No.	ご質問内容	弊社回答
1	JavaScriptの挿入/呼び出し機能を全く使っておらず、今後も使用しないという場合は、今回の対応は必要ないという認識で間違いないでしょうか。	JavaScriptの機能を利用しない場合、現在ご利用のバージョンが既に6.10.5かつブラウザ拡張機能がMV3版になっている、または7.1.XであればMV3対応は必要ありませんが、それ以外のケースではBAAを導入し、ブラウザ拡張機能をMV2版からMV3版に入れ替える必要があります。
2	６．Xと７．XだとBPと拡張機能の通信方法が大きく変わっていますが、なにかMV3に影響がありますか？	それぞれの通信方式にあわせてMV3拡張機能を開発、リリースしていますので、基本的には影響はありませんが 既知の不具合の情報をあらかじめ確認の上、MV3移行を行ってください。
4	ブラウザモードのスパイ要素についてEdgeの設定で「スタートアップブースト」を無効にすることによってアタッチがうまくいかずスパイ要素をハイライト出来ない障害や事象は過去に存在したことはあるか？	「スタートアップブースト」が有効な場合に、アタッチがうまくいかずスパイ要素をハイライト出来ない事象が発生した例が過去にあります。逆に無効化した場合にそれが原因でアタッチ、スパイ動作に問題が発生したという事例は確認されておりません。
5	Q.現状のStableなChromeはMV2とMV3が両方使えるようになっている、2023/6以降（延長しない場合）MV2が使えない設定になるという認識で正しいか？	現在のスケジュールとしてはご認識の通りです。2023/6以降のどこかでMV2が使えなくなるものとして、MV2の使用期限延長、MV3対応を実施いただくことを強く推奨します。
6	BPCユーザーにも配慮した内容だとよりありがたいです	BPCについてもBluePrismEnterpriseを使用していますので、基本的な対応方法は同様になります。 環境面でのご不明点等がございましたらBPCバージョンアップ時のBPC担当とのやり取りの中でご確認いただきますようお願いいたします。
7	現在edgeのバージョンが101です。極端な話で2023年5月末～12月末にバージョン101のままでも、enterprise policyによる延長必要でしょうか？ 2024年1月にはedgeのバージョン関係なく全てのMV2拡張機能が使えなくなるのでしょうか？	Chromeでは6 月以降に115以降のバージョンで MV2の実行を無効化する旨の発表がされています。但し、Microsoft社がMV2を無効化する際のバージョンや実装詳細が不明なことや、不意のバージョンアップ等によるトラブル防止等を考慮すると、念のためEnterprise Policyの適用確認作業と設定により、MV2の使用期間延長を実施いただくことを推奨いたします。
8	BluePrism 6.10.4から6.10.5にアップグレードした際に必要な注意事項	BluePrism 6.10.4から6.10.5にアップグレードした場合に、通常MV2のプラグイン(6.10.4)が引き継がれます。 Webinar資料のP41-42の作業により6.10.5のMV3拡張機能に変更するか、BAAをインストールしてMV3対応を行ってください。また、P54記載の6.10.5固有の不具合やその他の既知の不具合に自社の運用環境が抵触しないかどうかをご確認の上、アップグレードを実施してください。
9	セキュリティリスク軽減対策が必須なのかどうか分かりませんでした。 それぞれの構成が本番運用中のBluePrismで適用できるのか、それともバージョンアップのタイミングで実施すべき内容なのかが分かりませんでした。	今回の既知の脆弱性への対策としてはパッチ適用により既知の脆弱性への直接的な対策ができるため、パッチ適用を行う場合にはセキュリティリスク軽減対策は必須ではありません。 ただし、セキュリティリスク軽減対策はそもそもBlue Prismが推奨するセキュアなBlue Prism環境を構築するという観点や今後新たな脆弱性が判明した場合にパッチ適用までのセキュリティ強化対策としては、有効な対策ということになりますので、その観点でも適用するかどうかをご検討ください。 また、セキュリティリスク軽減対策とパッチ適用のいずれもいきなり本番運用中のBlue Prismへの適用は推奨されません。どちらも開発、検証環境に適用、動作確認を行った上での本番適用が必要となります。 セキュリティリスク軽減対策の実施タイミングとして、影響や作業負荷を考慮するとパッチ適用やその他のメジャー/マイナーバージョンアップのタイミングで作業を実施いただくのが効率は良いといえますが、自社のセキュリティポリシーや運用の状態によっては早く対策をいただくほうが良い場合もありますので、Webinar資料や参照リンク先の脆弱性の内容から適宜判断をいただく必要があります。