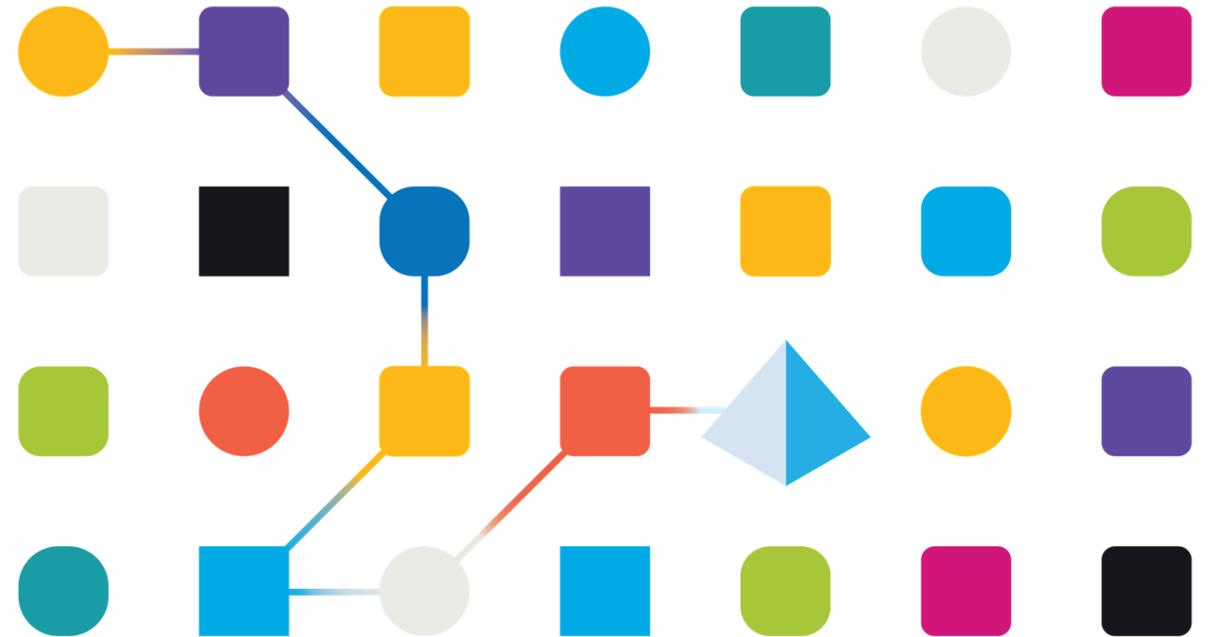


Chrome/Edge ブラウザ拡張機能 MV3 移行解説

Blue Prism Japan
Professional Services

清水 知陽 (Tomoaki Shimizu)

16-Nov-2022



免責

この資料に記載されている情報は、この資料の発表時点におけるBlue Prism 株式会社の見解を反映したものです。Blue Prism 株式会社は市場の変化に対応する必要があるため、この資料の内容に関する責任をBlue Prism 株式会社は問われないものとしします。また、発表日以降は記載されている情報の正確性を保証できません。この資料は情報提供のみを目的としています。

明示、黙示、または法令に基づく規定にかかわらず、これらの情報についてBlue Prism 株式会社はいかなる責任も負わないものとしします。

Blue Prism 株式会社は、この資料に記載されている事項に関して、特許、申請中特許、商標、著作権、および他の知的財産権を所有する場合があります。別途Blue Prism 株式会社のライセンス契約上に明示の規定のない限り、この情報はこれらの特許、商標、著作権、またはその他の知的財産権に関する権利をお客様に許諾するものではありません。

2022年11月16日

アジェンダ

1. 本セッションについて

2. 背景と概要

- ブラウザー拡張機能・マニフェストとは？
- MV3対応が必要な理由
- MV2の廃止スケジュール
- MV3 対応期限
- SS&C Blue Prism Enterpriseの脆弱性について
- MV3・脆弱性対応の進め方 概要
- パッチ適用・MV3拡張機能対応後の動作確認について

3. 修正・対策内容

- MV2使用期限の延長
- 脆弱性対策方針の検討
- 脆弱性対応パッチ
- MV3移行に伴う仕様変更
- Browser Automation Agent (BAA)
- MV3拡張機能 バージョン別対応方法一覧
- パッチ適用・MV3拡張機能対応後の動作確認について

4. 対応ステップと作業内容

- MV3・脆弱性対応 対応ステップ
- Enterprise Policy設定の確認
- Enterprise Policyの設定
- Blue Prismのアップグレード作業（パッチ適用）
- Webブラウザ推奨設定
- BAAのインストール手順
- MV3拡張機能 + BAA環境におけるJavaScript 機能の利用
- BAAを導入しない場合のMV3ブラウザ拡張インストール
- 拡張機能のオフラインインストール

5. Appendix

- MV3対応 - 関連資料／ツール
- SS&C Blue Prism Enterprise 脆弱性一覧
- SS&C Blue Prism のセキュリティリスク軽減対策
- SS&C Blue Prism Enterprise の不具合

1. 本セッションについて

- 本セッションの内容は2022年11月16日時点の情報に基づいています。今後、Google社、Microsoft社の方針変更やスケジュール変更、それに伴うBlue Prismの仕様、サポート、対応方法に関する変更が生じる可能性があります。
- 本セッションはGoogle Chrome と Microsoft Edge のブラウザ拡張機能の仕様変更に伴い、SS&C Blue Prism Enterprise のブラウザ拡張機能のアップグレードについて必要なアクションをお知らせすることを目的としています。
- ブラウザー拡張機能のMV3対応の際に、Blue Prismの既知の脆弱性への対策の検討も含んだ内容となっています。
- 本セッションの資料スライドは対応を検討する際に活用していただくために、後からダウンロードしていただけます。そのため、細かい設定値や手順等については割愛して説明をさせていただきます。
- お客様環境固有の問題が発生する可能性があるため、本セッション/資料で紹介した設定や作業を実施する場合、必ず開発/検証環境で作業と確認を行ってから本番環境に適用してください。
- 機能追加等を目的としたメジャー/マイナーバージョンアップグレード作業については、本セッションでは説明範囲外となっています。バージョンの機能差分等について、SS&C Blue Prism Enterprise のリリースノート等の情報を参照の上、個別に計画を行ってください。

【参考リンク】 [Blue Prism 7.X.Xリリースノート](#)
[Blue Prism 6.X.Xリリースノート](#)
[Blue Prismのアップグレード](#)



2. 背景と概要

ブラウザ拡張機能・マニフェストとは？

ブラウザ拡張機能とは？

ブラウザ拡張機能は、Webブラウザに特定の機能を追加するためのプログラムの総称です。アドオン、プラグイン、エクステンションなどと呼ばれることもあります。様々なベンダーから自社ソリューションの機能をブラウザに追加する目的やブラウザ自体の機能を追加するための拡張機能がリリースされています。Blue Prismのブラウザ拡張機能はBlue PrismのオブジェクトがWebブラウザ（Chrome/Edge/Firefox）と通信して、HTML要素のスパイや操作を行うための機能をブラウザに提供しています。

マニフェストとは？

ブラウザ拡張機能に関するブラウザ側のAPI仕様の定義です。マニフェストによりブラウザ側で拡張可能な機能/アクションやセキュリティ等のAPIの仕様が定められています。

マニフェストバージョンについて

マニフェストのバージョンを表し、このバージョンが上がるとブラウザ側のAPIの仕様がアップデートされ、利用可能な機能やセキュリティ等もアップデートされることとなります。これまで世の中でリリースされた多くの拡張機能はバージョン2（Manifest V2）の仕様に基づいて開発、提供されてきました。最新のバージョン3（Manifest V3）は2021年にChromeバージョン88でリリースされましたが、Manifest V2も引き続き利用が可能なことから、それ以降も多くの拡張機能がManifest V2の仕様で動作しており、現在各ベンダーがManifest V3への対応を行っています。

MV3対応が必要な理由

ChromeとEdgeの「Manifest V2」(以降、MV2) 拡張機能の実行を2023年1月から段階的に廃止することをGoogle社、Microsoft社が発表しました。

- Google社から「Google Chrome」のこれまでの拡張機能のマニフェストバージョンであるMV2の廃止と移行スケジュールが発表
- Chromeのエンジンを使用する「Microsoft Edge (Chromium版)」についてもMV2の廃止・移行スケジュールがMicrosoft社より発表



このブラウザ側の仕様変更は現在まで世の中で多く利用されてきたMV2ブラウザ拡張機能が動作しなくなることを意味します。

Blue PrismにおいてもChrome/Edgeの自動化向けに提供している従来のMV2版の「ブラウザ拡張機能」が動作しなくなり、ブラウザモードでスパイされているアプリケーションの操作ができなくなります。



MV2廃止までにChromeとEdgeについて、新バージョンとなる「Manifest V3」(以降、MV3) 版の「ブラウザ拡張機能」への移行が必須となります。

※FirefoxはMV2 廃止予定が発表されていないため、従来のMV2プラグインがそのまま動作

MV2の廃止スケジュール

※2022年11月15日時点のスケジュール
スケジュールは今後Google、Microsoftにより変更される場合があります

【参照URL】 <https://developer.chrome.com/docs/extensions/mv3/mv2-sunset/>



※¹: 安全で使いやすく、信頼できると判断した
拡張機能を示す認証バッジ

2023年1月以降

- バージョン112以降の**開発版 (Canary, Dev, Beta)**でMV2廃止機能のテストが開始
- 拡張機能のFeatured Badge※¹がMV3でのみ取得可能となる

ChromeのEnterprise Policyにより
MV2拡張機能の実行延長が可能

2023年6月以降

- バージョン115以降の全てのChromeでMV2廃止のテストが開始
(Enterprise Policyが適用されていないMV2の実行が停止)

2024年1月以降

- 全てのMV2拡張機能がWebストアから削除されEnterprise Policy適用環境を含む環境で実行不可となる。

2022年

2023年

2024年



※ Edgeに関してはこれまでに何度かスケジュール変更が発表されたため、現在個別のスケジュールが更新中になっていますが、現時点ではChromium側スケジュールを参照となっています。

2023年6月以降

- Enterprise Policyが適用されていないMV2の実行が停止

EdgeのEnterprise Policyにより
MV2拡張機能の実行延長が可能

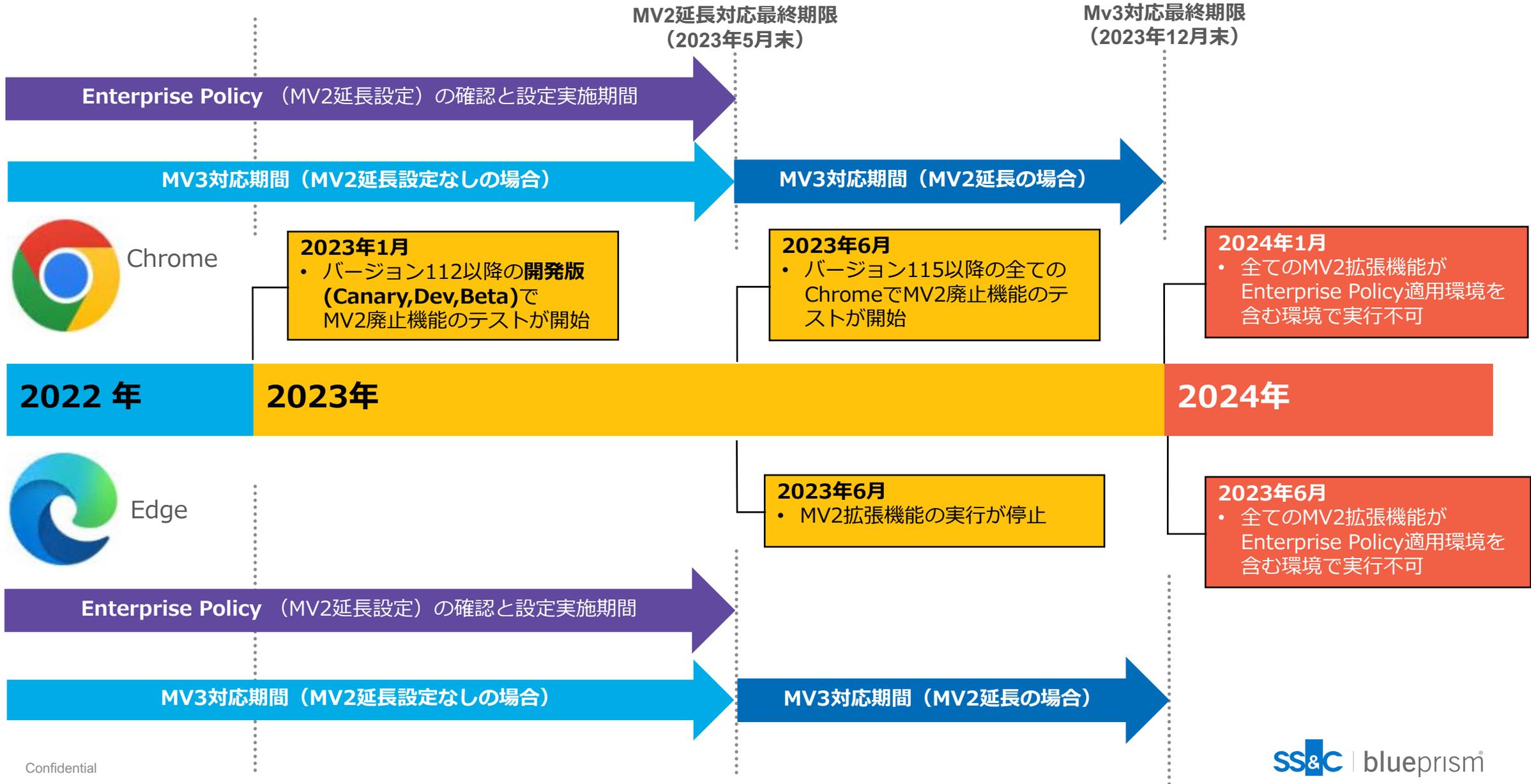
2024年1月以降

- 全てのMV2拡張機能がEnterprise Policy適用環境を含む環境で実行不可となる。

【参照URL】 <https://learn.microsoft.com/ja-jp/microsoft-edge/extensions-chromium/developer-guide/manifest-v3>

