バグは Chrome リリースのバグリスト (crbug.com) にご報告ください。

推奨事項:

Canary チャンネルは他よりも安定性が低いため、業務上高度なテストが必要な場合を除き、スタッフに Canary チャンネルを割り当てる必要はありません。

Chrome の更新方法



自動更新

既知の脆弱性が迅速に保護されます。ユーザーが Chrome を再起動するだけで更新が適用されます。自動更新を選択したユーザー全員に同じバージョ



ンの Chrome が適用された状態になるため、IT スタッフが手動で問題を修正する必要はありません。

推奨事項:

SaaS ウェブサイトを頻繁に使用するユーザーには、自動更新が適しています。IT 環境、運用ニーズ、セキュリティ ニーズを評価し、自動更新が適しているグループと適さないグループにユーザーを分けます。自動更新が適さないグループについては、バージョンの固定を検討します。その後、できるだけ多くのユーザーとデバイスを計画的に自動更新に切り替えます。

バージョンの固定

ユーザーが更新を受信するタイミングを制御したり、ソフトウェア配布の要件を満たしたりできるほか、組織の定期的な更新プロセスに合わせるすることができます。更新プロセスは IT 部門が管理し、ユーザーが自分で更新を適用することはできません。組織では、アプリケーションの互換性、テスト要件、チェンジ マネジメント、セキュリティ 審査、または規制要件に対応するために、Chrome を特定のバージョンに固定しなければならないことがあります。この場合は、できるだけ早くテスト担当スタッフを Beta チャンネルと

Dev チャンネルに割り当てることが大切です。早期にテストを実施することで、Chrome の最新バージョンに備えることができます。

推奨事項:

審査およびテストが完了した Chrome の最新のメジャーバージョンに固定し、[Chrome Enterprise リリースノート](#)を定期的にご確認ください。ユーザーは、セキュリティ修正を含むマイナー アップデートを引き続き受信します。新しいバージョンがリリースされたら、リリースノートで必要なテスト事項を確認し、テストを開始してください。準備が整ったら、テスト済みの最新のバージョンに固定しなおすか、設定を完全に削除してユーザーが最新バージョンの Chrome に更新できるようにします。

完全に手動で更新

組織によっては、厳格なロックダウン環境（インターネットに接続せずに、社内のウェブアプリにのみブラウザを使用）で Chrome を使用している場合があります。このような環境では、Google アップデートを使用するのではなく、毎回新しい MSI を手動でプッシュして Chrome を最新の状態に維持する必要があります。

推奨事項:

組織のコンプライアンスにとって重要でない限り、ブラウザを手動で更新することはお勧めしません。自動で更新しない場合、ブラウザに重要な修正が適用されないことがあるため、脆弱性の影響を受けて環境を危険にさらす可能性があります。適切なタイミングで更新を適用する作業は、必要に迫られてロールバックする作業と同様にとても手間がかかります。また、古いバージョンの Chrome で問題が発生しても、Chrome ブラウザ エンタープライズ サポートの対象とならない可能性があります。

Chrome 更新のハイブリッドアプローチ

組織によっては、Chrome 更新のハイブリッドアプローチが適している場合があります。ハイブリッドアプローチとは、自動更新、定期的な手動更新、更新の無効化（特定のバージョンを長期間使用）をユーザーに応じて使い分ける方法です。

このアプローチでは、ビジネスニーズに応じて複数の方法を組み合わせて Chrome を更新できるほか、自動更新によるセキュリティと効率性のメリットもあります。たとえば、さまざまな事業部門にほぼ対応するように複数の組織部門を設定し、一部の組織部門には自動更新モデルを適

用し、他の組織部門にはバージョン固定モデルを適用します。

ハイブリッドアプローチを採用する場合は、一般的に事業部門単位でのアプローチが必要になり、事業部門ごとに異なるアプリケーション ニーズや要件をしっかりと把握する必要があります。

Chrome のポリシー テンプレートの機能

Chrome ブラウザ エンタープライズ バンドルに含まれているファイルを使用すると、管理対象の Windows デバイスに Chrome ブラウザをインストールして管理できます。Chrome をユーザーのデバイスにインストールしたら、好みのオンプレミス ツール（Windows グループ ポリシーなど）または Google 管理コンソールを使用して、デバイスにポリシーを適用できます。

次のことが可能です。

- デバイスレベルでポリシーを設定する（ユーザー個人には適用しない）
- OS ユーザーレベルでポリシーを設定する（指定したユーザーがデバイスにログインするとポリシーが適用される）

