BOM for Windows Ver.8.0

監視テンプレート個別注意事項

■ 目次

第1章 本書について
1. 表記
2. 使用上のご注意
第2章 更新内容
第3章 新規公開テンプレート
1. 標準構成テンプレート
システム安定運用-セキュリティテンプレート
Windows Server 2025 監視
2. Windowsオプション
Hyper-V インプレースアップグレード後の状態チェック
第4章 既存テンプレート
1. 標準構成テンプレート
Windows システム監視 Basic (ローカル監視)
Windows システム運用監視 Basic (ローカル監視)
システム安定運用-セキュリティテンプレート
システム安定運用-パフォーマンス改善テンプレート
朝監視
2. レポートテンプレート
Windows サーバー診断レポート用
Arcserve UDPv6/v6.5/v7/v8ログ取得レポート用
セキュリティログレポート用
VMware レポート用
Hyper-Vレポート用
Linuxサーバー診断レポート用
3. Windows 基本
EV自動復旧機能
4. Windows オプション
WSUS監視
セキュリティログ
5. ハードウェア
NEC ESMPRO/ServerAgent Service Ver1.0-1.3
Fujitsu ServerView Agents v8_v9 監視
Hitachi JP1 Server Conductor / Blade Server Manager V10
6. データベース サーバー
[オプション] Oracle Database 19c/21c
[オプション] SQL Server
SQL Server 2014
SQL Server 2016
SQL Server 2017 (Windows版)
SQL Server 2019 (Windows版)
SQL Server 2022 (Windows版)
7. Web サーバー
Internet Information Services 10.0
8. バックアップ ソフト
Backup Exec 20_21
Arcserve Backup r17.5

- CA ARCserve RHA r16.5
- Arcserve RHA 18.0
- Arcserve UDP v6.5 & v7 & v8
- ActiveImage Protector 2018 -RE
- ActiveImage Protector 2018 ServerEditon
- ActiveImage Protector 2022 -RE
- ActiveImage Protector 2022 ServerEditon
- Windows Server Backup 監視
- Acronis Cyber Protect 15 監視
- Arcserve UDP 9 & 10

9. ウイルス対策 ソフト
   - Trend Micro Apex One 監視
   - ESET_PROTECT 監視
   - Trellix Endpoint Security 10.7 監視
   - Symantec Endpoint Protection 14 監視
10. BOMカスタム監視補助
11. Windows その他
    - MylogStar 4 Enterprise - MylogStar Server 監視
    - MylogStar 4 Enterprise - MylogStar Agent 監視
12. Linux 標準構成テンプレート
    - Linux システム監視 Basic
    - Linux システム監視 Basic with UUIDディスク監視
13. Linux 基本
    - Linux ディスク監視
    - Linux テキストログ監視
    - Linux UUIDディスク監視
14. Linux アプリケーション
    - Linux Apache サーバー監視
    - Linux Postfix 監視
    - Linux NFS 監視
    - Linux DHCP サーバー監視
15. VMware 標準構成テンプレート

免責事項

本書に記載された情報は、予告無しに変更される場合があります。セイ・テクノロジーズ株式会社は、本書に関していかなる種類の保証 (商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません) もいたしません。
セイ・テクノロジーズ株式会社は、本書に含まれた誤謬に関しての責任や、本書の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。

著作権

商標

文中の社名、製品名、サービス名等は各社の商標または登録商標である場合があります。
なお、本文および図表中では「™ (Trademark)」、「® (Registered Trademark)」を明記しておりません。

第1章 本書について

本書では、BOM for Windows Ver.8.0 同梱の監視テンプレートおよび、追加公開された各監視テンプレートについて、個別の注意事項が存在するものをまとめています。

これらの注意事項は BOM for Windows Ver.8.0 の「テンプレートのインポート」画面で、プレビュー欄に表示されるものと同等の内容です。

1. 表記

本書では、製品、サービス名について以下の略称を使用する場合があります。

製品・サービス名	本書での略称
BOM for Windows Ver.8.0	BOM 8.0

2. 使用上のご注意

- 監視テンプレートの適用方法については、製品同梱の「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。