MV3対応期限

※2022年11月7日時点の想定スケジュールは今後Google社、Microsoft社により変更される場合があります



SS&C Blue Prism Enterpriseの脆弱性について

MV3対応を行う際に、あわせてBlue Prismの脆弱性対応の対策に関する検討を行ってください。

■ 脆弱性概要

これまでのバージョンのBlue Prism Enterpriseにおいて、複数の複雑な前提条件が必要で悪用が成功する可能性は低いものの、深刻度は高いとされる脆弱性が判明しています。

■ 脆弱性内容

脆弱性のリスクが特に高くなるケースは以下のようなケースです。

- 不特定多数のユーザーがアプリケーションサーバーにアクセスが可能な場合や外部インターネットからアプリケーションサーバーにアクセスが可能な場合（Blue Prism非推奨の構成）
- Blue Prismのアカウントを保有しているユーザーが悪意を持っており、リバースエンジニアリング等、ソフトウェアに関する高い知識を持っている

脆弱性の詳細は本書Appendix「[脆弱性一覧](#)」および以下のリンクのKBを参照してください。

KB（英語版・最新）：<https://portal.blueprism.com/customer-support/support-center#/path/-Featured-Articles/1873292732/>

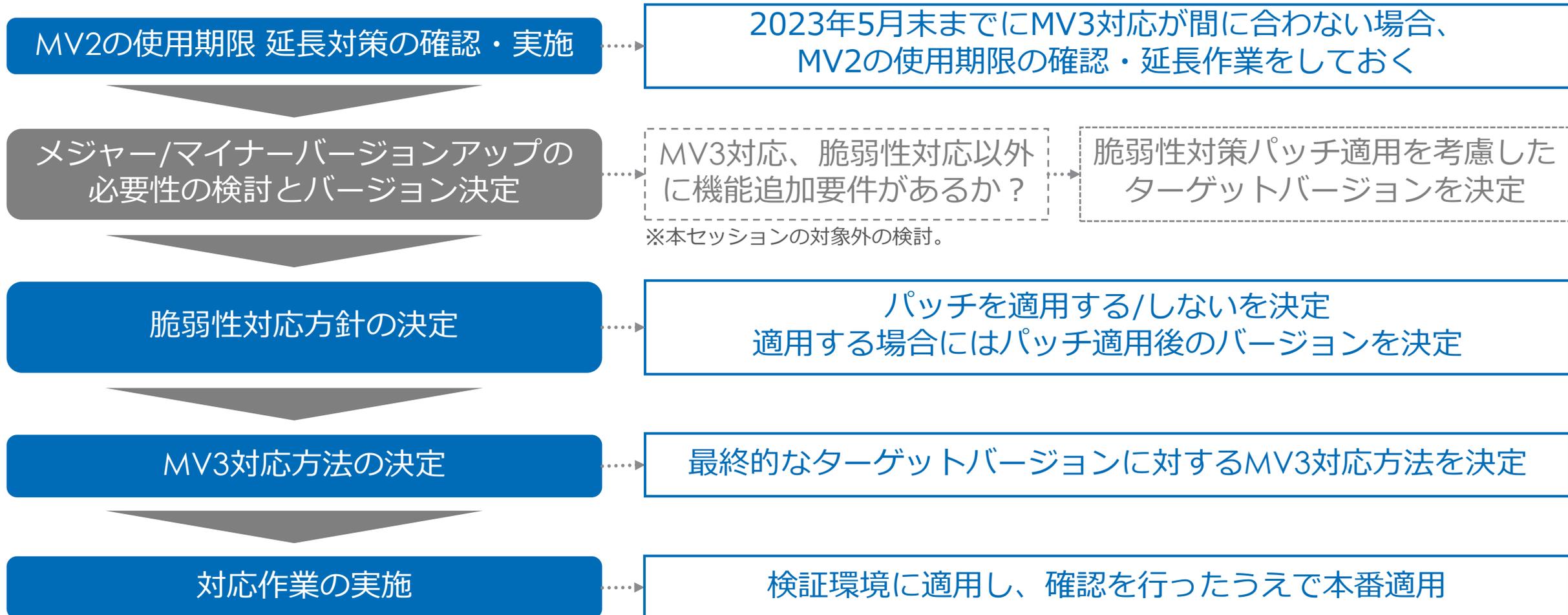
KB（日本語版）：<https://help-jp.blueprism.com/1878659032>

■ パッチリリース状況

- 2022/11/15 現在、**v6.4.x以降のすべてメジャー/マイナーバージョンに対するパッチはリリース済み**

MV3・脆弱性対応の進め方 概要

MV3対応、脆弱性対応は最終的に対象となるBlue Prismバージョンはどれか？
という点がポイントとなるため、以下の順序で確認・検討を行い、最終的なターゲットバージョンと対応方法を決定します。





3. 修正点と対策内容

MV2使用期限の延長

Enterprise Policyの設定について

- 2023年5月末までにMV3対応が間に合わない場合、Edge/ChromeのEnterprise Policyの設定により拡張機能の設定を行うことで、**MV2拡張機能の使用期限を2023年の年末まで延長することが可能**になります。
- Enterprise PolicyはChrome/Edgeの設定をポリシー設定（Windowsの場合にはレジストリまたはグループポリシーで行うのが一般的）により行います。従って、MV2使用期限の延長設定はブラウザ拡張機能を使用するマシンの**レジストリにBlue Prismのブラウザ拡張機能の設定を追加**することで設定が可能です。
- Blue Prismのインストーラーから拡張機能をインストールした場合、特定のバージョン以降ではインストーラーによりEnterprise Policy(レジストリ)が自動的に追加されてインストールが行われているため、基本的にはMV2使用期限延長の設定作業は必要ありませんが、MV3対応が2023年5月末までにMV3対応が完了しない見込みの場合には念のため**Enterprise Policyの適用確認を行うことを推奨**します。
（確認方法は後述）
 - Chrome : Blue Prismインストーラーからインストールした拡張機能はEnterprise Policyが適用済み
※「Chrome ウェブストア」サイトから手動で追加した拡張機能についてはEnterprise Policyが未適用の状態
 - Edge : Enterprise Policyが適用済みのバージョン⇒**6.10.3以降の6.10.X、7.0.1以降の7.0.X、7.1.X以降**
※上記バージョンであっても「Chrome ウェブストア」または「Edgeアドオン」サイトから手動で追加した拡張機能についてはEnterprise Policyが未適用の状態

Enterprise Policyが未適用のバージョン⇒**6.9-6.10.2、7.0**

脆弱性対策方針の検討

今回のタイミングでの脆弱性対策方針としては以下のような方針が考えられます。

- **今回は対応しない：**
以下のような点を考慮して今回のMV3対応のタイミングでは追加の対策は行わず、別のタイミングで改めて（なるべく早い段階で）対策を行う。
 - 自社の環境はある程度対策ができていて、またはリスクが高くない環境
 - 自社の環境、利用方法において、脆弱性パッチを適用したバージョンで判明している不具合によるリスクあり
 - パッチ適用後の動作確認にまで作業の手が回らない
- **リスク軽減対策を実施：**
Blue Prismの**ベストプラクティス**を踏襲し権限管理、ネットワークアクセス制限等の強化を行う
※対策内容は本書Appendix「[SS&C Blue Prism のセキュリティリスク軽減対策](#)」を参照
- **パッチ適用を行う（完全な対策）：**
MV3対応作業時にあわせて**パッチ適用（パッチバージョンのアップグレード）**を行う

最終的には本書Appendix記載の「[脆弱性の内容](#)」、「[リスク軽減対策](#)」、[不具合の情報](#)(下記のリンク先)を確認の上、**自社のセキュリティポリシーや作業影響や作業量を考慮**して今回どのような方針をとるかを決定してください。

【6.10 known issues】※ページ下部に以前のバージョンのIssuesへのリンクあり

<https://portal.blueprism.com/customer-support/support-center#/path/Upgrade-Expansion/Upgrade/1579866972/What-are-the-known-issues-in-Blue-Prism-Version-6-10.htm>

【7.1 known issues】※ページ下部に以前のバージョンのIssuesへのリンクあり

<https://portal.blueprism.com/customer-support/support-center#/path/Upgrade-Expansion/Upgrade/1813008122/What-are-the-known-issues-in-Blue-Prism-Version-7-1-releases.htm>

脆弱性対応パッチ

パッチバージョンのアップグレード

以下の対策バージョンに記載の対策パッチバージョンにアップグレードを行うことで、脆弱性への対応が可能です。
パッチはBPEの全コンポーネント(Application Server、Runtime Resource、Interactive Client)に適用する必要があります。

パッチ適用対象	対策パッチバージョン	リリース日	(2022年11月15日時点)
7.1.x	7.1.1	2022/9/5	
7.0.x	7.0.2	2022/8/19	
6.10.x	6.10.5 ^{※1}	2022/8/16	
6.9.x	6.9.1	2022/8/10	
6.8.x	6.8.3	2022/8/9	
6.7.x	6.7.4	2022/8/16	
6.6.x	6.6.2	2022/8/9	
6.5.x	6.5.2	2022/8/9	
6.4.x	6.4.5	2022/8/5	

※1：6.10.5にアップデートした場合、脆弱性対応が行われますが、特定の利用方法への影響があると考えられる6.10.5固有の未解決の不具合 BP-11535が確認されています。本書Appendix「[SS&C Blue Prism の不具合](#)」の内容を参照のうえ、**パッチ適用をするか、適用を延期するかを決定**してください。

KB（英語版・最新）：<https://portal.blueprism.com/customer-support/support-center#/path/-Featured-Articles/1873292732/>

KB（日本語版）：<https://help-jp.blueprism.com/1878659032>

MV3移行に伴う仕様変更

MV3ではブラウザー（Chrome/Edge）側のセキュリティの仕様が強化されることにより、Blue PrismのMV2ブラウザー拡張機能では使用可能だった以下の機能が動作しなくなります。

- JavaScriptフラグメントを挿入（Insert JavaScript）
- JavaScript関数の呼び出し（Invoke JavaScript）



Blue PrismではMV3対応後も「JavaScriptフラグメント挿入」と「JavaScript関数の呼び出し」を実行できるようにするため、ランタイムリソース上にインストールして、MV3拡張機能と連携動作する追加モジュールを開発しました。

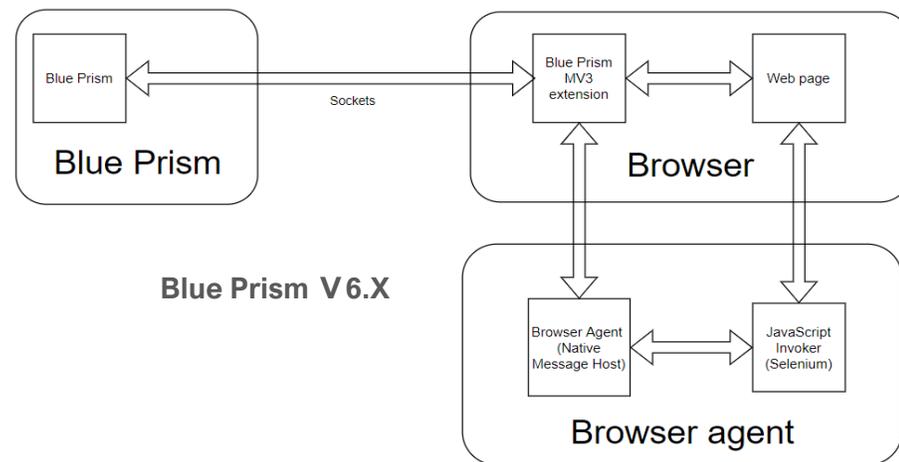
- Blue Prism Browser Automation Agent（以降BAA）

