PRIMEQUEST シリーズ
各コンソール機能の Web ブラウザ動作確認情報

2025 年 2 月 27 日更新

【はじめに】

PRIMEQUEST シリーズにおける以下の各コンソール機能と Web ブラウザとの動作確認情報を掲載します。

- MMB Web-UI
- MMB Web-UI と OSIV/XSP 動作機構(SVP コンソール)の組み合わせ
- MMB Web-UI と ASP 動作機構(ASP 動作機構マネージャー)の組み合わせ

Internet Explorer 11 のサポートは、2022 年 6 月 16 日に終了となりました。これに伴い、Internet Explorer 11 を使用した MMB Web-UI の動作についてはサポート対象外になりますのでご了承ください。
Windows® 10 のサポートは、2025 年 10 月 14 日に終了となります。これに伴い、Windows® 10 での MMB Web-UI の動作についてはサポート対象外になりますのでご了承ください。

【OS エディションについて】

使用できる OS のエディションは、以下のとおりです。

OS	エディション	備考
Windows® 10	Pro	Windows® 10 のサポートは、 2025 年 10 月 14 日に終了予定です。
	Enterprise	
Windows® 11	Pro	ー
	Enterprise	ー
Linux(64bit 版)	ー	CentOS7(64bit 版)で動作検証を実施しています。

【各コンソール操作における注意事項】

各コンソール機能を操作する際の注意事項は以下のとおりです。各コンソール機能を操作する前に以下の注意事項を確認してから操作を開始してください。

◆ MMB Web-UI の操作の注意事項

- MMB Web-UI の System Event Log 画面、Operation Log 画面の横スクロールで表の表題部分が追随しないため、Web ブラウザの横幅を広げてスクロールしないでください。
- 1 台の MMB 接続用 PC から、1 台の PRIMEQUEST シリーズに MMB Web-UI を使って複数ログインしないでください（同一ユーザー名で複数ログインする場合も含む）。操作する Web ブラウザの種類やバージョンにもよりますが、複数ログインした場合は以下の現象が起こる場合があります。また、複数タブから複数ログインしないでください。
  - 先に MMB Web-UI でログインしているユーザーの操作権限が、後からログインしたユーザーの操作権限に変わることがあります。
  - 1 つの MMB Web-UI のログアウトですべての MMB Web-UI がログアウトしてしまうことがあります。
- https で接続すると、証明書が「自己発行証明書」の場合、警告メッセージが表示されますが、そのまま接続を続行してください。

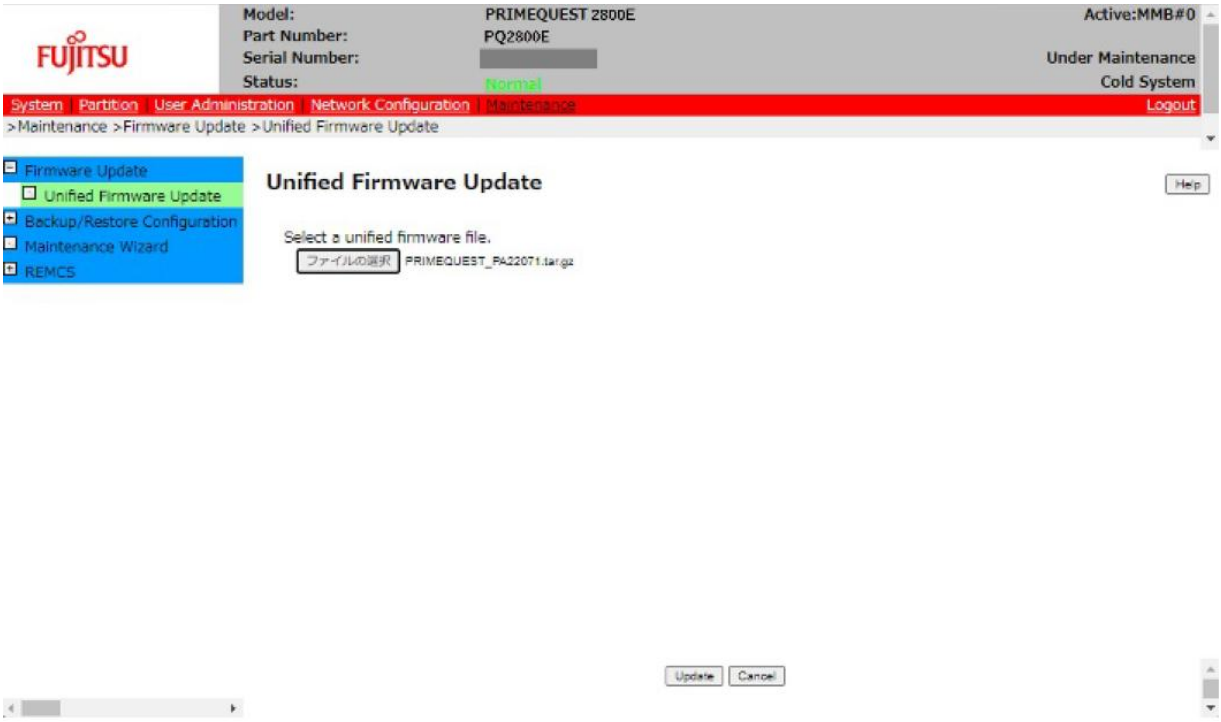
- 統合版数 SA16061/SB16061 以前の PRIMEQUEST 1000 シリーズにおいて MMB Web-UI に https 接続し、かつ、マイクロソフト社のルート証明書プログラムに参加している証明機関から発行され証明書で暗号化アルゴリズムとして SHA-1 を使用している場合、警告メッセージが表示されますが、そのまま接続を続行してください。
- MMB Web-UI で、処理の実行確認、処理完了の通知などのダイアログボックスが表示された状態で 2 分以上経過すると、MMB Web-UI との接続が切断されます。この場合は、再度 MMB Web-UI にログインしてください。
- PRIMEQUEST 3000 シリーズにおいて MMB Web-UI の System > System Information 画面の Asset Tag に全角文字を設定しないでください。
- Web ブラウザによっては、MMB Web-UI が表示する確認ダイアログ等に「追加のダイアログ表示を抑止する」旨のチェックボックスが表示されることがあります。以降の操作を行えなくなることがあるため、抑止しないでください。
- TLS1.2 をサポートしているファームウェア版数は以下になります。

シリーズ名	サポート版数	TLS1.0/1.1 有効無効設定
PRIMEQUEST 1000 シリーズ	SA16111/SB16111 版以降	無し
PRIMEQUEST 2000 シリーズ	BA17034/BB17034/BC17034 版	無し
	BA17072/BB17072/BC17072 版以降	有り
PRIMEQUEST 3000 シリーズ	全版数	無し