第2章 更新内容

以下の更新を行いました。

改版日	
2022/06/15	初版
2022/07/01	■以下の新規公開テンプレートについて、注意事項を追加。 ・ハードウェア - NEC ESMPRO/ServerAgent Service Ver1.0-1.3 ・ハードウェア - Fujitsu ServerView Agents v8_v9 監視 ・ハードウェア - Hitachi JP1 Server Conductor / Blade Server Manager V10 ■以下のテンプレートについて、注意事項を追加 ・Linux 標準構成テンプレート - Linux システム監視 Basic ・Linux 基本 - Linux テキストログ監視
2022/09/14	■以下の新規公開テンプレートについて、注意事項を追加。 ・バックアップ ソフト - Acronis Cyber Protect 15 監視
2022/10/24	■以下の新規公開テンプレートについて、注意事項を追加。 ・ウイルス対策 ソフト - Trend Micro Apex One 監視
2022/12/12	■「更新内容」の記載方法を変更 ■以下の新規公開テンプレートについて、注意事項を追加。 ・ウイルス対策 ソフト - ESET_PROTECT 監視
2023/02/15	■以下の新規公開テンプレートについて、注意事項を追加。 ・Windows その他 - MylogStar 4 Enterprise - MylogStar Server 監視 ・Windows その他 - MylogStar 4 Enterprise - MylogStar Agent 監視
2023/05/24	■以下の新規公開テンプレートについて、注意事項を追加。 ・ウイルス対策 ソフト - Trellix Endpoint Security 10.7 監視
2023/08/25	■以下の新規公開テンプレートについて、注意事項を追加。 ・データベースサーバー - SQL Server 2022 (Windows版) ・バックアップ ソフト - Arcserve UDP 9.0 監視 ・ウィルス対策 ソフト - Symantec Endpoint Protection 14 監視
2025/04/01	■以下の新規公開テンプレートについて、注意事項を追加。 ・標準構成テンプレート - システム安定運用-セキュリティテンプレート ・標準構成テンプレート - Windows Server 2025 監視 ・Windowsオプション - Hyper-V インプレースアップグレード後の状態チェック ■以下の既存テンプレート（※）について、注意事項を追加。 ・Linux 標準構成テンプレート - Linux システム監視 Basic with UUIDディスク監視 ・Linux 基本 - Linux UUIDディスク監視
2025/12/05	■以下の更新されたテンプレートについて、注意事項を追加。 ・Linux アプリケーション - Linux DHCP サーバー監視

改版日	
2026/03/31	■以下の更新されたテンプレートについて、注意事項を追加。 ・Windows オプション - セキュリティログ ■以下のテンプレートについて、テンプレート名を更新 ・バックアップ ソフト - Arcserve UDP 9.0 監視 (旧名称) → Arcserve UDP 9 & 10 (新名称)

※ これらのテンプレートは、既存で個別にウェブ公開されていたものを、テンプレートパッケージへ同梱したものです。

第3章 新規公開テンプレート

1. 標準構成テンプレート

システム安定運用-セキュリティテンプレート

- 「Windowsの運用管理を快適にする10の裏ワザ表ワザ(セキュリティ編)」に沿って作成された、 監視・アクション設定およびバッチファイルから成る BOM for Windows Ver.8.0向けのテンプレートで、Windows Update監視グループの監視項目2つは以下の当社ブログと連携しています。
  - 最後の更新からの経過日数を監視して「Windows Update監視」を強化する－BOM for Windows活用例
    https://www.say-tech.co.jp/contents/blog/column/202503_bompuse_wu
- 本テンプレートはスクリプトファイルを必要とし、スクリプトファイルは下記のディレクトリに保存されている必要があります。

  > [BOM インストールディレクトリ]¥SAY Technologies¥BOMW8¥Bin¥Support¥

- 本設定項目には監視項目と連携したメール送信のアクションがありますが、メール送信アクションについては、送信先メールアドレスの設定と、メールサーバーの設定が必要になります。詳細は「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。
- 本設定項目は、ローカル監視のみ動作します。代理監視では動作しません。

Windows Server 2025 監視

- 本テンプレートは **Windows Server 2025 に対応**する、**BOM 8.0 SR2 専用**のテンプレートです。それ以外の環境では動作しません。
- 本テンプレートは以下の当社ブログと連携しています。必要に応じて監視を有効にしてください。
  - OSConfigのセキュリティベースライン対応状況の確認をスクリプト化する
    https://www.say-tech.co.jp/contents/blog/yamanxworld/2025memo36
  - Windows Server 2025で非推奨になった機能の状態を監視する
    https://www.say-tech.co.jp/contents/blog/column/202501_bompuse_sv25
- 本テンプレートはスクリプトファイルを必要とし、スクリプトファイルは下記のディレクトリに保存されている必要があります。