Browser Automation Agent (BAA)

BAAはBlue Prism MV3拡張機能と一緒に使用することを前提とした新しいコンポーネントです。BAAを導入することにより従来のMV2拡張機能と同様にMV3拡張機能からJavaScriptの挿入/呼び出し (Insert JavaScript/ Invoke JavaScript)の実行を可能にするとともに、v6.4.2以降のバージョンのBlue PrismにMV3拡張機能を提供します。

【特徴・注意点】

- Blue Prismバージョン**6.4.2～7.1.1との互換性**があります。
- BAAをインストールするとBAAと連携して動作する**専用のMV3拡張機能**をWebストアから自動インストールするためのレジストリがセットされます。つまり、**BAAをインストールすることでMV3ブラウザ拡張が自動インストールされ6.4.2以降のバージョンのMV3対応**を行うことができます。
- BAAはすべてのランタイムリソースに同時に適用する必要はありません。
- ChromeおよびEdgeのバージョンが**105 (2022年9月リリース) 以降**である必要があります。
- Blue Prismのバージョンに応じてインストールするべきBAAのバージョンが異なります。
BAA v1: Blue Prism 6.5.x ~ 6.10.5 ※2022年9月リリース済
BAA v2: Blue Prism 6.4.2 ~ 6.4.5、7.x ※2022年11月リリース予定
- JavaScriptの挿入/呼び出し機能を使用する場合には以下の追加作業が必要です。
 - 利用ブラウザのバージョンに対応した、Google/Microsoftが提供する**Webドライバー**をインストールし、**ブラウザのバージョンアップにあわせて更新していく**必要があります。
 - JavaScriptの挿入/呼び出し機能機能を利用する**既存BPオブジェクト内のアプリケーション起動設定の変更が必要** (※設定内容は後述)



【ダウンロード元】

Blue Prism ポータルサイトにログイン

製品 > Blue Prism Enterprise > [Blue Prism Browser Automation Agent](#)

MV3拡張機能 バージョン別対応方法一覧

Blue Prismバージョン毎のMV3対応方法は以下のようになります。

基本的な対応方法はBrowser Automation Agentのインストールとなりますが、JavaScriptフラグメントを挿入（Insert JavaScript）機能とJavaScript関数の呼び出し（Invoke JavaScript）機能を今後を含めて使用しない場合には7.1.Xと6.10.5のみ標準のMV3 Extensionを単独で使用する選択肢が存在します。

MV3対応するにはBAAおよび拡張機能が**サポートするブラウザのバージョン**にも注意が必要です。

BPバージョン	現在の状況・要件	MV3対応方法	インストール方法	インストールされるChrome Extensionバージョン	インストールされるEdge Extensionバージョン	ブラウザバージョン要件※1	JavaScriptの挿入・呼び出し機能の使用
6.4.2 ~ 6.4.5 or 7.0.x	6.10.5や7.1.Xにアップグレードせずに現在のバージョンでMV3拡張機能を使用	Browser Automation Agent v2の導入 ※2022/11リリース予定	BAAインストーラー(MSI)	Blue Prism Extension XXX Manifest V3	Blue Prism Extension XXX Manifest V3	XXXX	○
6.5.x ~ 6.10.4	6.10.5や7.1.Xにアップグレードせずに現在のバージョンでMV3拡張機能を使用	Browser Automation Agent v1の導入	BAAインストーラー(MSI)	Blue Prism Extension 6.5 - 6.10 Manifest V3	Blue Prism Extension 6.9 - 6.10 Manifest V3	v105以降	○
6.10.5	Insert/Invoke JavaScriptを使用しているまたは、今後使用する	Browser Automation Agent v1の導入	BAAインストーラー(MSI)	Blue Prism Extension 6.5 - 6.10 Manifest V3	Blue Prism Extension 6.9 - 6.10 Manifest V3	v105以降	○
	Insert/Invoke JavaScriptを使用していないかつ今後も使用しない	v6.10.5 MV3拡張機能の利用	BPインストーラーからMV3ブラウザ拡張をインストール (Webストアから自動更新)	Blue Prism v6.10.5 Browser Extension	Blue Prism v6.10.5 Browser Extension	v104以降	×
7.1.x	Insert/Invoke JavaScriptを使用しているまたは、今後使用する	Browser Automation Agent v2の導入 ※2022/11リリース予定	BAAインストーラー(MSI)	Blue Prism Extension XXX Manifest V3	Blue Prism Extension XXX Manifest V3	XXXX	○
	Insert/Invoke JavaScriptを使用していないかつ今後も使用しない	v.7.1.x MV3拡張機能の利用	BPインストーラーからMV3ブラウザ拡張をインストール (Webストアから自動更新)	Blue Prism v7.1 Browser Extension	Blue Prism v7.1 Browser Extension	※1のリンク先 参照	×

・ BAAv2は2022/11/16時点で未リリースのため情報が未確定ですリリース後にリリースノート等で確認をしてください。

※1 <https://bpdocs.blueprism.com/en-us/browser-compatibility.htm>

MV3拡張機能対応、パッチ適用後の動作確認について

MV3拡張機能対応、セキュリティパッチの適用後は以下の点に注意して動作確認を行ってください。

まずは開発/検証環境で全ての作業と動作確認を行い、手順と問題が発生しないことを確認してから本番環境に同様の作業を実施してください。

<バージョンアップグレードなし(MV3対応のみを実施した場合) >

- Chrome/Edgeを操作しているプロセス/オブジェクトの動作およびスケジュール実行の確認とアプリケーションモデラーでのスパイ操作の確認を実施してください。
- JavaScript機能を使用しているオブジェクトについては、特にJavaScript機能が動作することの確認が必要です。

<バージョンアップグレードあり（パッチ適用した場合） >

- 全コンポーネントが更新されているため、念のため使用している一通りの機能および全てのプロセス/オブジェクトの動作確認、スケジュール実行確認を実施してください。
- アップグレード前バージョンとアップグレード後バージョンの間のバージョンのリリースノートを確認し、機能・仕様変更が行われた内容や影響を確認した上で、特に変更部分に注意して動作確認を実施してください。

【Blue Prism Docs-リリースノート】 <https://bpdocs.blueprism.com/bp-7-1/ja-jp/release-notes/upgrade-notices.htm>



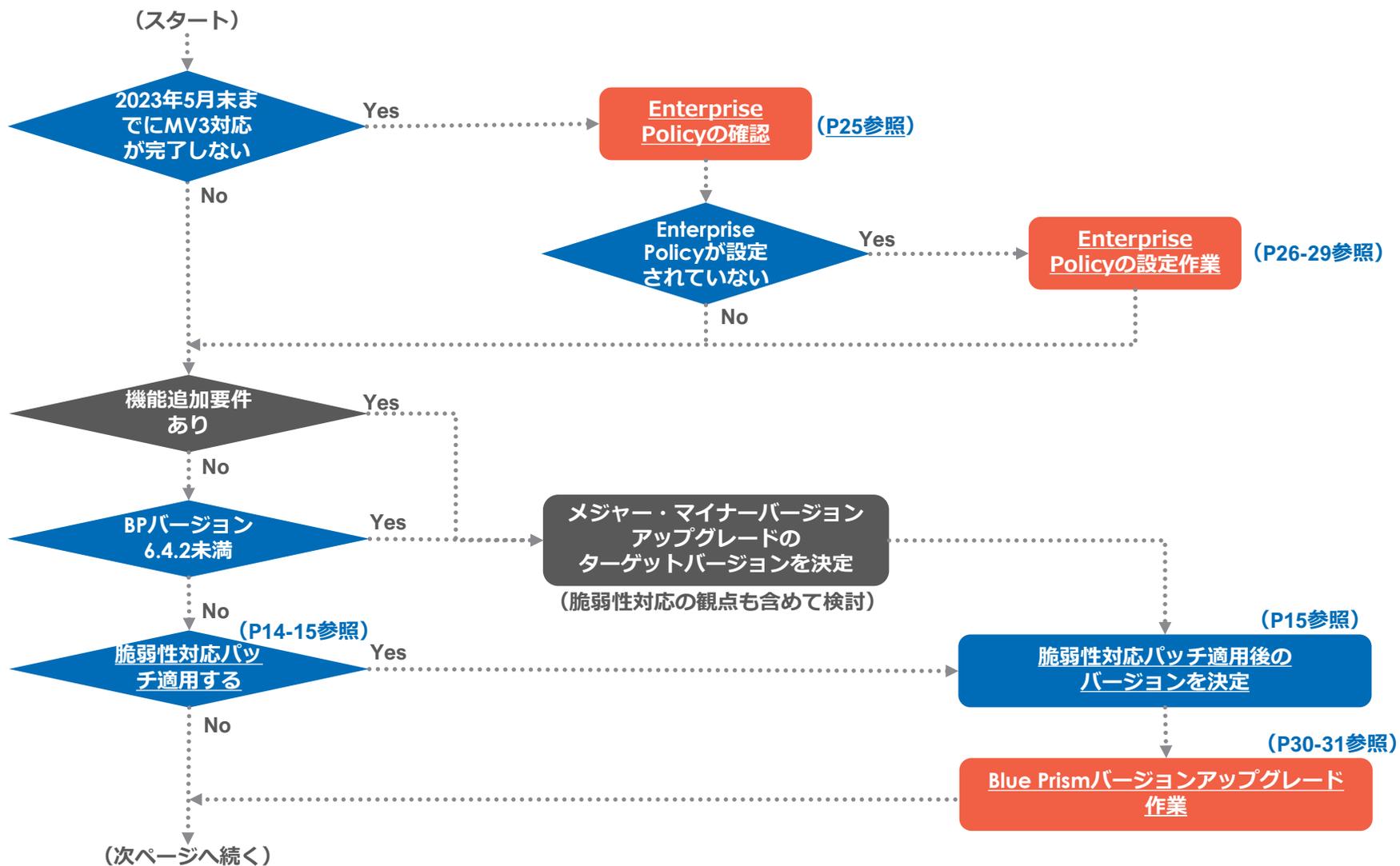
※Docsのアップグレード通知画面でアップグレード元と先を指定することで関連するバージョンのリリースノートのみを表示することができます。
ドロップダウンリストに表示されない最新バージョンについては個別にリリースノートを確認してください。



4. 対応ステップと 作業内容

MV3・脆弱性対応 対応ステップ

ステップ (1/4)



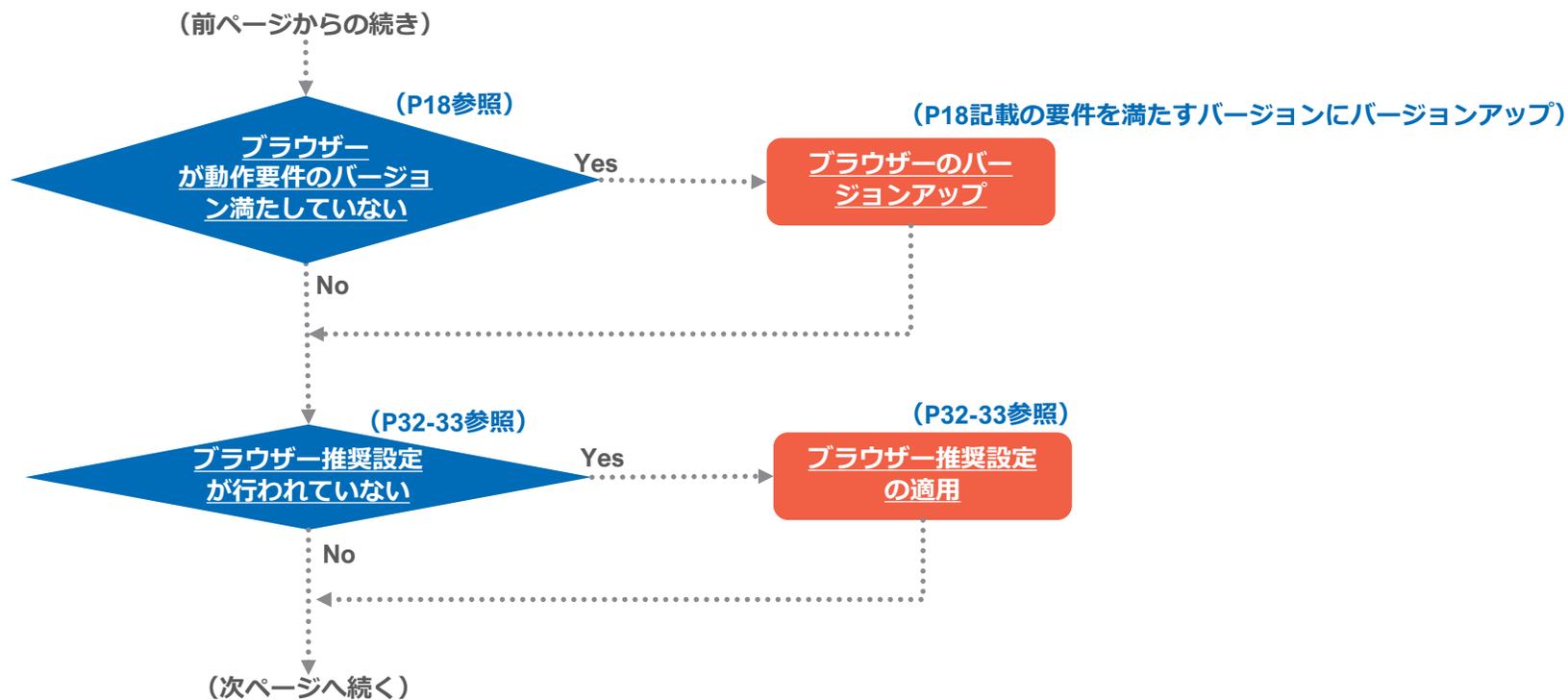
MV2実行期限延長

- 2023年5月末までに実施
- 検証環境での確認後に本番環境で実施

ターゲットバージョンの決定とバージョンアップ作業

- 2023年12月末までに実施
- 検証環境での確認後に本番環境で実施

MV3・脆弱性対応 対応ステップ ステップ (2/4)