PRIMEQUEST 2000 シリーズにおける、BA17072/BB17072/BC17072 版以降のファームウェアには、TLS1.0/1.1 の有効無効を切り替える機能があります。
ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

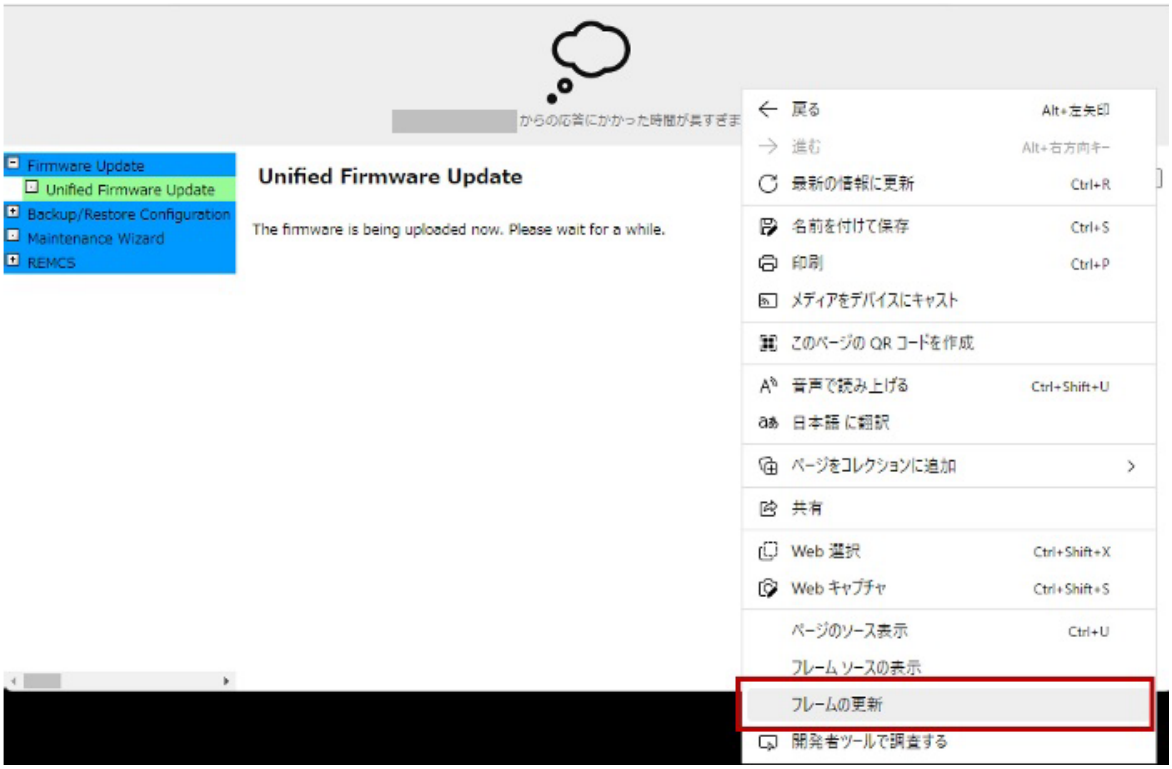
TLS 1.2 のサポート有無により、MMB Web-UI への https 接続設定が異なります。詳細は、本ドキュメント内の【各コンソールにおける設定事項】をご確認ください。

- MMB Web-UI での、統合ファームアップにおいて、
  https 接続で統合ファームウェアを選択し、アップデートを開始すると、ファイルのアップロードでタイムアウトが発生、Information 領域がグレーになり、「応答時間が長すぎる」旨のメッセージを表示、さらに Web-UI からログアウトされることがあります。
  二通りの回避手段があります。
  http 接続が利用可能な場合
  http 接続でファームウェアアップデートを実行してください。
  http 接続が利用不可能な場合
  https 接続で以下の手順を実施してください。
  1. >Maintenance >Firmware Update >Unified Firmware Update 画面で、統合ファームウェアを選択し、Update ボタンをクリックします。

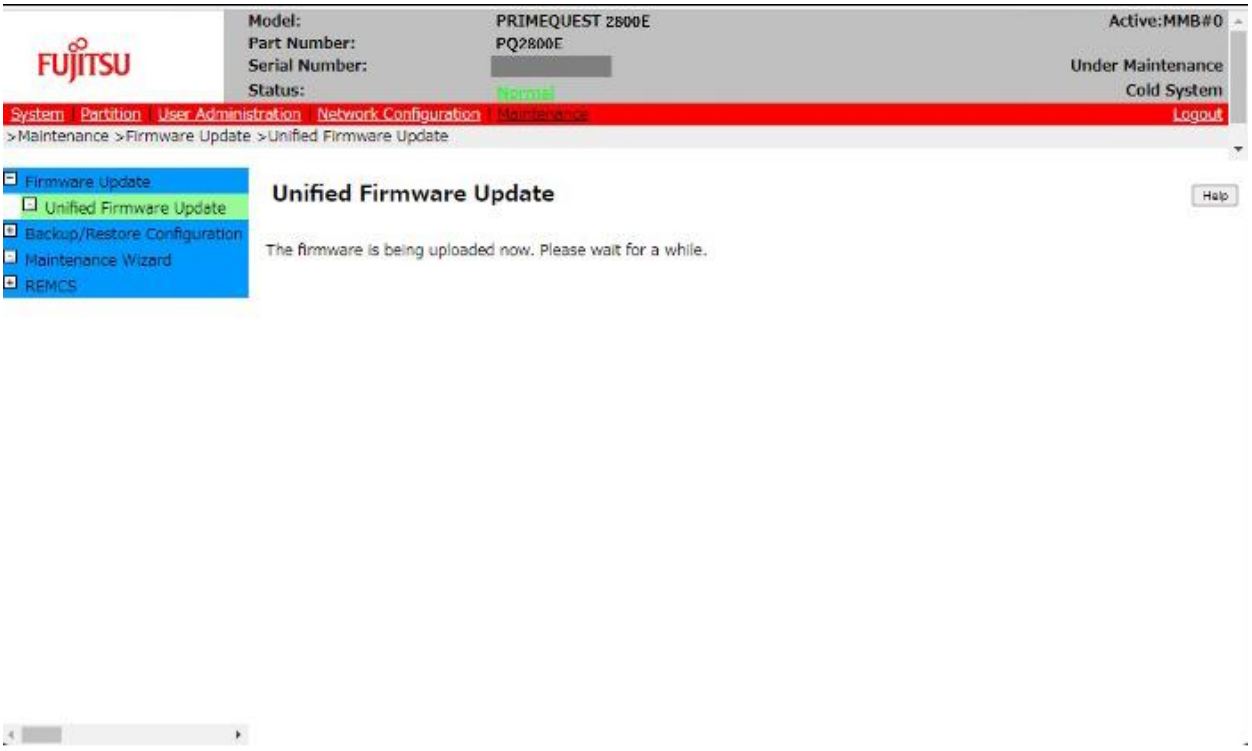


2.Update ボタンをクリック後、画面上部の Information 領域にカーソルを合わせます。

3.以下の画面のように、Information 領域に「<IP Address>からの応答にかかった時間が長すぎます」とメッセージが表示された場合、90 秒以内に画面上の Information 領域で右クリックを行い、「フレームの更新」をクリックします。