  > [BOM インストールディレクトリ]¥SAY Technologies¥BOMW8¥Bin¥Support¥

- 各セキュリティベースラインチェック監視のしきい値は参考程度の仮の値です。ベースラインと一致しない項目については、各セキュリティチェックリスト項目を実行し、出力リストを参考にしてください。
- 非推奨機能の状態チェックは、「危険」ステータスの項目は非推奨機能がアクティブの状態です。
- 本設定項目には監視項目と連携したメール送信のアクションがありますが、メール送信アクションについては、送信先メールアドレスの設定と、メールサーバーの設定が必要になります。詳細は「BOM for Windows Ver.8.0 SMTP ファイル送信ユーザーズマニュアル」を参照してください。
- 本設定項目は、ローカル監視のみ動作します。代理監視では動作しません。

2. Windowsオプション

Hyper-V インプレースアップグレード後の状態チェック

- 本テンプレートは以下の当社ブログと連携しています。
  - 旧バージョンからのアップグレード（Hyper-Vサーバー編）｜Windows Server 2025大特集（3）
    https://www.say-tech.co.jp/contents/blog/yamanxworld/2024vol066
- Hyper-VホストとVMの構成バージョンを比較し、構成バージョンが異なるVM数をカウントする監視テンプレートです。
- 本テンプレートはスクリプトファイルを必要とし、スクリプトファイルは下記のディレクトリに保存されている必要があります。

  [BOM インストールディレクトリ]¥SAY Technologies¥BOMW8¥Bin¥Support¥

- 本設定項目は、ローカル監視のみ動作します。代理監視では動作しません。

第4章 既存テンプレート

1. 標準構成テンプレート

Windows システム監視 Basic (ローカル監視)

- 本監視テンプレートは代理監視インスタンスに適用できません。自立 (ローカル) 監視で使用してください。

Windows システム運用監視 Basic (ローカル監視)

- 「Windows システム監視 Basic (ローカル監視)」テンプレートとの違いとして、しきい値の基準を本監視項目では取得値の平均値にしています。また、インスタンス開始時にメール送信する監視項目と一日一度生死を通知するハートビード通知項目が追加されています。
- 「通知」設定項目には監視項目と連携したメール送信のアクションがありますが、メール送信アクションについては、送信先メールアドレスの設定と、メールサーバーの設定が必要になります。詳細は「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。

システム安定運用-セキュリティテンプレート

- 「Windowsの運用管理を快適にする10の裏ワザ表ワザ(セキュリティ編)」に沿って作成された、 監視・アクション設定およびバッチファイルから成る BOM for Windows Ver.8.0向けのテンプレートです。
- 本設定項目には監視項目と連携したメール送信のアクションがありますが、メール送信アクションについては、送信先メールアドレスの設定と、メールサーバーの設定が必要になります。詳細は「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。

システム安定運用-パフォーマンス改善テンプレート

- 「Windowsの運用管理を快適にする10の裏ワザ表ワザ(パフォーマンス改善編)」に沿って作成された、監視・アクション設定およびバッチファイルから成る BOM for Windows Ver.8.0 向けのテンプレートです。
- 本設定項目には監視項目と連携したメール送信のアクションがありますが、メール送信アクションについては、送信先メールアドレスの設定と、メールサーバーの設定が必要になります。詳細は「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。

朝監視

- 本監視項目は朝監視用の監視設定です。本監視設定はメール送信の設定が必要です。詳細は「BOM for Windows Ver.8.0 朝監視設定ユーザーズマニュアル」を参照してください。

2. レポートテンプレート

Windows サーバー診断レポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。
- 「システムログ監視」「アプリケーションログ監視」ではしきい値として通常許容されない「0件より小さい」が設定されているため、プロパティの「しきい値」タブを表示すると適切な値の入力を促すダイアログが表示されます。この際は[OK]→[キャンセル]とクリックしてプロパティを一度閉じてください。

Arcserve UDPv6/v6.5/v7/v8ログ取得レポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。

セキュリティログレポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。

VMware レポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。
- 「VMware イベント監視」「vCenter ログ監視」ではしきい値として通常許容されない「0件より小さい」が設定されているため、プロパティの「しきい値」タブを表示すると適切な値の入力を促すダイアログが表示されます。この際は[OK]→[キャンセル]とクリックしてプロパティを一度閉じてください。
- 監視項目「vCenter ログ監視」を使用する際は、プロパティで「有効」にチェックを入れ、「接続先」タブで「vCenterサーバー」のユーザーとパスワードを登録する必要があります。

Hyper-Vレポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。

Linuxサーバー診断レポート用

- 本監視項目はレポート向けのログ収集用のため、しきい値は監視向けに構成されていません。

3. Windows 基本

EV自動復旧機能

- BOM はイベントログ監視の監視開始位置管理のためイベントログの EventRecordID を記録していますが、この値がまれにシステムの想定外の動作によって異常値となり、イベントログ監視が正常に実行されないことがあります。
  本テンプレートを導入することにより、この異常の検知と、正常な EventRecordID への復旧を自動的に行うことができます。
- 本監視テンプレートの内容は「Windows システム監視 Basic (ローカル監視)」テンプレートおよび「Windows システム運用監視 Basic (ローカル監視)」テンプレートにも含まれており、すでにこれらのテンプレートを適用済みの場合、本テンプレートのインポートは不要です。
- 本監視テンプレートは、各インスタンスについて一度適用するだけで、同一インスタンス内のすべてのイベントログ監視に有効です。
- 本監視テンプレートは代理監視インスタンスには適用できません。自立 (ローカル) 監視で使用してください。

4. Windows オプション

WSUS監視

- 本監視テンプレートは、テクニカルライター 山市 良 氏の著作「WSUS 正常性監視のポイント - Windows 10 時代の重要インフラ WSUS、安定運用の勘所」に沿った内容となっており、このテンプレートを利用することで WSUS の監視ポイントである「ネットワーク使用帯域」、「サービスの正常性」、「ディスク使用率」の情報が取得できます。
  設定内容の根拠や詳細については、本テンプレートが基にした以下のドキュメントを参照してください。
  - WSUS 正常性監視のポイント - Windows 10 時代の重要インフラ WSUS、安定運用の勘所 (PDF)
    https://www2.say-tech.co.jp/hubfs/download-sales/yamaichi/WSUS正常性監視のポイント.pdf
- ディスク使用率に応じてクリーンアップタスクを実施する「WSUSクリーンアップタスク」アクションが「WsusContentフォルダー監視」に設定されています。初期値は「無効」となっていますので、必要に応じて「有効」に設定してください。
- 「WSUSクリーンアップタスク」アクションを動作させる際は、事前に PowerShell を開いて以下のコマンドラインを一度だけ実行する必要があります。

```
PS > New-EventLog -LogName Application -Source "WSUS Cleanup Task"
```

- 本監視テンプレートは代理監視インスタンスには適用できません。自立 (ローカル) 監視で使用してください。

セキュリティログ

- 本監視テンプレートはセイ・テクノロジーズのブログ記事とリンクしています。詳細は以下の記事を参照してください。
  - 製品コラム-セキュリティ監視の基本－BOM for Windows活用例
    https://www.say-tech.co.jp/contents/blog/column/2024jun_bomsec01
- 「追加のセキュリティ監視」グループの監視項目には、監視結果と連携したメール送信のアクションが登録されていますが、このメール送信アクションを実行するためには、事前のメールサーバー設定と送信先メールアドレスの設定が必要です。設定の詳細は「BOM for Windows Ver.8.0 ユーザーズマニュアル」を参照してください。
- 本監視テンプレートでは、しきい値として通常許容されない「0件より小さい」が設定されているため、プロパティの「しきい値」タブを表示すると適切な値の入力を促すダイアログが表示されます。この際は[OK]→[キャンセル]とクリックしてプロパティを一度閉じてください。

5. ハードウェア

NEC ESMPRO/ServerAgent Service Ver1.0-1.3

- 監視対象サーバーに合わせて、各サービス監視の有効/無効設定を変更してください。
  本テンプレートに設定されたサービス監視は既定ですべて「有効」となっていますが、監視対象のサーバーに該当のサービスがない場合、監視は失敗します。

Fujitsu ServerView Agents v8_v9 監視

- 監視対象サーバーに合わせて、各サービス監視の有効/無効設定を変更してください。
  本テンプレートに設定されたサービス監視は既定ですべて「有効」となっていますが、監視対象のサーバーに該当のサービスがない場合、監視は失敗します。