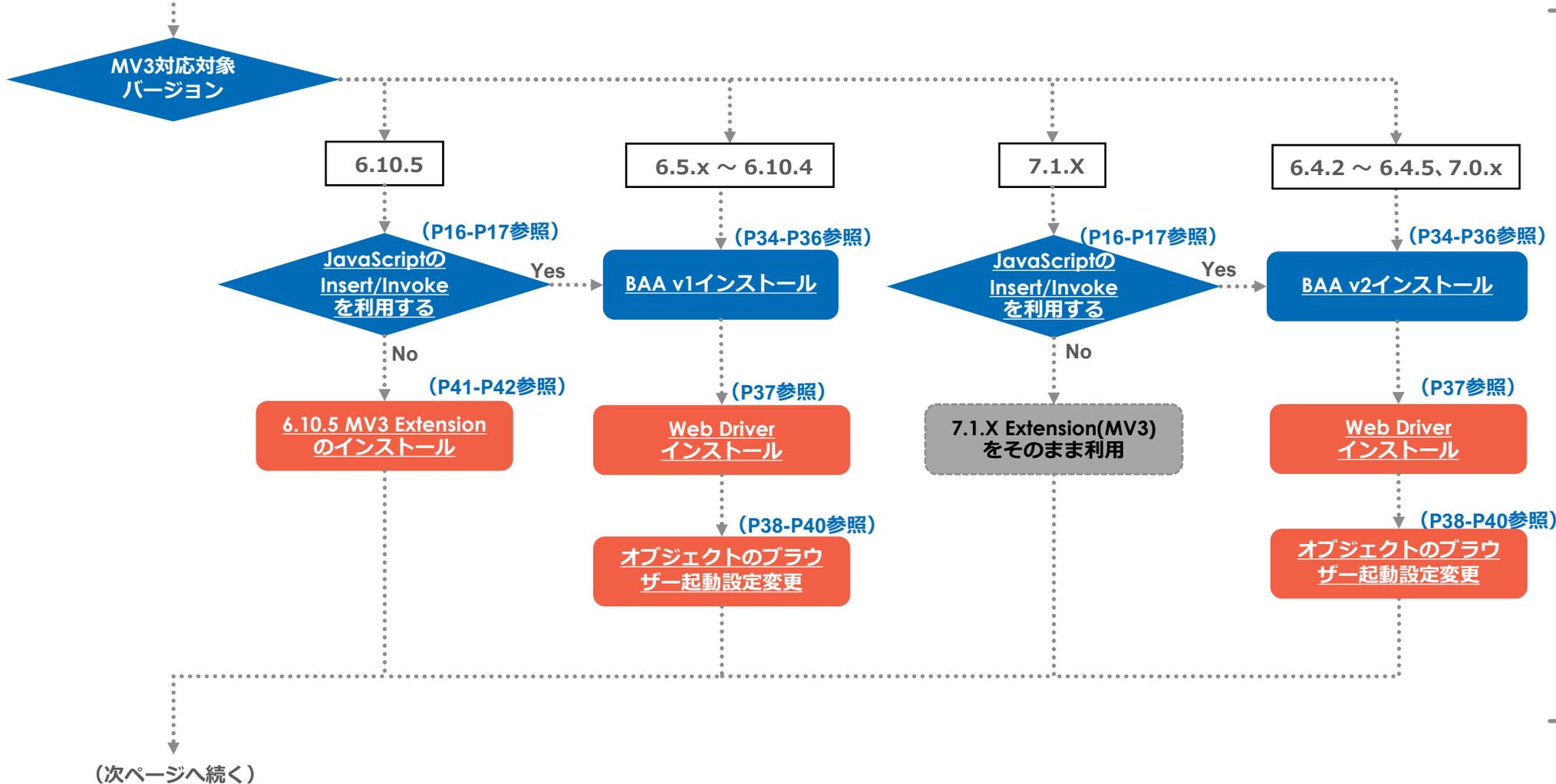
ブラウザ設定変更作業

- 2023年12月末までに実施
- 検証環境での確認後に本番環境で実施

MV3・脆弱性対応 対応ステップ

ステップ (3/4)

(前ページからの続き)

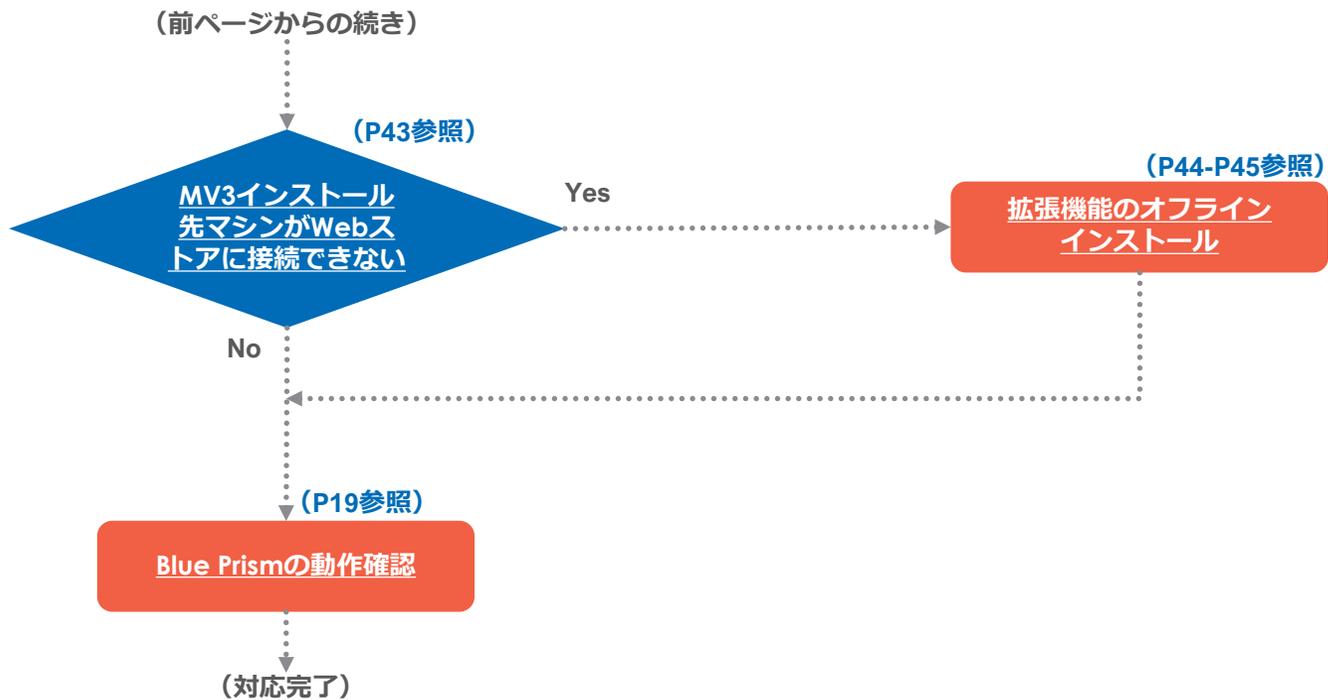


MV3対応作業

- 2023年12月末までに実施
- 検証環境での確認後に本番環境で実施

(次ページへ続く)

MV3・脆弱性対応 対応ステップ ステップ (4/4)



拡張機能のオフライン展開

- 2023年12月末までに実施
- 検証環境での確認後に本番で実施

プロセスの動作確認

- 2023年12月末までに実施
- 検証環境での確認後に本番で実施

Enterprise Policy設定の確認

Enterprise Policyにより拡張機能が導入されている(MV2の使用期限が2023年末まで延長される)かどうかを確認します。



Enterprise Policy有効

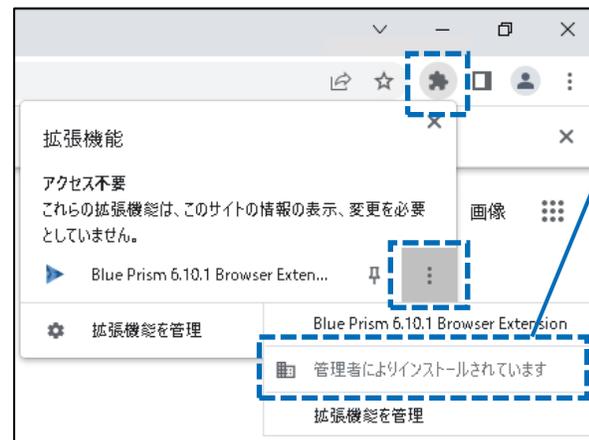
MV2の使用期限が延長される
(2023年12月末が期限)

Edge



「組織によってインストールされています」が表示されていることを確認

Chrome

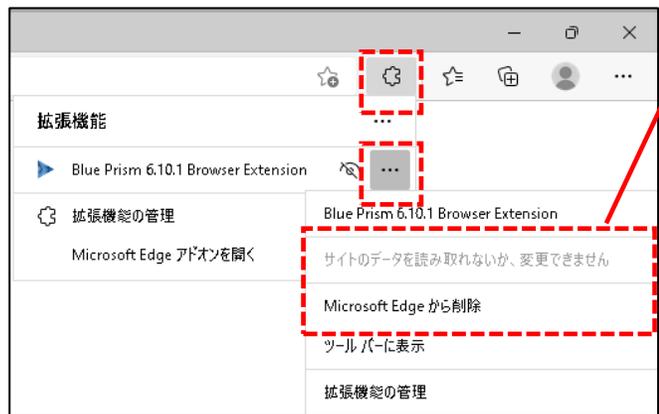


「管理者によりインストールされています」が表示されていることを確認

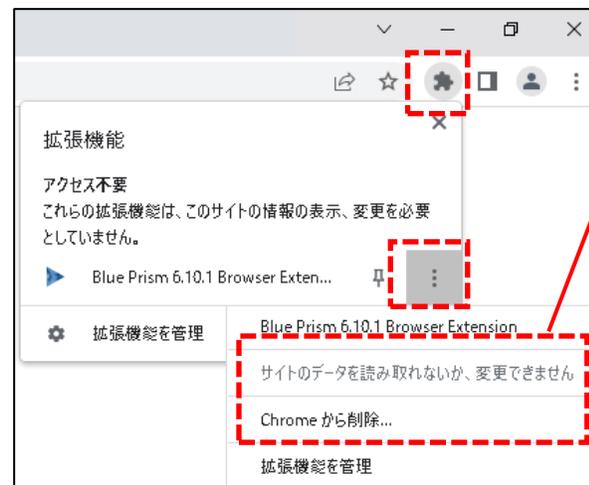


Enterprise Policy無効

MV2の使用期限が延長されない
(2023年5月末が期限)



「組織によってインストールされています」が表示されていない & 「Microsoft Edgeから削除」が表示されている



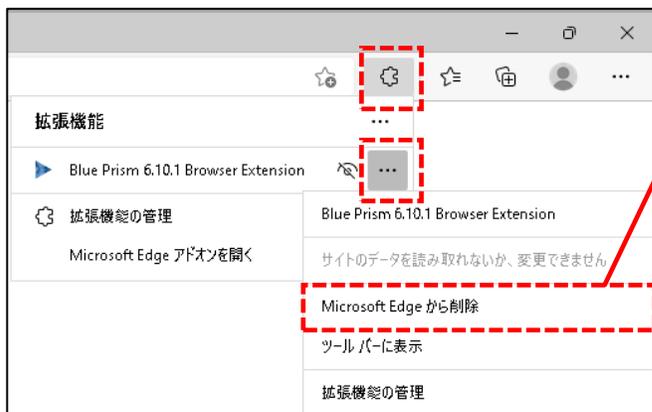
「管理者によりインストールされています」が表示されていない & 「Chromeから削除」が表示されている