4.以下の画面に戻り、統合ファームアップデートを継続します。



◆ SVP コンソールの操作の注意事項

- SVP コンソールからログアウトする場合は、すぐに Web ブラウザを閉じずに、[Logout]ボタンをクリックしてログアウトしてから閉じてください。
- ログイン中の SVP コンソールで、Web ブラウザの[戻る]、[進む]などのボタンは操作しないでください。
- ログイン中の SVP コンソールで、Web ブラウザに表示されている現在のページを更新する以下の操作は、実行しないでください。
  – [F5]キー
  – [Ctrl]+[F5]キー
  – [Shift]+[F10]キーまたは右マウスボタンをクリックして、[最新の情報に更新]
- SVP コンソールにログインする場合、直接「http://XSP パーティションの IP アドレス/login.cgi」に接続しないでください。なお、SVP コンソールを Web ブラウザのお気に入りに追加する場合、「/login.cgi」を削除して登録してください。
- 単一の PC 共用コンソール上で、2 つ以上の Web ブラウザを使用する場合、それぞれ異なる利用者で、SVP コンソールにログインしないでください。
- 単一の PC 共用コンソール上で、2 つ以上の Web ブラウザを開き、そのうちの 1 つで、SVP コンソールにログインしてから[Logout]ボタンをクリックせずに、Web ブラウザを閉じないでください。
- ポップアップ画面が表示された状態で放置しないでください。
- Backup 機能によるファイルのダウンロード中は、SVP コンソールを操作しないでください。ダウンロード中は、通知バーによるファイルダウンロードの進行度表示が行われます。この際、[ダウンロードが完了しました。]と表示されるまで、SVP コンソールを操作しないでください。

◆ ASP 動作機構マネージャーの操作の注意事項

- 同一端末で Internet Explorer の複数のウィンドウを使って異なるユーザーでログインする場合は、次の手順で新規 Web ブラウザを起動してログイン操作を実施します。
  1. Internet Explorer の[ファイル(F)]→[新規セッション(I)]をクリックします。
- Internet Explorer の設定がタブブラウザの場合、サブ画面、および確認ダイアログが表示されているときは、他のタブへの移動ができません。
- PRIMEQUEST1000 シリーズで Internet Explorer を使う場合、「一括マイグレーションの実行」画面において、[マイグレーション先 ASP 動作機構ファーム名(必須)]の選択項目の表示位置がずれますが、操作上の問題はありません。
- PRIMEQUEST1000 シリーズで Internet Explorer を使う場合、「ASP 動作機構ファーム管理」画面において、[ASP 動作機構ファームの登録]ボタンの「録」の部分が欠けて表示されますが、操作上の問題はありません。

【各コンソールにおける設定事項】

使用する OS と Web ブラウザの組み合わせによっては、各コンソール機能の操作を行う前に事前設定が必要な組み合わせがあります。以下に PRIMEQUEST シリーズ毎に OS と Web ブラウザの組み合わせにおける動作確認情報の一覧を示します。この一覧の中で「※x」(x は追番)の記載がある組み合わせについては、事前設定が必要になりますので、各コンソール機能の操作を開始する前に該当する番号に記載されている全ての項目の設定を行ってから、各コンソール機能の操作を開始してください。

凡例　〇 ： 検証済
　　－ ： 検証対象外（白色）
　　－ ： 製品未提供（灰色網かけ）

全てのコンソール機能が未サポートの OS と Web ブラウザの組み合わせについては記載しておりません。
コンソール機能の動作検証は、最新版ファームと、最新版ブラウザの組み合わせで実施しております。そのため、新しい版数のブラウザを使用することを推奨します。

PRIMEQUEST1000 シリーズの場合]

OS	Web ブラウザ	MMB Web-UI	MMB Web-UI + OSIV/XSP 動作機構	MMB Web-UI + ASP 動作機構
Windows 10 (32bit 版)(注 7)	Internet Explorer 11(注 6)	〇 ※2	〇※4	〇(注 2) ※7
	Firefox	〇 ※11	－	－
Windows 10 (64bit 版)(注 7)	Internet Explorer 11(注 6)	〇(注 1) ※2	〇※4	〇(注 2) ※7
	Firefox	〇 ※11	－	－
Windows 11	Firefox	〇 ※11	－	－
	Microsoft Edge	－	－	〇 ※21

[PRIMEQUEST2000 シリーズの場合]

OS	Web ブラウザ	MMB Web-UI	MMB Web-UI + OSIV/XSP 動作機構	MMB Web-UI + ASP 動作機構
Windows 10 (32bit 版)(注 7)	Internet Explorer 11(注 6)	○ ※1	○※6	○(注 2) ※15
	Firefox	○ ※12	―	―
	Chrome	○ ※13	―	―
	Microsoft Edge	○ ※16	△(注 4)	○ ※21
Windows 10 (64bit 版)(注 7)	Internet Explorer 11(注 6)	○(注 1) ※1	○※6	○ ※15
	Firefox	○ ※12	―	―
	Chrome	○ ※13	―	―
	Microsoft Edge	○ ※16	△(注 4)	○ ※21
Windows 11	Firefox	○ ※12	―	―
	Chrome	○ ※13	―	―
	Microsoft Edge	○ ※16	△(注 4)	○ ※21
Linux(64bit 版)	Firefox	○ ※12	―	―

[PRIMEQUEST3000 シリーズの場合]

OS	Web ブラウザ	MMB Web-UI	MMB Web-UI + OSIV/XSP 動作機構	MMB Web-UI + ASP 動作機構
Windows 10 (32bit 版)(注 7)	Internet Explorer 11(注 6)	○ ※9	○(注 3) ※18	―
	Firefox	○	―	―
	Chrome	○ ※14	―	―
	Microsoft Edge	○※20	○(注 5) ※19	―
Windows 10 (64bit 版)(注 7)	Internet Explorer 11(注 6)	○(注 1) ※9	○(注 3) ※18	―
	Firefox	○	―	―
	Chrome	○ ※14	―	―
	Microsoft Edge	○※20	○(注 5) ※19	―
Windows 11	Firefox	○	―	―
	Chrome	○ ※14	―	―
	Microsoft Edge	○※20	○(注 5) ※19	―
Linux(64bit 版)	Firefox	○	―	―