- ポリシーを適用する（ユーザーはポリシーを変更できない）
- デフォルトの設定を適用する（ユーザーは設定を変更できる）

Google はポリシーの設定に役立つポリシー テンプレート（ADMX および ADM）を提供しており、管理者はこのテンプレートをインストールして更新できます。テンプレートは、新しいバージョンに合わせて新しいポリシーで更新されますが、場合によっては、ポリシーのサポートが終了することもあります。自動更新を適用している場合でも、最新のポリシーを使用するには、新しいポリシー テンプレートをダウンロードする必要があります。

推奨事項:

新しいポリシーと変更予定のポリシーについては、Chrome Enterprise リリースノートをご覧ください。Dev チャンネルと Beta チャンネルのポリシー テンプレートをダウンロードして、事前に変更を確認することもできます。

Chrome ブラウザの更新に関するその他の考慮事項

企業は、Chrome の次のような機能の更新についても把握しておく必要があります。

- サードパーティ拡張機能の管理
- 従来のブラウザのサポート

サードパーティ拡張機能の更新の管理

IT チームはオンプレミスのポリシーとクラウド管理の両方を使用して、拡張機能の利用と管理を制御できます。拡張機能の更新プロセスは、Chrome の更新とは異なります。管理者は自動更新、手動更新、更新の無効化、またはハイブリッドアプローチを使用して拡張機能を管理できます。詳細については、[社内での拡張機能の管理](#)をご覧ください。

従来のブラウザのサポート

組織で Chrome を利用したいと考えていても、ユーザーが従来のウェブサイトやアプリにアクセスするために引き続き Microsoft Internet Explorer が必要になることがあります。このような場合は、Chrome の「従来のブラウザのサポート」を使用して、Chrome ブラウザと別のブラウザを自動的に切り替えることができます。従来のブラウザを必要とするリンク（ActiveX を必要とするサイトなど）をクリックすると、その URL は自動的に従来のブラ



ブラウザで開きます。その後、他のサイトにアクセスすると、Chrome ブラウザにシームレスに戻ります。

「従来のブラウザのサポート」はエンタープライズバンドルに含まれており、Chrome ブラウザク

ラウド管理またはグループポリシーを使用して有効にできます。

次のステップとリソース

Google は、企業が複雑なポリシーと要件に沿ってソフトウェアの更新を管理していることを理解しています。企業は、ソフトウェアの機能と互換性、セキュリティアップデート、社内でのアプリケーションテストとポリシー管理、従業員のトレーニングなど、多くの重要な要素を考慮しなければなりません。このテクニカルペーパーに記載されている更新チャンネル（Stable、Beta、Dev、Canary）とその他の更新方法を利用することで、セキュリティと運用効率を維持しながら Chrome の更新方法を独自に策定できます。

Chrome の更新方法を策定する際は、次の点に留意してください。

- 組織で新規更新に使用できる帯域幅と許容誤差を判断します。
- セキュリティと更新タイミングとのトレードオフを判断します。
- Chrome のリリースノートとドキュメントを早めに確認します。
- Chrome の更新チャンネルを十分に理解して、テストの機会を最大限に活用します。
- IT スタッフ、デベロッパー スタッフ、ビジネスユーザーの 5% を Beta チャンネルでのテストに割り当て、Stable チャンネルで変更がリリースされる前に問題を見つけて報告できるようにします。
- 必要に応じてユーザーを複数の組織部門に分けて、一部のユーザーには自動更新を適用し、残りのユーザーにはバージョンを固定します。
- いずれかのチャンネルでバグが見つかった場合は、crbug.com でご報告ください。



報告された問題は Chrome チームが積極的に調査します。

Chrome ブラウザ エンタープライズ サポートを購入して、組織内のユーザーに対する Chrome の設定、導入、管理に関するサポートを受けることもできます。Stable、Beta、Dev チャンネルでは、エキスパートによる 24 時間 365 日体制のサポートを利用できます。手動で更新を管理する組織も、いつでもエキスパートに問い合わせることで問題を迅速に解決できるため、独自の方法で予定どおりに更新を展開できます。

[Chrome ブラウザ ヘルプフォーラム](#)

バグの報告:

[Chrome ブラウザの公開バグトラッカー](#)

企業向けの Chrome の機能について理解を深めるために、**必要に応じて次のリソースもご活用ください。**

エンタープライズ版のダウンロード:

[Chrome ブラウザ](#)

サポートの詳細:

[Chrome ブラウザ エンタープライズ サポート](#)
[ブラウザのスペシャリストに問い合わせる](#)

ポリシーの詳細:

[Chrome ブラウザのポリシーリスト](#)

リリースノート:

[Chrome ブラウザ エンタープライズのリリースノート](#)

ヘルプ:

[Chrome ブラウザ エンタープライズ](#)
[ヘルプセンター](#)