Hitachi JP1 Server Conductor / Blade Server Manager V10

- 監視対象サーバーに合わせて、各サービス監視の有効/無効設定を変更してください。
  本テンプレートに設定されたサービス監視は既定ですべて「有効」となっていますが、監視対象のサーバーに該当のサービスがない場合、監視は失敗します。

6. データベース サーバー

[オプション] Oracle Database 19c/21c

- 本監視テンプレートは Oracle オプション専用です。

[オプション] SQL Server

- 本監視テンプレートは SQL Server オプション専用です。必要に応じて基本機能でも適用可能な SQL Server 向けテンプレートと合わせて利用してください。

SQL Server 2014

- 本監視項目中、(MSSQLSERVER) とあるのは既定インスタンス名を示しています。名前付きインスタンスの場合にはインスタンス名を変更してください。

SQL Server 2016

- 本監視項目中、(MSSQLSERVER) とあるのは既定インスタンス名を示しています。名前付きインスタンスの場合にはインスタンス名を変更してください。

SQL Server 2017 (Windows版)

- 本監視項目中、(MSSQLSERVER) とあるのは既定インスタンス名を示しています。名前付きインスタンスの場合にはインスタンス名を変更してください。

SQL Server 2019 (Windows版)

- 本監視項目中、(MSSQLSERVER) とあるのは既定インスタンス名を示しています。名前付きインスタンスの場合にはインスタンス名を変更してください。

SQL Server 2022 (Windows版)

- 「SQL Server 2022 サービス監視」グループの以下の監視項目に設定されているサービス名は、SQL Serverのインスタンスが「既定のインスタンス」の場合に表示されるサービス名です。「名前付きインスタンス」の場合はサービス名が異なるため、必要に応じて変更してください。
  - SQL Server (MSSQLSERVER) 監視
  - SQL Server エージェント (MSSQLSERVER) 監視
  - SQL Server CEIP service (MSSQLSERVER) 監視
- 「SQL Server 2022 イベントログ監視」グループの以下の監視項目に設定されているイベントソースは、SQL Serverのインスタンスが「既定のインスタンス」の場合に表示されるソース名です。「名前付きインスタンス」の場合はソース名が異なるため、必要に応じて変更してください。
  - MSSQLSERVER イベント監視
  - SQLSERVERAGENT イベント監視

7. Web サーバー

Internet Information Services 10.0

- Microsoft FTP Service 監視は、Microsoft FTP Service が IIS 10.0 の標準でインストールされないため「無効」となっています。FTPサーバーを使用する場合は本監視の設定を「有効」にしてください。
- W3C Logging Service 監視は、W3C Logging Service の既定の設定が「手動・停止状態」のため「無効」となっています。W3C Logging Serviceを実行する場合は本監視の設定を「有効」にしてください。

8. バックアップ ソフト

Backup Exec 20_21

- 監視項目「バックアップ正常性監視」は、Backup Execによるバックアップ処理が正常に開始した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。
  当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

Arcserve Backup r17.5

- 監視項目「バックアップ正常性監視」は、Arcserve Backupによるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。
  当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

CA ARCserve RHA r16.5

- インストール時は監視グループが無効となっていますので、必要に応じて有効に変更してください。

Arcserve RHA 18.0

- 監視項目「Arcserve RHA エンジン 正常性監視」は、Arcserve RHAによるバックアップ処理が正常に完了した際にテキストログへ出力されるメッセージを1日に1度の間隔で監視し、該当のメッセージが48件存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化するため、実際に運用する環境で確認した上で設定してください。
- 当監視項目にメールアクション等を追加することで、バックアップが正常に終了していない事を通知できます。
- 監視項目「Arcserve RHA エンジン 重大/エラー/警告ログ監視」は、あらかじめArcserve RHAのイベント通知設定で「イベントログへの書き込み」が「オン」に設定されている必要があります。

Arcserve UDP v6.5 & v7 & v8

- 本監視テンプレートと、監視テンプレート「Windows システム監視 Basic」の「ログ監視」を併用することで、Arcserve UDPの異常を監視することが可能となります。
- 監視項目「バックアップ正常性監視」は、Arcserve UDPによるバックアップ処理が正常に開始した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。
  当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。
- 監視項目「バックアップ正常性監視」を実行する際は、Arcserve UDPのアクティビティ ログをWindowsのイベントログに登録する設定が行われている必要があります。本設定の詳細についてはarcserve社の技術資料を参照してください。