【注意事項】

注1. Internet Explorer 32bit 版のみ使用できます。

注2. MMB Web-UI は検証対象外です。

注3. PRIMEQUEST3000 シリーズの Type2 でサポートしています。

注4. PRIMEQUEST2000 シリーズの Type3 のみ個別対応でサポートします。Microsoft Edge の使用には制限事項があるため、使用を希望する場合は下記の専用窓口までご連絡ください。
fj-pxm-edge-support@dl.jp.fujitsu.com

注5. また、SVP コンソールはバージョン 94 以降の利用を推奨します。それ以前のバージョンにおいてはエンタープライズサイトリストマネージャーが使用できない場合があるため、その場合は Microsoft Edge のバージョンアップ、または注 4 の専用窓口までご相談ください。

注6. Internet Explorer 11 のサポートは、2022 年 6 月 16 日に終了となりました。これに伴い、Internet Explorer 11 を使用した MMB Web-UI の動作についてはサポート対象外になりますのでご了承ください。

注7. Windows® 10 のサポートは、2025 年 10 月 14 日に終了となります。これに伴い、Windows® 10 での MMB Web-UI の動作についてはサポート対象外になりますのでご了承ください。

※1. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI にログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定2. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

- 統合ファームウェア版数がTLS1.2サポート版の場合。(BA17034/BB17034/BC17034以降)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

  さらに TLS1.0/1.1 有効無効の設定が可能な場合。(BA17072/BB17072/BC17072 以降)

  TLS1.0/1.1 を有効にして、https 接続を行う場合

  1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をEnableに設定する。

     https接続可能な場合、以下の手順は不要です。
  2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  3. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  4. [OK]ボタンをクリックします。

     ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

  TLS1.0/1.1 を無効に、TLS1.2 を有効にして、https 接続を行う場合

  1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をDisableに設定する。

     https接続可能な場合、以下の手順は不要です。
  2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  3. [セキュリティ]項目の[TLS1.2を使用する]にチェックを入れます。

4. [OK]ボタンをクリックします。

※2. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI にログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定2. https接続時、次の操作を行う場合は、以下の設定を行ってください。

ただし、SA/SB14092以降の本体ファームウェアが適応されている場合は設定不要です。

- Network Configuration -> Network Interface -> Dualization の操作
- Network Configuration >SNMP Configuration の SNMP Community の操作
- Network Configuration >Remote Server Management の操作
- Network Configuration >Network Interface MMB#1 IP Address Disable の操作
- System >System Event Log の System Event Log Filtering Condition の操作
- System >System Setup の操作
- Maintenance >Maintenance Wizard でEnter Maintenance の操作
- Maintenance > Backup/Restore Configuration > Backup/Restore MMB Configuration のRestore MMB Configuration の操作
- Maintenance >Backup/Restore Configuration のRestore BIOS Configuration の操作
- ファームアップの操作

1. 上記操作を実施する時はhttp接続で実施し、実施後https接続に戻す。

設定3. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(SA16111/SB16111以降)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、[TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※3. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI、SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)と SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定2. https接続時、MMB Web-UIで次の操作を行う場合は、以下の設定を行ってください。
ただし、SA/SB14092以降の本体ファームウェアが適応されている場合は設定不要です。

- Network Configuration -> Network Interface -> Dualization の操作
- Network Configuration >SNMP Configuration の SNMP Community の操作
- Network Configuration >Remote Server Management の操作
- Network Configuration >Network Interface MMB#1 IP Address Disable の操作
- System >System Event Log の System Event Log Filtering Condition の操作
- System >System Setup の操作
- Maintenance >Maintenance Wizard でEnter Maintenance の操作
- Maintenance > Backup/Restore Configuration > Backup/Restore MMB Configuration のRestore MMB Configuration の操作
- Maintenance >Backup/Restore Configuration のRestore BIOS Configuration の操作
- ファームアップの操作

1. 上記操作を実施する時はhttp接続で実施し、実施後https接続に戻す。

設定 3. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 4. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックしま

す。

4. [OK]ボタンをクリックします。

設定 5. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無効にする]をチェックします
4. [OK]ボタンをクリックします。

設定 7. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェッ クを外します。
3. [OK]ボタンをクリックします。

設定 8. 以下の方法で信頼済みサイトに SVP コンソールの URL を登録します

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[信頼済みサイト]を選択し、[保護モードを有効にする(Internet Explorer の再起動が必要)(P)]のチェックが付いている場合は外し、[サイト]ボタンをクリックします。
3. [信頼済みサイト]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする(S)]のチェックを外し、[この Web サイトをゾーンに追加する(D)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定9. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(SA16111/SB16111以降)

https接続可能な場合、以下の手順は不要です。

1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、[TLS1.2を使用する]のいずれかにチェックを入れます。
3. [OK]ボタンをクリックします。

ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※4. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI、SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)と SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定2. https接続時、MMB Web-UIで次の操作を行う場合は、以下の設定を行ってください。
ただし、SA/SB14092以降の本体ファームウェアが適応されている場合は設定不要です。

- Network Configuration -> Network Interface -> Dualization の操作
- Network Configuration >SNMP Configuration の SNMP Community の操作
- Network Configuration >Remote Server Management の操作
- Network Configuration >Network Interface MMB#1 IP Address Disable の操作
- System >System Event Log の System Event Log Filtering Condition の操作
- System >System Setup の操作
- Maintenance >Maintenance Wizard でEnter Maintenance の操作
- Maintenance > Backup/Restore Configuration > Backup/Restore MMB Configuration のRestore MMB Configuration の操作
- Maintenance >Backup/Restore Configuration のRestore BIOS Configuration の操作
- ファームアップの操作

1. 上記操作を実施する時はhttp接続で実施し、実施後https接続に戻す。

設定 3. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 4. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。
4. [OK]ボタンをクリックします。

設定 5. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無効にする]をチェックします
4. [OK]ボタンをクリックします。

設定 7. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 8. 以下の方法でローカルイントラネットに SVP コンソールの URL を登録します