Enterprise Policyの設定

設定手順

Enterprise Policyが無効の拡張機能について、MV2の使用期限を延長したい場合には以下のように設定を行います。

1. Enterprise Policyが無効な拡張機能を一旦削除してから開いているWebブラウザを全て終了します。



「Microsoft Edgeから削除」をクリックして拡張機能を削除



「Chromeから削除」をクリックして拡張機能を削除

2. MV2の使用期限延長対象となるBlue Prismのバージョンに対応するブラウザ拡張機能のEnterprise Policyを次ページ記載の[レジストリ設定](#)を参考の上、ブラウザ拡張が導入されている各マシンに以下のような方法で追加してください。
 - レジストリエディタを起動して手動設定（「regedit」をWindows上で検索・指定して起動）
 - バッチファイルを作成/実行してレジストリを追加 ※参考：[reg add | Microsoft Learn](#)
 - グループポリシーによるレジストリ配布
※グループポリシーによるレジストリの設定は自社のActive Directory構成やグループポリシーを把握した上で実施してください。
⇒BAA/MV3拡張機能のインストール時にここで設定したレジストリを削除する必要がでてくるため、設定したレジストリを記録しておきます。
3. Enterprise Policyが有効になっていることを[前ページ](#)の手順で再度確認します。

Enterprise Policyの設定

レジストリ設定内容

該当するレジストリが存在しない場合には以下のレジストリを追加することで、Enterprise Policyによりブラウザ拡張機能が管理、インストールされた状態になります。

Chrome ブラウザ拡張用 レジストリキー	レジストリキー	HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Google¥Chrome¥ExtensionInstallForcelist
	名前	0 ※他のExtensionが設定済みの場合には通番で利用されていない番号を設定
	タイプ	REG_SZ
	データ	<現在使用しているブラウザ拡張機能のID> ; https://clients2.google.com/service/update2/crx ※ブラウザ拡張機能のIDはバージョンによって設定値が異なるため本章「 ブラウザ拡張機能のID 」項を参照のうえ、ブラウザ拡張のID文字列を設定します。 (例 6.10.1の場合) ocmhoiiiibobfmailfagflkgbgajddem; https://clients2.google.com/service/update2/crx
Edge ブラウザ拡張用 レジストリキー	レジストリキー	HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Edge¥ExtensionInstallForcelist
	名前	0 ※他のExtensionが設定済みの場合には通番で利用されていない番号を設定
	タイプ	REG_SZ
	データ	<現在使用しているブラウザ拡張機能のID> ※本章「 ブラウザ拡張機能のID 」項を参照のうえ、ブラウザ拡張のID文字列を設定します。 (例 6.10.1の場合) gdappmgmiaanopfdghgjbkafmiaidlb

(参考) グループポリシーテンプレートを使用した設定について

「ExtensionInstallForcelist」キー配下へのレジストリ設定はグループポリシーのChrome/Edgeの管理用テンプレートを使用して下記グループポリシーから設定することも可能ですが、管理用テンプレートの設定を使用した場合、「ExtensionInstallForcelist」キー配下のレジストリが全て上書きされてしまうため、Blue Prism以外の拡張機能への影響を考慮して本Webinarではレジストリを直接する方法をご紹介します。

既にグループポリシーを使用して「ExtensionInstallForcelist」の設定を実施している場合には、設定のリストに上記「データ」部分の値を追加してください。

- Chrome ポリシー名：「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」
- Edgeポリシー名：「サイレントインストールされる拡張機能を制御する」

Enterprise Policyの設定

ブラウザ拡張機能のID

ChromeとEdgeのブラウザ拡張機能のEnterprise Policy設定の際に必要なブラウザ拡張機能のID（バージョン固有の文字列）は以下となります。

BPバージョン・BAA	マニフェストバージョン	Chrome用拡張機能	Edge用拡張機能
BAA v2(6.4.X,7.X.X)	MV3	※2022年11月リリース予定（未定）	※2022年11月リリース予定（未定）
BAA v1(6.5-6.10)	MV3	klbaonekdddbnllienjepielnkjmhjdo	iahgjfpdlfklnkloonnhokgnojbpcfof
7.1.1 7.1	MV3	koibfinjpefmmmdmmdiiicglmhefhjllhn	alphbcchbekpcafaknckinfpapdaiiol
7.0.1	MV2	hpaajmgfhgakaamoopdhieneihpmeapm	chgmlbmnllciejdidlnllecnifgjhepe
7.0	MV2	lbnooplepikajpiphjgfoniaakpclemh	jecmlbbpjadglfjggkpcckhheoblfdohf
6.10.5 (MV3)	MV3	pgdpmkfahhejhfpgejaendjeeacoknjf	bcbgfmnbngklahikmeloakcpkaakelojd
6.10.4/6.10.5 (MV2)	MV2	gccejhjelnjpcpfodkdhkcgpalkihdc	dafncfjkbhbdcdbdnaingpgiglcbbggeh
6.10.3	MV2	oiapacjhgpaojehgcndepionkjphanoe	iopomglpadeamepdjjnhcmacjhphbcda
6.10.2	MV2	bnkfnbanaddcalcbanfmlbeljhbhjmmba	mpdplhcjcmelfpjbhipheipoekblggm
6.10.1	MV2	ocmhoiilbobfmailfagflkbgagjddem	gdapppmgmiaanopfdghgjbkafmiaidlb
6.10	MV2	aaedoanmdcohhdbadkgjjfdmbbmiffe	hekghghgjpohegdkkakdkgpcgelmemkk
6.9	MV2	apjdloapfacpgloidbikcdcigljkogg	ibnlinbgdfifaiecfljcedlcfpfhakco
6.5.x~6.8.x	MV2	nadpbbdaaifbaebnniobcfpiifbfokij	
6.4.x	MV2	oafhlmnamdgbgdgkpihkkdfapkebfp	

Enterprise Policyの設定

注意点

- **Blue Prismのアップグレード/インストール時の注意事項**

MV2の使用期限延長のためにEnterprise Policyのレジストリ設定を後から追加した場合、次にBlue PrismのアップグレードやBAA/MV3拡張機能のインストールを行う際には、念のため**手動設定したレジストリを削除**してからアップグレード/インストール作業を実施してください。

手動追加したレジストリの削除を行わないと、場合によって複数のブラウザ拡張機能がインストールされた状態となり、Blue Prismのブラウザ連携機能が正しく動作しなくなります。

- **オフラインマシン環境に関する注意**

Enterprise Policyによるブラウザ拡張機能の設定は該当マシンのブラウザがインターネット上の以下のWebストアに接続が可能な場合のみインストールされ有効になります。

- Chrome : <https://clients2.google.com/service/update2/crx>
- Edge : <https://edge.microsoft.com/extensionwebstorebase/v1/crx>

インターネットに接続していない環境（オフライン環境）のランタイムリソースに対してはEnterprise Policyを適用して拡張機能の展開ができませんが、そもそもChrome/Edgeの自動アップデートが行えず、Webストアサイトにも接続しないため、MV2期限の延長を行わなくてもMV2拡張機能の継続利用が可能な可能性が高いと考えられます。

但し、Webブラウザをインストーラーから手動更新したり、一時的にインターネットに接続されるようなことがあった場合に、突然MV2が使用できなくなる等のトラブルが考えられるため、早い段階でMV3対応プラグインの**オフラインインストール**を実施することを推奨します。

Blue Prismのアップグレード作業（パッチ適用）

作業手順（1/2）

Blue Prism Enterpriseの一般的なバージョンアップグレード(パッチ適用)作業は以下のような手順で実施します。必ず、開発/検証環境で先に実施して問題がないことを確認の上、本番環境で実施してください。

1. 現在実行中のプロセス/スケジュールを停止します。
2. インタラクティブクライアント、ランタイムリソース、アプリケーションサーバーを終了します。
3. 可能な場合にはインタラクティブクライアント、ランタイムリソース、アプリケーションサーバーの仮想マシンスナップショットを取得します。（仮想マシン切り戻し用）
4. データベース（データファイルとトランザクションログ）をバックアップします。（データベースの切り戻し用）
5. インタラクティブクライアント、ランタイムリソース、アプリケーションサーバーでアップグレードのターゲットバージョンのBlue Prism MSIインストーラーを実行し、新しいバージョンをインストールします。
6. アップグレードでデータベースバージョンが更新される場合、これらはBlue Prismの接続構成画面、または手動で適用されるSQLアップグレードスクリプトを介して適用します。（更新前後のデータベースバージョンはリリースノートに記載を確認してください。）
データベースをアップグレードする場合は、以下の役割を持つSQLユーザーアカウントが必要です。
 - ▶ アップグレードに既存のデータベースの削除が含まれる場合：sysadmin（サーバーの役割）。
 - ▶ アップグレードに既存のデータベースの削除が含まれていない場合：sysadmin（サーバーの役割）またはdbowner（データベースの役割）。

Blue Prismのアップグレード作業（パッチ適用）

作業手順（2/2）

7. Blue Prism環境にログインし、インストールを検証して、画面上に警告等のメッセージがないことを確認します。
8. Login Agentが環境内で使用されており、更新版を適用する必要がある場合、すべての適切なデバイスで付属のMSIインストーラーを実行して更新版をインストールします。（更新前後のバージョンのリリースノートを確認してください。）
Blue Prismがインストールされると、Login AgentのインストーラーはBlue Prismのインストール場所のインストーラーフォルダー(規定のパスは C:¥Program Files¥Blue Prism Limited¥Blue Prism Automate¥Installers)に格納されます。
9. Login Agentの更新後、更新されたLogin Agent Blue Prismのリリースファイル(プロセス/オブジェクト)を関連環境にインストールし、関連プロセスが更新されたLogin Agent VBOを参照することを確認します。
10. 各Blue PrismサーバーでBlue Prismサーバーサービスを開始し、すべてのBlue Prismクライアントを再開します。

【参照URL】

<https://bpdocs.blueprism.com/bp-6-10/ja-jp/Release%20Notes/Release%20Notes/applying-updates.htm>

<https://bpdocs.blueprism.com/bp-7-1/ja-jp/release-notes/applying-updates.htm>

<https://www.blueprism.com/japan/resources/webinars/webinar-blue-prism-upgrade-20210609>

Webブラウザ推奨設定

推奨設定 (1/2)

MV3、MV2によらず、拡張機能の動作やスパイ動作を安定させるため、以下の設定が推奨されます。

■ブラウザのシステム設定

- Edgeの推奨設定
[設定] > [システムとパフォーマンス]
 - スタートアップブースト：無効
 - Microsoft Edge が閉じられたときにバックグラウンド拡張機能とアプリの実行を続行する：無効
- Chromeの推奨設定
[設定] > [システム]
 - Google Chrome を閉じた際にバックグラウンド アプリの処理を続行する：無効

【参照 URL】 [Modern Browser Automation - 問題と解決策 第4回 - ブラウザー拡張機能が検知できない問題 | Blue Prism 公式 note](#)

Webブラウザ推奨設定

推奨設定 (2/2)

■ブラウザの自動更新の停止

- ブラウザーの自動アップデートによりロボットの動作が不安定になる等のリスクを考慮して、ブラウザ自動更新設定を停止し、定期的に検証環境で事前検証を行った上で、手動アップデートを行うことを推奨します。
※自動更新が有効な場合、Webブラウザのバージョンが自動更新されたタイミングでWebドライバーとのバージョンの不一致が発生し、Blue Prismの「JavaScriptフラグメント挿入」、「JavaScript関数の呼び出し」機能が動作しなくなるリスクも発生します。
- 自動更新の停止方法の例としてはグループポリシーで設定する方法や直接レジストリ設定を行う方法があります。以下のサイト等を参照し、必ず事前に開発/検証環境で確認をした上で設定を行ってください。
 - Chrome :
(グループポリシーによる設定) [Chrome のアップデートを管理する \(Windows\) - Chrome ブラウザーの更新を無効にする](#)
(レジストリ設定) キー : HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Google¥Update
名前 : Update{8A69D345-D564-463C-AFF1-A69D9E530F96}
値 : 0 (REG_DWORD) ※0=更新を無効にする
 - Edge:
(グループポリシーによる設定) [ポリシー設定を使用して Microsoft Edge for Windows を構成する | Microsoft Learn](#)
[Microsoft Edge Update のポリシーに関するドキュメント | Microsoft Learn](#)
(レジストリ) キー : HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥EdgeUpdate
名前 : Update{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
値 : 0 (REG_DWORD) ※0=更新を無効にする
- 自動更新を無効化したブラウザのアップデートを実施する際には上記の設定を一次的に「手動更新のみ」(レジストリは「2」)に変更した上で手動アップデートを実施して再度、再度自動更新の無効化を行ってください。

Browser Automation Agent (BAA) のインストール手順

BAAインストール手順 (1/3)

1. Blue Prism Portalサイト (<https://portal.blueprism.com/>) にアクセスします。
2. 上部のメニューから、製品(Product) > Blue Prism Enterprise > Blue Prism Browser Automation Agent のページを開き [Download the installer]ボタンからインストーラーをダウンロードします。
3. 手動でMV2ブラウザ拡張のEnterprise Policy (レジストリ) の設定を行っている場合には以前に追加したレジストリを削除します。
4. 起動しているChrome/Edgeを全て終了します。
5. ダウンロードしたインストーラーを実行します。
6. [開始する]ボタンをクリックします。



Browser Automation Agent (BAA) のインストール手順

BAAインストール手順 (2/3)

6. 「ライセンス契約の条件に同意します」のチェックを入れて、[次へ]ボタンをクリックします。

← 戻る blueprism

ライセンス契約

重要な契約内容に同意していただけます。

We (Blue Prism Software, Inc. if you are in the Americas or Blue Prism Limited if you are in any other jurisdiction) have set out here the terms that apply to the digital workforce we provide to you.