ActiveImage Protector 2018 -RE

- 監視項目「バックアップ正常性監視」は、ActiveImage Protector 2018 -REによるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化するため、実際に運用する環境で確認した上で設定してください。
- 当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

ActiveImage Protector 2018 ServerEditon

- 監視項目「バックアップ正常性監視」は、ActiveImage Protector 2018 ServerEditonによるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化するため、実際に運用する環境で確認した上で設定してください。
- 当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

ActiveImage Protector 2022 -RE

- 監視項目「バックアップ正常性監視」は、ActiveImage Protector 2022 -REによるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化するため、実際に運用する環境で確認した上で設定してください。
- 当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

ActiveImage Protector 2022 ServerEditon

- 監視項目「バックアップ正常性監視」は、ActiveImage Protector 2022 ServerEditonによるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化するため、実際に運用する環境で確認した上で設定してください。
- 当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

Windows Server Backup 監視

- 監視項目「Windows Backup 正常性監視」は、Windows Server Backup によるバックアップ処理が正常に開始した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。
- 当監視項目にメール通知アクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。

Acronis Cyber Protect 15 監視

- 監視項目「バックアップ正常性監視」は、Acronis Cyber Protect 15によるバックアップ処理が正常に完了した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが7件存在しなかった場合はステータスが「危険」になるよう設定されています。そのため、初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
  なお、本メッセージの件数は構成によって変化いたしますので、お客様の環境で確認して設定ください。
- 当監視項目にメールアクション等を追加することで、バックアップが正常に終了していない事を通知できます。
- 監視項目「バックアップエラー監視」、「バックアップ正常性監視」はあらかじめAcronis Cyber Protect 15のバックアップオプションでWindows イベントログに記録する設定が「はい」である必要があります。

Arcserve UDP 9 & 10

(旧名称： Arcserve UDP 9.0 監視)

- 監視項目「バックアップ正常性監視」は、Arcserve UDPによるバックアップ処理が正常に開始した際にイベントログへ出力されるメッセージを7日に1度の間隔で監視し、該当のメッセージが1件も存在しなかった場合はステータスが「危険」になるよう設定されています。初回監視は必ず危険ステータスになります。初回ステータスは無視してください。
- 当監視項目にメールアクション等を追加することで、長期間バックアップが正常に終了していない事を通知できます。
- 監視項目「バックアップ正常性監視」「バックアップ 重大/エラー/警告ログ監視」を実行する際は、Arcserve UDPのアクティビティ ログをWindowsのイベントログに登録する設定が行われている必要があります。本設定の詳細についてはarcserve社の技術資料を参照してください。

9. ウイルス対策 ソフト

Trend Micro Apex One 監視

- 本テンプレートには「Trend Micro Apex One サーバー監視」と「Trend Micro Apex One エージェント監視」を同梱しています。それぞれの監視対象に応じて監視グループを適切に有効・無効にしてください。

ESET_PROTECT 監視

- 本テンプレートは ESET PROTECT Entry オンプレミス のサービスを監視対象にしています。環境に応じて有効・無効を変更してください。

Trellix Endpoint Security 10.7 監視

- 監視項目「Trellix Endpoint Security ログ監視」は、あらかじめ Trellix Endpoint Security の共通設定で「Windows アプリケーションログにイベントを記録する」が「オン」に設定されている必要があります。

Symantec Endpoint Protection 14 監視

- 本テンプレートには「Symantec Endpoint Protection 14 サーバー監視」と「Symantec Endpoint Protection 14 クライアント監視」を同梱しています。監視対象に応じてそれぞれの監視グループを適切に有効・無効にしてください。

10. BOMカスタム監視補助

個別注意事項のある監視テンプレートはありません。

11. Windows その他

MylogStar 4 Enterprise - MylogStar Server 監視

- MylogStar Agent ローカルログ容量監視を実行する際は、「MylogStar Console」のポリシー設定で隠蔽レベルを「中」または「なし」に設定する必要があります。設定方法については、以下のURLかダウンロードできる手順書を参照してください。
  - MylogStar 4 Enterprise 監視テンプレート用導入手順書
    https://www.say-tech.co.jp/support/download/bom80/99086339397
- 「注意」および「危険」とする値は、環境に合わせて「しきい値」タブで変更してください。
- ローカルログファイルの出力先を標準設定から変更している場合は「設定」タブで設定してください。