1. SVP コンソールのログイン画面を表示します。
2. ブラウザの[ツール]-[インターネットオプション]の[セキュリティ]タブを開きます。
3. ゾーンとして「ローカルイントラネット」が選択されており、[保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが外れていることを確認してくだい。
   [保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが付いている場合はチェックを外してください。
   「ローカルイントラネット」が選択されていない場合、以下の手順で SVP コンソールの URL を「ローカルイントラネット」に登録します。
4. [セキュリティ]タブで[ローカルイントラネット]を選択し、[サイト]をクリックします。
5. [詳細設定]をクリックします。

6. [ローカルイントラネット]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする]のチェックが外れていることを確認し、[この Web サイトをゾーンに追加する]に URL(http://XSP パーティションの IP アドレス/)を入力し[追加]をクリックします。

設定 9. 以下の方法で 2016 年 1 月以降に配信された Windows Update を適用してください。

1. Windows の[設定]-[更新とセキュリティ]の[Windows Update]を選択します。
2. [更新プログラムのチェック]ボタンをクリックします。
3. 利用可能な更新プログラムが検出されたら[インストール]ボタンをクリックします。
4. [今すぐ再起動]ボタンが表示されたら、[今すぐ再起動]ボタンをクリックします。 (この際、コンピューターが自動的に再起動します)。
   [今すぐ再起動] ボタンが表示されなければ、Windows Update の画面を閉じて終了します。

設定10. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(SA16111/SB16111以降)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※5. 以下の設定を行ってください。

設定 1. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 2. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。

2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。
4. [OK]ボタンをクリックします。

設定 3. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 4. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無 効にする]をチェックします
4. [OK] ボタンをクリックします。

設定 5. 以下の操作で互換表示の有効設定をしてから SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます。
2. [互換表示設定]画面の[追加する Web サイト]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 7. 以下の方法で信頼済みサイトに SVP コンソールの URL を登録します

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[信頼済みサイト]を選択し、[保護モードを有効にする(Internet Explorer の再起動が必要)(P)]のチェックが付いている場合は外し、[サイト]ボタンをクリックします。
3. [信頼済みサイト]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする(S)]のチェックを外し、[この Web サイトをゾーンに追加する(D)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定8. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(BA17034/BB17034/BC17034以降)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。
  さらに TLS1.0/1.1 有効無効の設定が可能な場合。(BA17072/BB17072/BC17072 以降)

  TLS1.0/1.1 を有効にして、https 接続を行う場合
  1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をEnableに設定する。
     https接続可能な場合、以下の手順は不要です。
  2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  3. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  4. [OK]ボタンをクリックします。
     ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

  TLS1.0/1.1 を無効に、TLS1.2 を有効にして、https 接続を行う場合
  1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をDisableに設定する。
     https接続可能な場合、以下の手順は不要です。
  2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  3. [セキュリティ]項目の[TLS1.2を使用する]にチェックを入れます。
  4. [OK]ボタンをクリックします。

※6. 以下の設定を行ってください。

設定 1. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。

4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 2. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。
4. [OK]ボタンをクリックします。

設定 3. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 4. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無 効にする]をチェックします
4. [OK] ボタンをクリックします。

設定 5. 以下の操作で互換表示の有効設定をしてから SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます。
2. [互換表示設定]画面の[追加する Web サイト]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 7. 以下の方法でローカルイントラネットに SVP コンソールの URL を登録します

1. SVP コンソールのログイン画面を表示します。
2. ブラウザの[ツール]-[インターネットオプション]の[セキュリティ]タブを開きます。
3. ゾーンとして「ローカルイントラネット」が選択されており、[保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが外れていることを確認してくだい。
   [保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが付いている場合はチェックを外してください。
   「ローカルイントラネット」が選択されていない場合、以下の手順で SVP コンソールの URL を「ローカルイントラネット」に登録します。
4. [セキュリティ]タブで[ローカルイントラネット]を選択し、[サイト]をクリックします。
5. [詳細設定]をクリックします。
6. [ローカルイントラネット]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする]のチェックが外れていることを確認し、[この Web サイトをゾーンに追加する]に URL(http://XSP パーティションの IP アドレス/)を入力し[追加]をクリックします。

設定 8. 以下の方法で 2016 年 1 月以降に配信された Windows Update を適用してください。

1. Windows の[設定]-[更新とセキュリティ]の[Windows Update]を選択します。
2. [更新プログラムのチェック]ボタンをクリックします。
3. 利用可能な更新プログラムが検出されたら[インストール]ボタンをクリックします。
4. [今すぐ再起動]ボタンが表示されたら、[今すぐ再起動]ボタンをクリックします。 (この際、コンピューターが自動的に再起動します)。
   [今すぐ再起動] ボタンが表示されなければ、Windows Update の画面を閉じて終了します。

設定9. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(BA17034/BB17034/BC17034以降)
  https接続可能な場合、以下の手順は不要です。
  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。
  さらに TLS1.0/1.1 有効無効の設定が可能な場合。(BA17072/BB17072/BC17072 以降)
  TLS1.0/1.1 を有効にして、https 接続を行う場合
  1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) -

TLS1.0/1.1をEnableに設定する。

https接続可能な場合、以下の手順は不要です。

2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
3. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
4. [OK]ボタンをクリックします。

ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

TLS1.0/1.1 を無効に、TLS1.2 を有効にして、https 接続を行う場合

1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をDisableに設定する。

https接続可能な場合、以下の手順は不要です。

2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
3. [セキュリティ]項目の[TLS1.2を使用する]にチェックを入れます。
4. [OK]ボタンをクリックします。

※7. 以下の設定を行ってください。

設定1. 以下の方法でセキュリティゾーンを[ローカル イントラネット]に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[サイト(S)]ボタンをクリックします。
3. [ローカル イントラネット]画面の[詳細設定(A)]ボタンをクリックします。
4. [この Web サイトをゾーンに追加する]ボックスに、ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL アドレス（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。
5. [閉じる(C)]ボタンをクリックします。

設定2. 以下の方法でJavaScriptを有効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[アクティブスクリプト]の[有効にする]を選択します。
4. [OK]ボタンをクリックします。

設定3. 以下の方法でポップアップブロックを解除してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス]に ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。

4. [閉じる(C)]ボタンをクリックします。

設定4. 以下の方法で拡張保護モードを無効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [拡張保護モードを有効にする]のチェックを外します。
3. [OK]ボタンをクリックします。

設定5. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。
- 統合ファームウェア版数がTLS1.2サポート版の場合。(SA16111/SB16111以降)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、[TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※8. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI にログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定2. https 接続時、次の操作を行う場合は、以下の設定を行ってください。