The relevant Parts of this document, and the order (where "order" means an order on the Blue Prism Order Form or other document agreed with us, or between you and an authorised Blue Prism reseller ("Reseller")), contain the whole agreement between you and us relating to the subject matter hereof and set out the terms on which you can use our products and services (our "Agreement"). The order sets out the software licensed to you (the "Software") and the support we provide. The Agreement starts on the date set out in the order and lasts until the end of the license term also specified there, unless it is terminated earlier in accordance with these terms.

PART 1 CONTAINS A STANDARD LICENSE. IF YOU ARE AUTHORISED TO USE THE SOFTWARE ON A STANDARD BASIS, PART 1 WILL APPLY. PART 1 ALSO APPLIES IN THE FOLLOWING INSTANCES, ALONG WITH THE RELEVANT ADDENDUM:

ライセンス契約の条件に同意します。

次へ

7. 高度なインストールをチェックしてから[次へ]ボタンをクリックします。

← 戻る blueprism

インストール場所

Blue Prism ブラウザー自動化エージェントをどこにインストールしますか?

高度なインストール

C:\Program Files\Blue Prism Limited\Blue Prism Browser Automation Agent

場所を変更

次へ

8. 利用するブラウザ拡張機能がチェックされていることを確認して [インストール] をクリックします。

← 戻る blueprism

高度なインストール

どの機能をインストールしますか?

Blue Prism ブラウザー自動化エージェント

Chromeブラウザ拡張機能

Edgeブラウザ拡張機能

リセット ディスク使用量 ヘルプ

インストール

【注意】インターネットに接続されていない環境の場合には拡張機能をチェックを外しておき、後からオフラインインストールを実施してください

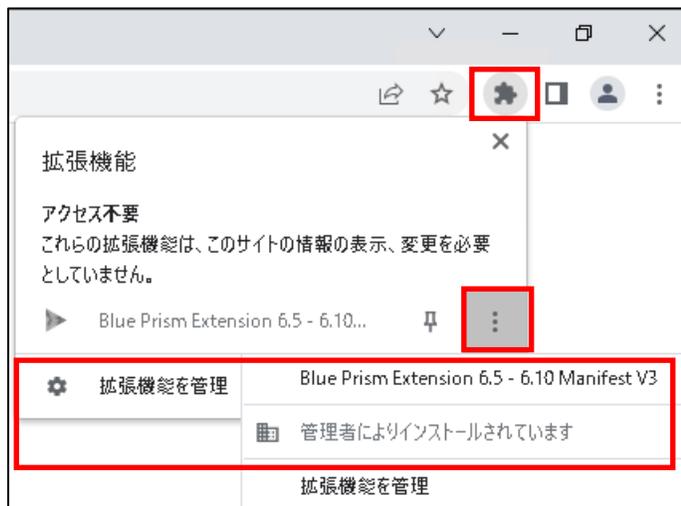
Browser Automation Agent (BAA) のインストール手順

BAAインストール手順 (3/3)

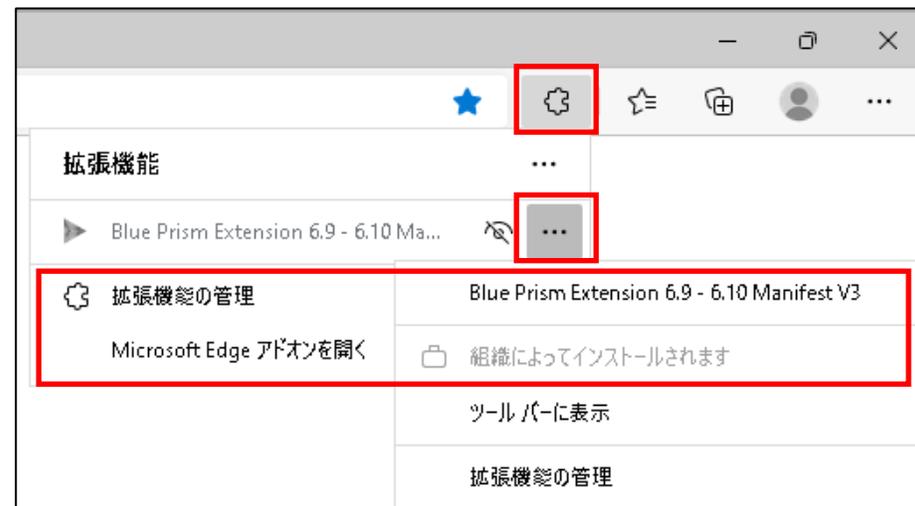
- [OK]ボタンをクリックしてインストーラーを終了します。
- Edge、Chromeを開き、「Blue Prism ExtensionManifest V3」がインストールされていることを確認します。



【Chrome】



【Edge】



MV3拡張機能 + BAA環境におけるJavaScript 機能の利用

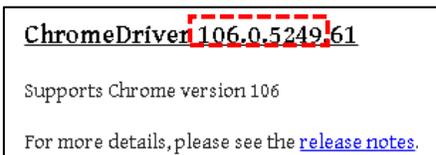
Webドライバーのインストール

- JavaScript機能を利用する場合にはブラウザのバージョンに対応するWebドライバを下記URLからZIPファイルとしてダウンロードします。（JavaScriptの機能を使用しない場合にはインストールは必須ではない）
 - Chrome: <https://chromedriver.chromium.org/downloads>
 - Edge: <https://developer.microsoft.com/en-us/microsoft-edge/tools/webdriver/>
- ダウンロードしたZIPファイルからWebドライバーの実行可能ファイル(chromedriver.exe, msedgedriver.exe)を解凍抽出し、BAAのインストール フォルダ (既定の場所は **C:¥Program Files¥Blue Prism Limited¥Blue Prism Browser Automation Agent**) または Windowsの環境変数でPATH定義されているフォルダに保存します。

ヘルプ->Chromeについてからバージョンを確認



該当するバージョンのChrome Driverをダウンロード

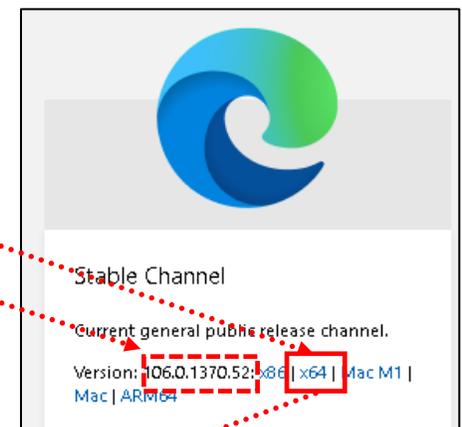


.....> chromedriver.exe

ヘルプとフィードバック->Microsoft Edgeについてからバージョンを確認



該当するバージョン/アーキテクチャーのDriverをダウンロード



msedgedriver.exe <..... (edgedriver_win64.zip)

MV3拡張機能 + BAA環境におけるJavaScript 機能の利用

変更対象の確認 (1/2)

JavaScript 機能（JavaScriptフラグメント挿入、JavaScript関数の呼び出し）を使用している既存プロセス/オブジェクトを調査するためのツール「**Process for Manifest v3 Impact Assessment Utility**」を提供しています。このツールを使用して、**Chrome/Edgeの起動パラメーター設定を変更する必要がある既存オブジェクトを特定**することができます。特定したオブジェクトのブラウザ起動設定を次ページ以降の設定内容に従って設定変更します。

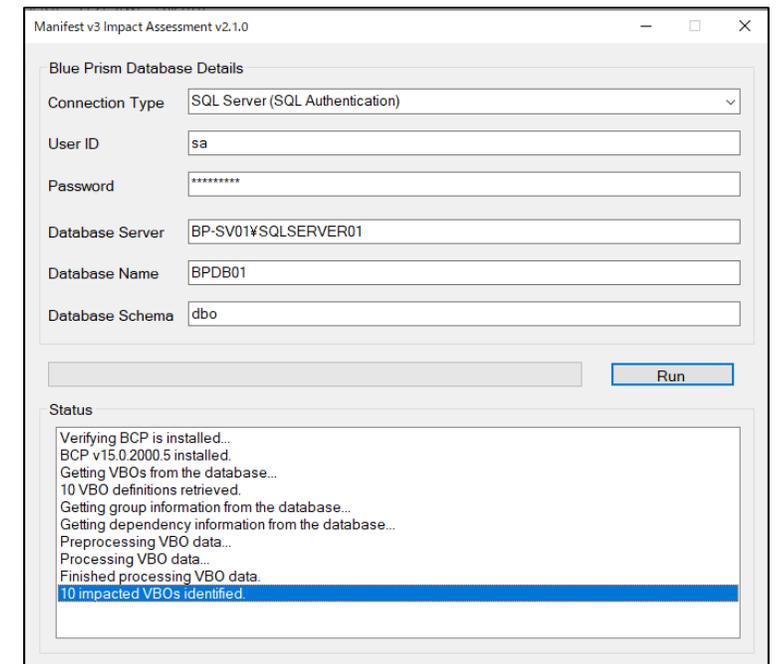
【Process for Manifest v3 Impact Assessment Utility - Download URL】

<https://digitalexchange.blueprism.com/dx/entry/3439/solution/manifest-v3-impact-assessment-utility>

【ツールの実行方法】

※ツールの実行のために必要な依存モジュールはダウンロードしたフォルダ内にある「README.pdf」を参照してください。

- ツールを起動し、確認対象となるBlue Prismデータベースへの接続情報を入力して、[Run]ボタンをクリックして実行します。



MV3拡張機能 + BAA環境におけるJavaScript 機能の利用 変更対象の確認 (2/2)

【実行結果】

ツールを実行すると、確認結果が以下の二つのcsvファイルに出力されます。

ImpactedVBOs.csv

	A	B	C	D	E
1	VBO Name	Group	Browser	Inject Javascript	Invoke Javascript
2	Google Cloud - Authentication 02	Default	CHROME	FALSE	FALSE
3	RoboReview	RevealGroup	CHROME	FALSE	FALSE
4	MFA Login - Chrome	Multifactor Authentication	CHROME	FALSE	FALSE
5	Google Chrome Browser	Google Chrome	CHROME	TRUE	TRUE
6	Open Bank Project - Authentication OLD	Default	CHROME	FALSE	FALSE
7	Digital Exchange - Chrome	Digital Exchange	CHROME	FALSE	FALSE
8	Digital Exchange - Edge	Digital Exchange	MSEDGE	FALSE	FALSE
9	Test Browser Object	Default	CHROME	FALSE	FALSE

「Inject Javascript」、「Invoke Javascript」欄のいずれか、または両方のデータがtrueとなっているVBOがJavaScriptの機能を利用しているオブジェクトです。

⇒ **ブラウザの起動設定を変更する必要がある既存オブジェクト**

DependentProcesses.csv

	A	B	C
1	VBO Name	Calling Process/VBO Name	Calling Process/VBO Type
2	COVID-19 Tracker	General Test 2	PROCESS
3	COVID-19 Tracker	Test for COVID-19 Tracker	PROCESS
4	Google Chrome Browser	Google Cloud - Authentication 02	OBJECT
5	MFA Login - Chrome	Microsoft MFA Login Test	PROCESS
6	MFA Registration - Chrome	Microsoft MFA Registration Test	PROCESS
7	Genesys PureCloud Authentication	Test - Genesys PureCloud	PROCESS
8	Johns Hopkins University COVID-19 Dashboard	Test for JHU COVID-19 Tracker	PROCESS
9	Digital Exchange - Chrome	Test Object	OBJECT

ImpactedVBOs.csvで判明したJavaScriptの機能を利用しているオブジェクト(VBO Name)を呼び出しているプロセス名を「Calling Process/VBO Name」欄で全て確認します。

⇒ **JavaScript機能の動作確認を行うべき既存プロセス**

MV3拡張機能 + BAA環境におけるJavaScript 機能の利用

ブラウザー起動設定の変更

■ Chrome/Edgeの起動設定変更

JavaScript機能を利用する/しているオブジェクトのアプリケーションモデラー内のブラウザーのコマンドラインパラメーター設定に以下のパラメーターを追加します。