MylogStar 4 Enterprise - MylogStar Agent 監視

- MylogStar Agent ローカルログ容量監視を実行する際は、「MylogStar Console」のポリシー設定で隠蔽レベルを「中」または「なし」に設定する必要があります。設定方法については、以下のURLかダウンロードできる手順書を参照してください。
  - MylogStar 4 Enterprise 監視テンプレート用導入手順書
    https://www.say-tech.co.jp/support/download/bom80/99086339397
- 「注意」および「危険」とする値は、環境に合わせて「しきい値」タブで変更してください。
- ローカルログファイルの出力先を標準設定から変更している場合は「設定」タブで設定してください。

12. Linux 標準構成テンプレート

Linux システム監視 Basic

- 本監視テンプレートでは既定でRHEL環境向けの監視項目が有効になっています。Ubuntu環境ではテンプレート適用後に以下の設定を行ってください。
  - RHEL環境向けの監視項目を無効化、または削除する。
  - Ubuntu環境向けの監視項目を有効化する。

Linux システム監視 Basic with UUIDディスク監視

- 本監視テンプレートでは環境に応じてインスタンス設定を必要としている項目があります。以下の設定を行ってください。
  - "/dev/sda IO 要求 (/min)"：
    デバイス名を指定してください。
  - "/dev/sda1 ディスク空き容量率監視 (%)"：
    デバイス名を指定してください。
  - "UUID 指定によるディスク容量監視"グループ内の各監視項目：
    UUID を取得し、各監視設定に設定した後に監視項目を有効化してください。
- 本監視テンプレートでは既定でRHEL環境向けの監視項目が有効になっています。Ubuntu環境ではテンプレート適用後に以下の設定を行ってください。
  - RHEL環境向けの監視項目を無効化、または削除する。
  - Ubuntu環境向けの監視項目を有効化する。

13. Linux 基本

Linux ディスク監視

- 環境に応じて監視対象を変更してください。

Linux テキストログ監視

- 本監視テンプレートでは既定でRHEL環境向けの監視項目が有効になっています。Ubuntu環境ではテンプレート適用後に以下の設定を行ってください。
  - RHEL環境向けの監視項目を無効化、または削除する。
  - Ubuntu環境向けの監視項目を有効化する。

Linux UUIDディスク監視

- 本監視テンプレートは各監視項目の設定を編集してから使用します。以下の設定を行ってください。
  - "UUID 指定によるディスク容量監視"グループ内の各監視項目：
    監視するディスクボリュームの UUID を取得し、各監視項目に設定した後に監視項目を有効化してください。

14. Linux アプリケーション

Linux Apache サーバー監視

- 本監視テンプレートでは既定でRHEL環境向けの監視項目が有効になっています。Ubuntu環境ではテンプレート適用後に以下の設定を行ってください。
  - RHEL環境向けの監視項目を無効化、または削除する。
  - Ubuntu環境向けの監視項目を有効化する。

Linux Postfix 監視

- 本監視テンプレートでは既定でRHEL環境向けの監視項目が有効になっています。Ubuntu環境ではテンプレート適用後に以下の設定を行ってください。
  - RHEL環境向けの監視項目を無効化、または削除する。
  - Ubuntu環境向けの監視項目を有効化する。

Linux NFS 監視

- 監視項目「NIS rpc.yppasswd 起動状況」は既定で無効となっています。監視を実行する際は有効化してください。
- 監視項目「NIS ypserv 起動状況 (RHEL)」および「NIS ypbind 起動状況 (Ubuntu)」は既定で無効となっています。監視を実行する際は、監視対象のOSに合わせて有効化してください。

Linux DHCP サーバー監視

- Red Hat Enterprise Linux 10より前のDHCPサーバーを監視する場合は、「dhcpd プロセス起動状況」監視を使用してください。
- Red Hat Enterprise Linux 10以降の環境で、Kea DHCPサーバーを使用している場合は、「Kea dhcp プロセス起動状況」監視を使用してください。

15. VMware 標準構成テンプレート

個別注意事項のある監視テンプレートはありません。

初版：2022年6月15日

改版：2026年3月31日

作成：セイ・テクノロジーズ株式会社