ただし、SA/SB14092以降の本体ファームウェアが適応されている場合は設定不要です。

- Network Configuration -> Network Interface -> Dualization の操作
- Network Configuration >SNMP Configuration の SNMP Community の操作
- Network Configuration >Remote Server Management の操作
- Network Configuration >Network Interface MMB#1 IP Address Disable の操作
- System >System Event Log の System Event Log Filtering Condition の操作
- System >System Setup の操作
- Maintenance >Maintenance Wizard でEnter Maintenance の操作
- Maintenance > Backup/Restore Configuration > Backup/Restore MMB Configuration のRestore MMB Configuration の操作

- Maintenance >Backup/Restore Configuration のRestore BIOS Configuration の操作
- ファームアップの操作

1. 上記操作を実施する時はhttp 接続で実施し、実施後https 接続に戻す。

設定3. 以下の方法でセキュリティゾーンを[ローカル イントラネット]に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[サイト(S)]ボタンをクリックします。
3. [ローカル イントラネット]画面の[詳細設定(A)]ボタンをクリックします。
4. [この Web サイトをゾーンに追加する]ボックスに、ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL アドレス（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。
5. [閉じる(C)]ボタンをクリックします。

設定4. 以下の方法でJavaScriptを有効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[アクティブスクリプト]の[有効にする]を選択します。
4. [OK]ボタンをクリックします。

設定5. 以下の方法でポップアップブロックを解除してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス]に ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定6. 以下の方法で拡張保護モードを無効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [拡張保護モードを有効にする]のチェックを外します。
3. [OK]ボタンをクリックします。

設定7. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。

3. [OK]ボタンをクリックします。

ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

- 統合ファームウェア版数がTLS1.2サポート版の場合。(SA16111/SB16111以降)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、[TLS1.2を使用する]のいずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※9. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI にログインします。

1. Internet Explorer の[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

※10. 以下の設定を行ってください。

設定 1. 以下の操作で互換表示の有効設定をしてから MMB Web-UI にログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます
2. [互換表示設定]画面の[追加する Web サイト]に MMB Web-UI の URL(http://MMB 仮想 IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

※11. 以下の設定を行ってください。

設定1. https接続時、次の操作を行う場合は、以下の設定を行ってください。

ただし、SA/SB14092以降の本体ファームウェアが適応されている場合は設定不要です。

- Network Configuration -> Network Interface -> Dualization の操作
- Network Configuration >SNMP Configuration の SNMP Community の操作
- Network Configuration >Remote Server Management の操作
- Network Configuration >Network Interface MMB#1 IP Address Disable の操作
- System >System Event Log の System Event Log Filtering Condition の操作
- System >System Setup の操作
- Maintenance >Maintenance Wizard でEnter Maintenance の操作
- Maintenance > Backup/Restore Configuration > Backup/Restore MMB Configuration のRestore MMB Configuration の操作
- Maintenance >Backup/Restore Configuration のRestore BIOS Configuration の操作
- ファームアップの操作

1. 上記操作を実施する時はhttp接続で実施し、実施後https接続に戻す。

設定2. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(SA16061/SB16061以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの「TLS1.0とTLS1.1を有効にする」ボタンをクリックします。

  上記ボタンが表示されない場合

  1. WebブラウザのURLに「about:config」を入力します。
  2. security.tls.version.minに"1"を設定します。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

※12. 以下の設定を行ってください。

設定1. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの「TLS1.0とTLS1.1を有効にする」ボタンをクリックします。

  上記ボタンが表示されない場合

  1. WebブラウザのURLに「about:config」を入力します。
  2. security.tls.version.minに"1"を設定します。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

※13. 以下の設定を行ってください。

設定 1. 以下の操作で Chrome のフォントサイズを「小」に変更します。

1. Web ブラウザの[設定]を選択します。
2. デザインの[フォントサイズ]を「小」に変更します。
3. 「設定」タブを閉じます。

設定2. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)

  https接続可能な場合、以下の手順は不要です。

  1. Webブラウザの[設定]を選択します。
  2. 詳細設定を選択します。
  3. システム内の[プロキシ設定を開く]を選択します。
  4. [詳細設定]タブで、[セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
  5. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

※14. 以下の設定を行ってください。

設定 1. 以下の操作で Chrome のフォントサイズを「小」に変更します。

1. Web ブラウザの[設定]を選択します。
2. デザインの[フォントサイズ]を「小」に変更します。
3. 「設定」タブを閉じます。

※15. 以下の設定を行ってください。

設定1. 以下の方法でセキュリティゾーンを[ローカル イントラネット]に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[サイト(S)]ボタンをクリックします。
3. [ローカル イントラネット]画面の[詳細設定(A)]ボタンをクリックします。
4. [この Web サイトをゾーンに追加する]ボックスに、ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL アドレス（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。
5. [閉じる(C)]ボタンをクリックします。

設定2. 以下の方法でJavaScriptを有効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[ローカル イントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[アクティブスクリプト]の[有効にする]を選択します。
4. [OK]ボタンをクリックします。

設定3. 以下の方法でポップアップブロックを解除してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス]に ASP 動作機構マネージャーをインストールした管理用 PC サーバの URL（http://管理用 PC サーバのドメイン名または IP アドレス/）を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定4. 以下の方法で拡張保護モードを無効に設定してください。

1. Internet Explorer の[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [拡張保護モードを有効にする]のチェックを外します。
3. [OK]ボタンをクリックします。

設定5. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。（BA17031/BB17031/BC17031以前）

https接続可能な場合、以下の手順は不要です。

1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[TLS1.0を使用する]のチェックを入れます。
3. [OK]ボタンをクリックします。

ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

- 統合ファームウェア版数がTLS1.2サポート版の場合。(BA17034/BB17034/BC17034以降)

https接続可能な場合、以下の手順は不要です。

1. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
3. [OK]ボタンをクリックします。

ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

さらに TLS1.0/1.1 有効無効の設定が可能な場合。(BA17072/BB17072/BC17072 以降)

TLS1.0/1.1 を有効にして、https 接続を行う場合

1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をEnableに設定する。
   https接続可能な場合、以下の手順は不要です。
2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
3. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]のいずれかにチェックを入れます。
4. [OK]ボタンをクリックします。
   ただし、TLS1.0/1.1はサポート終了しており、TLS1.0/1.1の有効時の動作はサポートしません。

TLS1.0/1.1 を無効に、TLS1.2 を有効にして、https 接続を行う場合

1. MMB Web-UIのNetwork Configuration >Network Protocols 画面のWeb (HTTP/HTTPS) - TLS1.0/1.1をDisableに設定する。
   https接続可能な場合、以下の手順は不要です。
2. Webブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
3. [セキュリティ]項目の[TLS1.2を使用する]にチェックを入れます。
4. [OK]ボタンをクリックします。