⇒既存オブジェクトの設定変更

--remote-debugging-port=9222

※URL等の既存パラメーターの次に半角スペースを開けて指定

※ポート番号9222は利用されていない任意のポート番号に変更することも可能

■ 確認方法

デバッグポートのパラメーターなしでブラウザーを起動すると、[BluePrism.BrowserAutomationAgent.exe]のみが起動します。

デバッグポートのパラメーターを有効にしてブラウザーを起動すると、[BluePrism.BrowserAutomationAgent.exe]に加えて **[BluePrism.JavaScriptInvoker.exe]** が起動します。

Windowsのタスクマネージャー > [詳細]タブ等で確認してください。

BluePrism.BrowserAutomationAgent.exe	11452	実行中
BluePrism.JavaScriptInvoker.exe	31812	実行中

【アプリケーションモデラーの設定】

アプリケーション名
MV3-Javascript

ブラウザーのパスを入力してください
C:\Program Files (x86)\Microsoft\Edge\Application\r

スタートページのURLや、ブラウザーの起動時に使用されるその他の[コマンドライン]パラメーターを入力してください。
https://yahoo.co.jp --remote-debugging-port=9222

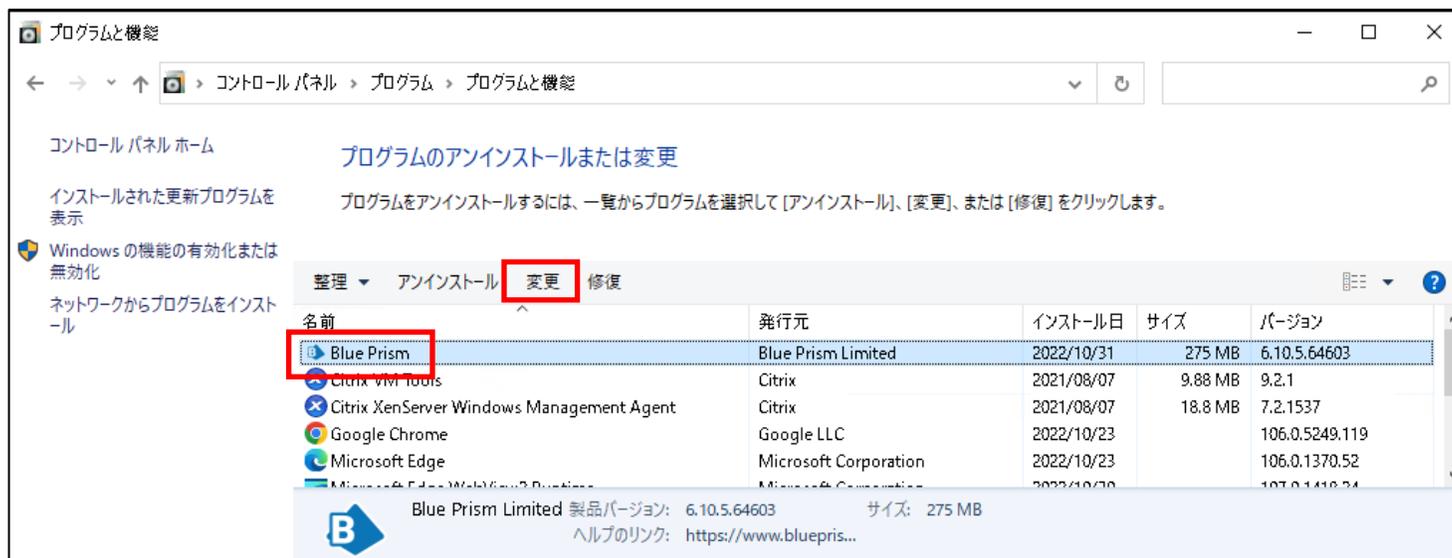
BAAを導入しない場合のMV3ブラウザ拡張インストール

Blue Prism 6.10.5 へのMV3拡張機能インストール (1/2)

MV2ブラウザ拡張機能がインストールされた環境を6.10.5にアップグレードした場合や6.10.5のインストールオプションでMV2ブラウザ拡張機能を選択してインストールした場合、Blue Prism 6.10.4 Browser Extension(MV2)がインストールされます。

このような環境で拡張機能をMV3に変更するには、以下の手順でMV3拡張機能をインストールする必要があります。

1. Windowsのコントロールパネル>プログラム>プログラムと機能を開きます。
2. 一覧で「Blue Prism」を選択し、[変更]ボタンをクリックします。



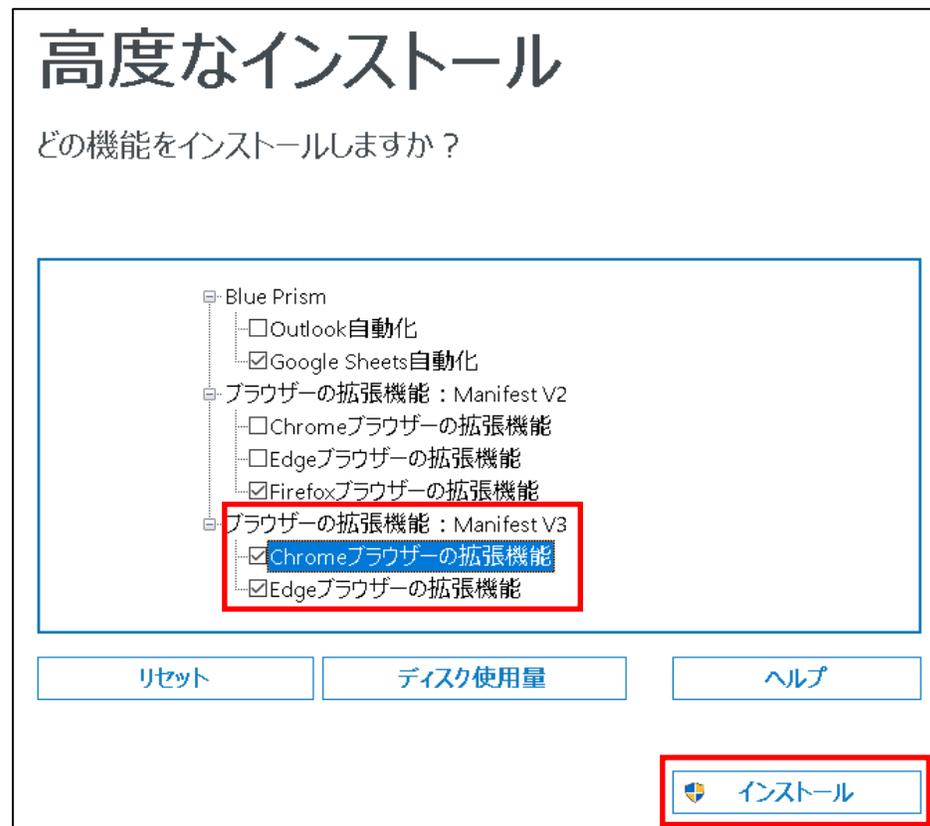
BAAを導入しない場合のMV3ブラウザ拡張インストール

Blue Prism 6.10.5 へのMV3拡張機能インストール (2/2)

3. 「機能を変更」をクリックします。



4. 「ブラウザの拡張機能：Manifest V3」の下のインストールしたいMV3拡張機能をチェックして、[インストール]ボタンをクリックして拡張機能のインストールを実行します。



拡張機能のオフラインインストール

- ランタイムリソースがインターネット環境に接続可能でWebストアサイトに接続可能な場合、BAAやBlue Prismのインストーラーからブラウザ拡張機能をインストールすると自動的にブラウザのEnterprise Policyが追加されブラウザ拡張機能がインターネット上のWebストアサイトから自動インストールされます。
インターネットに接続していない環境やWebストアへの接続が許可されない環境（オフライン環境）のマシンについては、次ページからの「拡張機能のオフラインインストール方法」等により**ブラウザ拡張機能をオフラインインストール**する必要があります。

【拡張機能インストール元WebストアURL】

Chrome : <https://clients2.google.com/service/update2/crx>

Edge : <https://edge.microsoft.com/extensionwebstorebase/v1/crx>

- オフラインインストールの実行はユーザープロファイルに対して実行されるため、インストール対象マシン上でブラウザ拡張機能を使用する予定の**全てのユーザーアカウントでログオンして、ユーザープロファイル毎に拡張機能をインストール**する必要があります。
- オフラインインストールを行った場合、Edgeはブラウザ拡張機能起動時に開発者モードに関する**警告メッセージ**を表示します。プロセス/オブジェクトの処理内で、メッセージを閉じる処理を加える等の対処を行ってください。

対象となるマシンやプロファイルが多数存在し、手動によるオフライン展開作業が困難な場合や、警告メッセージを出さないインストールを行いたい場合には、オフライン環境におけるブラウザ拡張機能の一括展開の仕組みの実装について、Blue Prism Professional Serviceによる有償支援サービスが可能です。お困りの場合にはお問い合わせください。

拡張機能のオフラインインストール手順

Chrome用ブラウザ拡張機能のオフラインパッケージインストール

本手順によるインストールを行う場合、各マシンでブラウザ拡張機能を使用する予定の**全てのユーザーアカウントでログオンして、ユーザープロファイル毎に拡張機能をインストール**する必要があります。

1. Chromeブラウザ拡張機能がインストールされた環境にログオンします。
2. エクスプローラーで拡張機能のファイルを探します。ブラウザ拡張機能のファイルは「C:¥Users¥%Username%¥Appdata¥Local¥Google¥Chrome¥User Data¥Default¥Extensions¥<ブラウザ拡張機能のID>¥<拡張機能のバージョン番号>」に存在します。
※<拡張機能のバージョン番号>に合致するフォルダを探して開きます。
この<拡張機能のバージョン番号>フォルダ内のすべてのファイルを選択し、ZIPファイル圧縮します。（フォルダではなく全てのファイルを選択）
※<ブラウザ拡張機能のID>：本章「ブラウザ拡張機能のID」項を参照のうえ、ブラウザ拡張のID文字列を設定します。
3. 手順2で作成したZIPファイルをブラウザ拡張機能をインストールしたいマシン/ログインユーザー環境からアクセス可能な場所に保存します。
4. ブラウザー拡張機能をインストールしたいマシン/ログインユーザー環境にログインして、Chromeを開きます。
5. メニュー (...) アイコンをクリックし、[設定] > [拡張機能] をクリックします。
「<chrome://extensions>」 に既存の拡張機能が表示されます。
6. デベロッパーモードのスライダーを操作して有効に切り替えます。
7. 手順3で保存した拡張機能のZIPファイルをChromeデベロッパーページにドラッグアンドドロップします。
8. 拡張機能がインストールされ、Chromeデベロッパーページに表示されます。
9. 手順6で有効にしたデベロッパーモードをオフにします。
10. ブラウザー拡張機能を利用するログオンユーザーアカウント（プロファイル）全てについて、手順4～手順9を繰り返します。

拡張機能のオフラインインストール手順

Edgeブラウザ拡張機能のオフラインパッケージインストール

本手順によるインストールを行う場合、各マシンでブラウザ拡張機能を使用する予定の**全てのユーザーアカウントでログオンして、ユーザープロファイル毎に拡張機能をインストール**する必要があります。

1. Edgeブラウザ拡張機能がインストールされた環境にログオンします。
2. エクスプローラーで拡張機能のファイルを探します。ブラウザ拡張機能のファイルは「C:\Users\%Username%\Appdata\Local\Microsoft\Edge\User Data\Default\Extensions \<ブラウザ拡張機能のID>\<Blue Prism拡張機能のバージョン番号>」に存在します。
※<拡張機能のバージョン番号>に合致するフォルダを探して開きます。
この<Blue Prismのバージョン番号>フォルダ内のすべてのファイルを選択し、ZIPファイル圧縮します。（フォルダではなく全てのファイルを選択）
※<ブラウザ拡張機能のID>：本章「ブラウザ拡張機能のID」項を参照のうえ、ブラウザ拡張のID文字列を設定します。
3. 手順2で作成したZIPファイルをブラウザ拡張機能をインストールしたいマシン/ログインユーザー環境からアクセス可能な場所に保存します。
4. ブラウザー拡張機能をインストールしたいマシン/ログインユーザー環境にログインして、Edgeを開きます。
5. メニュー (...) アイコンをクリックし、[拡張機能] > [拡張機能の管理]をクリックします。
「<edge://extensions>」 に既存の拡張機能が表示されます。
6. 画面左側にある開発者モードをスライダーを操作して有効に切り替えます。
7. 手順3で保存した拡張機能のZIPファイルをEdgeの拡張機能ページにドラッグアンドドロップします。
8. 拡張機能がインストールされ、Edgeの拡張機能ページに表示されます。
9. 手順6で有効にした開発者モードをオフにします。
10. ブラウザー拡張機能を利用するログオンユーザーアカウント（プロファイル）全てについて、手順4～手順9を繰り返します。