※16. 以下の設定を行ってください。

設定 1. 以下の操作で Microsoft Edge のフォントサイズを「小」に変更します。

Microsort Edge がレガシー版の場合は、以下の手順は不要です。

1. Web ブラウザの[設定]を選択します。
2. 外観の[フォントサイズ]を「小」に変更します。
3. 「設定」タブを閉じます。

設定2. https接続を行う場合、以下の設定をしてください。

- 統合ファームウェア版数がTLS1.2未サポートの場合。(BA17031/BB17031/BC17031以前)
  https接続可能な場合、以下の手順は不要です。
  1. Windowsの[コントロールパネル]→[インターネットオプション]の[詳細設定]タブを選択します。
  2. [セキュリティ]項目の[TLS1.0を使用する]、[TLS1.1を使用する]、 [TLS1.2を使用する]の
     いずれかにチェックを入れます。
  3. [OK]ボタンをクリックします。

  ただし、TLS1.0はサポート終了しており、TLS1.0の有効時の動作はサポートしません。

※17. 以下の設定を行ってください。

設定 1. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムと セキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 2. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。
4. [OK]ボタンをクリックします。

設定 3. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 4. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無 効にする]をチェックします

4. [OK] ボタンをクリックします。

設定 5. 以下の操作で互換表示の有効設定をしてから SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます。
2. [互換表示設定]画面の[追加する Web サイト]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 7. 以下の方法で信頼済みサイトに SVP コンソールの URL を登録します

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[信頼済みサイト]を選択し、[保護モードを有効にする(Internet Explorer の再起動が必要)(P)]のチェックが付いている場合は外し、[サイト]ボタンをクリックします。
3. [信頼済みサイト]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする(S)]のチェックを外し、[この Web サイトをゾーンに追加する(D)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

※18. 以下の設定を行ってください。

設定 1. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 2. 以下の方法でファイルのダウンロードを有効にします。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。

4. [OK]ボタンをクリックします。

設定 3. 以下の方法でポップアップブロックを解除します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 4. 以下の方法で XSS フィルターを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無 効にする]をチェックします
4. [OK] ボタンをクリックします。

設定 5. 以下の操作で互換表示の有効設定をしてから SVP コンソールにログインします。

1. Web ブラウザの[ツール(T)]→[互換表示設定(B)]を選択し[互換表示設定]画面を開きます。
2. [互換表示設定]画面の[追加する Web サイト]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
3. [閉じる(C)]ボタンをクリックします。

設定 6. 以下の方法で拡張保護モードを無効に設定します。

1. Web ブラウザの[ツール(T)]→[インターネットオプション(O)]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 7. 以下の方法でローカルイントラネットに SVP コンソールの URL を登録します

1. SVP コンソールのログイン画面を表示します。
2. ブラウザの[ツール]-[インターネットオプション]の[セキュリティ]タブを開きます。
3. ゾーンとして「ローカルイントラネット」が選択されており、[保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが外れていることを確認してくだい。
   [保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが付いている場合はチェックを外してください。
   「ローカルイントラネット」が選択されていない場合、以下の手順で SVP コンソールの URL を「ローカルイントラネット」に登録します。
4. [セキュリティ]タブで[ローカルイントラネット]を選択し、[サイト]をクリックします。
5. [詳細設定]をクリックします。
6. [ローカルイントラネット]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする]の

チェックが外れていることを確認し、[この Web サイトをゾーンに追加する]に URL(http:// XSP パーティションの IP アドレス/)を入力し[追加]をクリックします。

設定 8. 以下の方法で 2016 年 1 月以降に配信された Windows Update を適用してください。

1. Windows の[設定]-[更新とセキュリティ]の[Windows Update]を選択します。
2. [更新プログラムのチェック]ボタンをクリックします。
3. 利用可能な更新プログラムが検出されたら[インストール]ボタンをクリックします。
4. [今すぐ再起動]ボタンが表示されたら、[今すぐ再起動]ボタンをクリックします。 (この際、コンピューターが自動的に再起動します)。
   [今すぐ再起動] ボタンが表示されなければ、Windows Update の画面を閉じて終了します。

※19. 以下の設定を行ってください。なお、本設定はSVPコンソールのサイトのみをIEモードにて動作させるための設定であり、他のサイト接続には影響ありません。

設定 1. 以下の操作で Microsoft Edge のフォントサイズを「小」に変更します。

1. Web ブラウザの[設定]を選択します。
2. 外観の[フォントサイズ]を「小」に変更します。
3. 「設定」タブを閉じます。

設定 2. 以下の方法でスリープ状態と休止状態にならないように設定します。

1. Windows の[コントロールパネル]→[システムとセキュリティ]→[電源オプション]を選択します。
2. [コンピューターがスリープ状態になる時間の変更]を選択します。
3. [コンピューターをスリープ状態にする]の[適用しない]を選択します。
4. [変更の保存]ボタンをクリックします。
5. [電源ボタンの動作の選択]を選択します。
6. デスクトップ PC の場合は、[電源ボタンを押したときの動作]の[何もしない]を選択します。
   ノート PC の場合は、[カバーを閉じたときの動作]の[何もしない]を選択します。
7. [変更の保存]ボタンをクリックします。

設定 3. 以下の方法でファイルのダウンロードを有効にします。

1. Windows の[コントロールパネル]→[インターネットオプション]の[セキュリティ]タブを 選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面の[ダウンロード]項目の[ファイルのダウンロード]の[有効にする]をチェックします。
4. [OK]ボタンをクリックします。

設定 4. 以下の方法でポップアップブロックを解除します。

1. Windows の[コントロールパネル]→[インターネットオプション]の[プライバシー]タブを選択します。
2. [ポップアップブロックを有効にする(B)]にチェックを入れて、[設定(E)]ボタンをクリックします。
3. [ポップアップブロックの設定]画面の[許可する Web サイトのアドレス(W)]に SVP コンソールの URL(http://XSP パーティションの IP アドレス/)を入力し、[追加(A)]ボタンをクリックします。
4. [閉じる(C)]ボタンをクリックします。

設定 5. 以下の方法で XSS フィルターを無効に設定します。

1. Windows の[コントロールパネル]→[インターネットオプション]の[セキュリティ]タブを選択します。
2. ゾーンとして[インターネット]、または[ローカルイントラネット]が選択されていることを確認し、[レベルのカスタマイズ(C)]ボタンをクリックします。
3. [セキュリティ設定]画面で、[スクリプト]項目の[XSS フィルターを有効にする]の[無 効にする]をチェックします
4. [OK] ボタンをクリックします。

設定 6. 以下の方法で拡張保護モードを無効に設定します。

1. Windows の[コントロールパネル]→[インターネットオプション]]の[詳細設定]タブを選択します。
2. [セキュリティ]項目の[拡張保護モードを有効にする]がチェックされている場合はチェックを外します。
3. [OK]ボタンをクリックします。

設定 7. 以下の方法でローカルイントラネットに SVP コンソールの URL を登録します

1. SVP コンソールのログイン画面を表示します。
2. Windows の[コントロールパネル]→[インターネットオプション]の[セキュリティ]タブを開きます。
3. ゾーンとして「ローカルイントラネット」が選択されており、[保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが外れていることを確認してくだい。
   [保護モードを有効にする(Internet Explorer の再起動が必要)]のチェックが付いている場合はチェックを外してください。
   「ローカルイントラネット」が選択されていない場合、以下の手順で SVP コンソールの URL を「ローカルイントラネット」に登録します。
4. [セキュリティ]タブで[ローカルイントラネット]を選択し、[サイト]をクリックします。
5. [詳細設定]をクリックします。
6. [ローカルイントラネット]画面の[このゾーンのサイトにはすべてのサーバの確認(https:)を必要とする]のチェックが外れていることを確認し、[この Web サイトをゾーンに追加する]に URL(http:// XSP パーティションの IP アドレス/)を入力し[追加]をクリックします。

設定 8. 以下の方法で 2016 年 1 月以降に配信された Windows Update を適用してください。

1. Windows の[設定]-[更新とセキュリティ]の[Windows Update]を選択します。
2. [更新プログラムのチェック]ボタンをクリックします。
3. 利用可能な更新プログラムが検出されたら[インストール]ボタンをクリックします。
4. [今すぐ再起動]ボタンが表示されたら、[今すぐ再起動]ボタンをクリックします。 (この際、コンピューターが自動的に再起動します)。

[今すぐ再起動] ボタンが表示されなければ、Windows Update の画面を閉じて終了します。

設定9. 以下の方法でIEモードを有効化してください。なお、本手順で設定できない場合は、設定10に従ってIEモードを有効化してください。

1. 下記のMicrosoftのサイトからEdgeのバージョンに対応するポリシーファイルをダウンロードします。
   https://www.microsoft.com/ja-jp/edge/business/download
2. ポリシーファイルを解凍してできたファイルのうち、以下を格納先ディレクトリに格納します。

格納するファイル	格納先ディレクトリ
windows¥admx¥msedge.admx	C:¥windows¥PolicyDefinitions
windows¥admx¥msedgeupdate.admx	
windows¥admx¥msedgewebview2.admx	
windows¥admx¥ja-JP¥msedge.adml	C:¥windows¥PolicyDefinitions¥ja-JP
windows¥admx¥ja-JP¥msedgeupdate.adml	
windows¥admx¥ja-JP¥msedgewebview2.adml	

3. [Windows]＋[R]キーで[ファイル名を指定して実行する]ダイアログを開き、[gpedit.msc]と入力して[OK]をクリックします。
4. 起動したローカルグループポリシーエディターで[管理用テンプレート]→[Microsoft Edge]を選択します。
5. 設定項目の内、以下の項目をそれぞれ指定の値に設定します。

設定	状態	オプション
[Internet Explorer統合を構成する]	[有効(Y)]	[Internet Explorerモード]
[エンタープライズモードサイトリストを構成する]	[有効(Y)]	[C:¥Users¥〈*user名*〉¥Documents¥sites.xml] ※〈*user名*〉はPC共有コンソールのユーザー名
[エンタープライズモードサイトリストマネージャーのツールへのアクセスを許可する]	[有効(Y)]	-

6. 設定を反映するため、PCを再起動します。

設定10. 設定9が実施できない場合は以下の方法でIEモードの設定をしてください。なお、設定9によりIEモードを有効化できた場合、本設定は不要です。

1. [Windows]＋[R]キーで[ファイル名を指定して実行する]ダイアログを開き、[regedit.exe]と入力して OKをクリックします。
2. [レジストリエディター]で[コンピューター]を右クリックし、[エクスポート]を選択してバックアップファイルを保存します。
3. [スタートボタン]を右クリックし、[Windows PowerShell(管理者)]を選択します。
4. [PowerShell]で以下の3つのコマンドを実行し、レジストリを登録します。

```
reg add HKLM¥SOFTWARE¥Policies¥Microsoft¥Edge /v EnterpriseModeSiteListManagerAllowed /t REG_DWORD /d 1 /f
```

```
reg add HKLM¥SOFTWARE¥Policies¥Microsoft¥Edge /v InternetExplorerIntegrationLevel /t REG_DWORD /d 1 /f
```

```
reg add HKLM¥SOFTWARE¥Policies¥Microsoft¥Edge /v  InternetExplorerIntegrationSiteList /t REG_SZ /d C:¥Users¥〈user名〉¥Documents¥sites.xml /f
```

※〈user名〉はPC共有コンソールのユーザー名

5. 設定を反映するために、PCを再起動します。

設定11. 以下の方法でIEモードの対象としてSVPコンソールを登録してください。

1. Edgeを起動後、右上の[・・・]をクリックし、[設定]を選択します。
2. [ダウンロード]を選択し、[ダウンロード時の動作を毎回確認する]を有効にします。
3. Edgeのアドレスバーに[edge://compat/sitelistmanager]と入力後、[Enterキー]を押します。
4. [エンタープライズサイトリストマネージャー]の [サイトの追加]をクリックします。
5. [サイトの追加]ダイアログの[URL]欄にSVPコンソールのURL(http://XSPパーティションのIPアドレス/)を入力し、[開く]で[IEモード]、[互換モード]で[IE5 ドキュメントモード]を選択後、[追加]をクリックします。
6. [XMLにエクスポート]をクリックし、[バージョン番号:]に任意の値を入力後、[エクスポート]をクリックします。
7. [名前を付けて保存]を選択し、[C:¥Users¥〈user名〉¥Documents¥sites.xml]にファイルを保存します。
   ※〈user名〉はPC共有コンソールのユーザー名
8. [エンタープライズモードサイトリスト]をクリックし、 [強制的に更新]をクリックします。

※20. 以下の設定を行ってください。

設定 1. 以下の操作で Microsoft Edge のフォントサイズを「小」に変更します。

Microsort Edge がレガシー版の場合は、以下の手順は不要です。

4. Web ブラウザの[設定]を選択します。
5. 外観の[フォントサイズ]を「小」に変更します。
6. 「設定」タブを閉じます。

※21. Edge(IE モード)を設定してください。設定方法については、以下を参照してください。

[ASP 動作機構 Windows Web ブラウザの対応状況について]

https://fujitsu.sharepoint.com/sites/jp-server/media/products/office_computer/cloud/sales-information/20190529_1.pdf

以上