(参考) BAAの一括展開方法

複数端末への一括インストール

- BAAのインストーラーはMSI (Microsoft Windows Installer) 形式で提供されています。そのため以下のような**Active Directory/Windowsの機能により複数のランタイムリソース端末にBAAをまとめてインストールすることが可能**です。ランタイムリソースの数が多く、BAAの手動展開を行うことが困難な場合には、以下の参照URLやその他の情報を参照し、グループポリシーの仕組み等を理解した上で展開を実施してください。

➤ グループポリシーのスタートアップスクリプトで msiexec コマンドによるインストールを実行

【インストールコマンドの例】 ※Webドライバーもスクリプト内でコピーすると便利です。

```
msiexec /i "<インストーラーの配置フォルダパス> ¥BluePrism.BrowserAutomationAgent_1.0.msi"  
ADDLOCAL=BrowserAutomationAgent,ChromePlugin,EdgePlugin /qn /!*v <インストールログファイルの出カパス>
```

※1行で記載

【参照URL】 <https://learn.microsoft.com/ja-jp/windows-server/administration/windows-commands/msiexec>

➤ Active Directoryのグループポリシーによるソフトウェアのインストール

【参照URL】 <https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>

- ランタイムリソースがインターネット環境に接続可能な場合、BAAをインストールするとBAAに対応したMV3拡張機能がインターネット上のWebストアサイトから自動インストールされますが、Webストアに接続できない**オフライン環境ではブラウザ拡張機能がインストールされません**。

対象となるマシンやプロファイルが多数存在し、手動によるオフライン展開作業が困難な場合や、警告メッセージを出さないインストールを行いたい場合には、オフライン環境におけるブラウザ拡張機能の一括展開の仕組みの実装について、Blue Prism Professional Serviceによる有償支援サービスが可能です。お困りの場合にはお問い合わせください。



5 . APPENDIX

MV3対応 – 関連資料／ツール

※アクセスにはポータルアカウントが必要です

関連資料／ツール名	概要	言語	リンク
KB	Manifest V3導入に関するKnowledge base	日本語	https://help-jp.blueprism.com/1834536112
		英語	https://portal.blueprism.com/customer-support/support-center#/path/-Featured-Articles/1831250872
Manifest V3 Self-Service Portal	Manifest V3導入の概要説明、関連情報へのリンク集	英語	https://community.blueprism.com/manifestv3
コミュニティ	Manifest V3導入に関するコミュニティスレッド	英語	https://community.blueprism.com/communities/community-home/digestviewer/viewthread?MessageKey=eb61f944-a694-4023-9357-eff7425a64ae&CommunityKey=3743dbaa-6766-4a4d-b7ed-9a98b6b1dd01
Manifest V3 Action Guide	ご自身の利用状況（ご利用Ver、VerUp可否、JavaScript(JS)のInsert/Invoke利用有無等）に応じて必要なアクションを提示するWebツール	英語	https://blue-prism.docebosaaS.com/learn/course/19869
Process for Manifest v3 Impact Assessment Utility	Chrome、Edgeを利用しているVBO名、JSのInsert/Invoke利用有無、VBOを利用しているプロセスの一覧等を出力するツール	英語	https://digitalexchange.blueprism.com/dx/entry/3439/solution/manifest-v3-impact-assessment-utility

SS&C Blue Prism Enterprise 脆弱性一覽

脆弱性一覽 1/2

CVEコード	CVSS 3.1	前提条件	概要	影響
CVE-2022-36115	HIGH	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力ユーザーの関与	Blue Prismアプリケーションサーバーを公開するような誤った設定の環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングし、アクセス制御を回避して意図しない機能を実現可能です。	CreateProcessAutosave()メソッドを悪用して、開発プロセスに独自の機能を注入できます。警告を受けたユーザーが、最後に保存されたバージョンを使用して未保存の作業を回復することを決定した場合、悪意のあるコードがワークフローに入り込む可能性。また、公開前にプロセスの動作段階を十分に確認しない場合、悪意のあるコードが本番環境で実行される可能性。
CVE-2022-36116	MEDIUM	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開するような誤った設定の環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングして、setValidationInfo管理機能のアクセス制御を回避することができます。	新しく設計されたプロセスに適用されるバリデーションを削除すると、本番環境で実行される可能性のある悪意のあるコードをうまく隠蔽できる可能性が高まります。
CVE-2022-36117	CRITICAL	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開するような誤った設定の環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングして、管理機能のアクセス制御を回避することが可能です。	クレデンシャルアクセスがマシンまたはランタイムリソースセキュリティグループからアクセスできるように構成されている場合、さらなるリバースエンジニアリングを用いて、攻撃者は既知のマシンになりすまし、既知の暗号化されたクレデンシャルを要求し、後で復号することが可能。
CVE-2022-36118	HIGH	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開する誤った環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングして、SetProcessAttributes管理機能のアクセス制御を回避することが可能です。	この機能を悪用すると、Blue Prismユーザーであれば誰でもプロセスの公開、公開解除、リタイアができるようになります。この機能を使用すると、ログインしているすべてのユーザーがプロセスのステータスを変更できます。

<https://portal.blueprism.com/security-vulnerabilities-august-2022>

SS&C Blue Prism Enterprise 脆弱性一覧

脆弱性一覧 2/2

CVEコード	CVSS 3.1	前提条件	概要	影響
CVE-2022-36119	CRITICAL	<ul style="list-style-type: none">ドメインユーザーアカウントBPコンポーネントへのネットワークアクセスBPのAPサーバ通信チャンネルを標的としたスクリプトを実行する能力	Blue Prismアプリケーションサーバーを公開する誤った設定環境において、ドメイン認証されたユーザーが細工したメッセージをBlue Prismサーバーに送信し、安全でないデシリアライズのために可能なリモートコード実行攻撃を達成できます。	この脆弱性を利用されると、Blue Prism Server サービスのコンテキスト内でコードを実行される可能性があります。
CVE-2022-36120	CRITICAL	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開する誤った環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングし、getChartData管理機能のアクセス制御を回避することが可能です。	低/無権限のBlue Prismユーザーアカウントを使用して、攻撃者はgetChartDataメソッドを悪用してサーバーの設定を変更し、Blue Prismサーバーが名前によって任意のMSSQLストアプロシージャを実行できるようにします。
CVE-2022-36121	HIGH	<ul style="list-style-type: none">BPユーザーアカウントBPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開する誤った環境では、認証されたユーザーがBlue Prismソフトウェアをリバースエンジニアリングし、UpdateOfflineHelpData管理機能のアクセス制御を回避することが可能です。	当該機能を悪用するとBlue PrismユーザーはオフラインヘルプURLを任意のURLに変更することができ、なりすましたヘルプページへ誘導する、ローカルファイルを実行させる、といった操作が可能になります。
CVE-2022-36662	HIGH	<ul style="list-style-type: none">BPコンポーネントへのネットワークアクセスまたはデコンパイル、デバッグツールのインストールと実行能力	Blue Prismアプリケーションサーバーを公開するような誤った設定の環境では、認証されていないユーザーがBlue Prismソフトウェアをリバースエンジニアリングして、GetEncryptionSchemesへのメソッド呼び出しを追加することが可能です。このアクションは、難読化された暗号化キーを含む暗号化スキーム情報を返します。	さらにリバースエンジニアリングにより、メモリから鍵を取り出すことが可能であり、後日、これを利用して機密情報を開示することができます。

<https://portal.blueprism.com/security-vulnerabilities-august-2022>

SS&C Blue Prism のセキュリティリスク軽減対策

1. 基本的なセキュリティ対策

基本的なセキュリティの考え方

基本的な Blue Prism セキュリティは、次の構成を実装することで実現できます。
これは完全なリストではなく、Blue Prism 環境をさらに強化するための追加の構成があることにご注意ください。

- MSSQL データベースで混合モード認証ではなく **Windows 認証**を使用する
※Windows 認証を使用する場合、使用されるすべてのサービス アカウントには、必要最小限の特権が必要です。
- データベースではなく、**アプリケーション サーバーで暗号化キーをホスト**します。
- Blue Prism ネイティブ認証で はなく**SSO 認証を使用**します。(Blue Prism Version 7.1より“二者択一” の考えは非推奨となりました。)
- デジタル ワーカーの認証を構成し、**[匿名のパブリック ランタイム リソースを許可する] を無効**にします。
- **「セキュア」接続モード**のいずれかを使用します。
- Blue Prism 環境に**ファイアウォール**をインストールします。必要なユーザーとアプリケーションのみがファイアウォールを介してアクセスできるようにします。
- **論理アクセス モデル**が制御され、目的に適合していることを確認します。
- 作成されたすべての Blue Prism 認証情報に、実行可能な**最小限のアクセス権**が付与されていることを確認します。
- **ワーク キューを暗号化**します。
- **すべてのコンポーネントを同じ VLAN およびデータ センターでホスト**します。
- 全体として、Blue Prism 環境が安全であることを確認し、**許可されたユーザーのみがハードウェアとアプリケーションにアクセス**できるようにします。

【参照URL】<https://portal.blueprism.com/robotic-operating-model/technology/security>

SS&C Blue Prism のセキュリティリスク軽減対策

2. データベースのセキュリティ対策

データベースのセキュリティの考え方

基本的なデータベース セキュリティは、次の 2 つの簡易的な方法を採用することで実現できます

■ 転送中のデータ

- Blue Prism データベース接続を構成して、**接続を暗号化**する必要があり、さらに検証を行わなくても**サーバー証明書を信頼**できるように指定します。これにより、SQL Server の自己署名証明書を利用できるようになります。これは、「追加の SQL 接続パラメーター」に以下を追加するだけで実行できます。encrypt=true; trustservercertificate=true
- 検証可能なサーバー証明書を SQL Server にインストールし、**すべての接続に対して暗号化を強制**するように SQL インスタンスを構成します。
- 検証可能なサーバー証明書を SQL Server にインストールし、Blue Prism データベース接続を構成して、接続を暗号化する必要があることを指定します。

■ 保存中のデータ

- **透過的なデータ暗号化** (Transparent Data Encryption) 。TDE は SQL データベースに簡単に実装でき、ページが Blue Prism データベースに書き込まれる前に確実に暗号化されます。

【参照URL】 <https://portal.blueprism.com/robotic-operating-model/technology/security>

SS&C Blue Prism のセキュリティリスク軽減対策

3.データ暗号化/ネットワークの保護

データ暗号化

新しい暗号化キーを作成する場合、暗号化方法には 3 つの選択肢があります

- **AES 256 AesCryptoService** (推奨)
- AES 256 RijndaelManaged
- トリプル DES (192 ビット) (非推奨)

Blue prism ネットワークの保護

以下URLに記載の観点でネットワークコネクティビティを適切にセキュリティ保護します

<https://bpdocs.blueprism.com/bp-6-10/ja-jp/Guides/securing-network-connectivity/securing-bp-network-connectivity-overview.htm>

SS&C Blue Prism の不具合

Blue Prism 6.10.5 - 固定拡張ポートの使用に関する問題

ID	BP-11535
確認されたバージョン	Blue Prism 6.10.5
状態	確認済み- 今後のリリースで対応予定
問題	モダンブラウザの自動化を含むプロセスが実行され、Blue Prism でシステム設定の [固定ブラウザの拡張ポート (31924) のみを使用] (Use fixed browser extension port (31924) only) が有効になっている場合、ポート 31924 は割り当てられますが解放されません。これにより、同じマシン上で実行されている Blue Prism の別のインスタンスがポート31924でブラウザ拡張機能と通信することができなくなります。Blue Prism の最初のインスタンスを再起動すると、ポートが解放されます。
回避策	ブラウザの自動化に固定ポートを使用しているランタイム リソースを再起動します。 Process Studio または Control Room でプロセスを実行するときに固定ポートが使用されている場合は、Blue Prism インタラクティブ クライアントを再起動します。 ※発生条件を避ける方法：実行方法を一つとする（本番環境では、スケジュール実行のみとする）
解決方法	次期対策済みパッチバージョンへのバージョンアップ（リリース未定） ※現時点では6.10.6で対応予定

その他の不具合の情報は以下のページおよびページ下部の別バージョンのリンク先を参照してください。

【6.10 known issues】※ページ下部に以前のバージョンのリストへのリンクあり

<https://portal.blueprism.com/customer-support/support-center#/path/Upgrade-Expansion/Upgrade/1579866972/What-are-the-known-issues-in-Blue-Prism-Version-6-10.htm>

【7.1 known issues】※ページ下部に以前のバージョンのリストへのリンクあり

<https://portal.blueprism.com/customer-support/support-center#/path/Upgrade-Expansion/Upgrade/1813008122/What-are-the-known-issues-in-Blue-Prism-Version-7-1-releases.htm>

SS&C | blueprism[®]