

VERITAS™

Veritas NetBackup 10.3

異常検出構成ガイド

ベリタステクノロジーズ合同会社

Veritas テクニカルガイド

免責事項

- ベリタステクノロジーズは、この文書の著作権を留保します。また、記載された内容の無謬性を保証しません。
- 当ガイドは代表的な構成方法や操作の一般的な手順をご紹介することを目的としています。
- 機能の全ての範囲を網羅した説明を行うものではありません。詳細な情報は、製品マニュアルを参照ください。
- NetBackupは将来に渡って仕様を変更する可能性を常に含み、これらは予告なく行われることもあります。
- なお、当ドキュメントの内容は参考資料として、読者の責任において管理/配布されるようお願いいたします。

当資料の コンテンツ

1. 異常検出の概要
2. 異常検出の設定手順
3. 異常検出の通知
4. 参考情報

1. 異常検出の概要

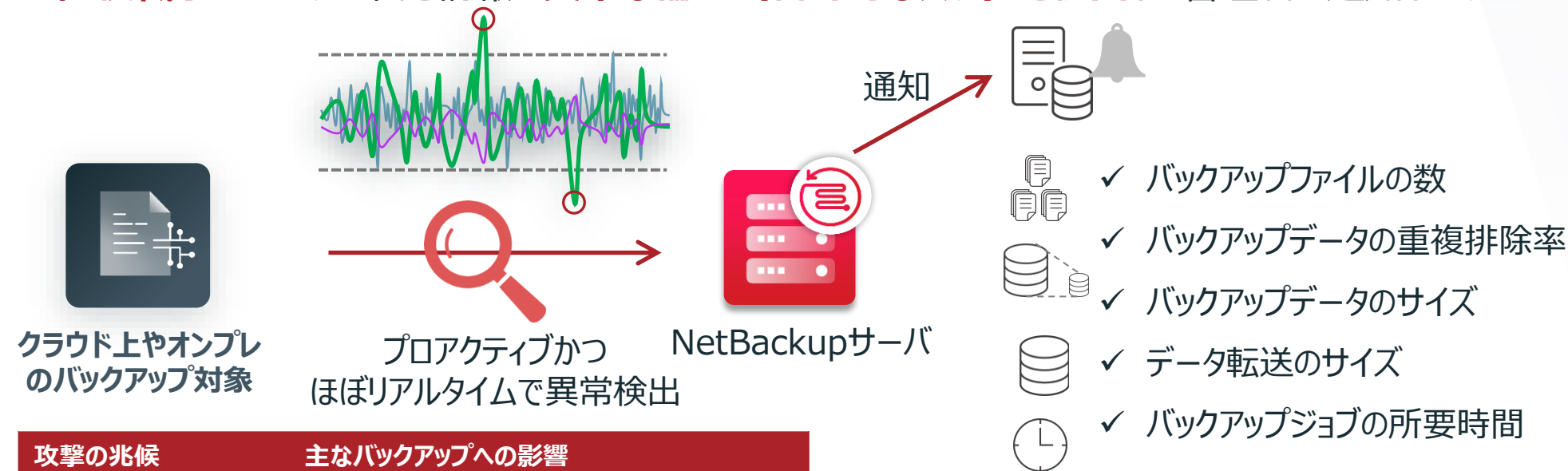
1. 異常検出の概要

1-1 ランサムウェアに対抗するAIによる異常検出とは

ランサムウェアの攻撃による被害拡大を防止する、異常検出による攻撃の早期検出

NetBackupは、ほぼリアルタイムでバックアップ実行時の異常を検出できます。

AI／機械学習により、下記情報の異常な偏差（統計的なズレ）を検出し、管理者に通知します。



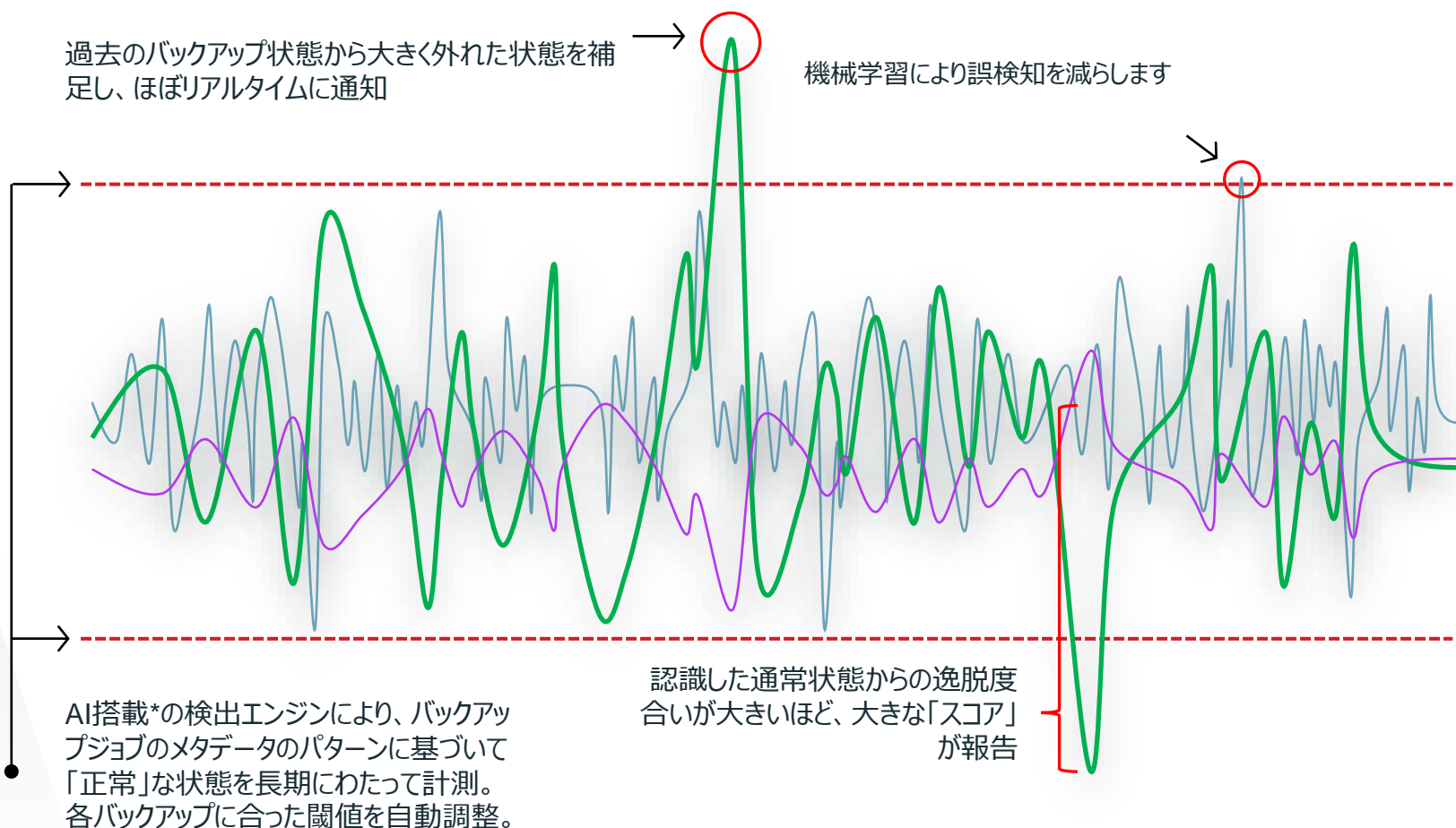
攻撃の兆候	主なバックアップへの影響
ファイルの暗号化	バックアップ時の重複排除率が低下
ファイル名の変更	バックアップされるファイル数が増加
ファイルの削除	バックアップされるファイル数やサイズが減少
新しい拡張子の追加	バックアップされるファイル数やサイズが増加

バックアップの状況から被害の可能性を検出
あらゆるデータを保護できるNetBackupにより、
統合的なチェックが可能

1. 異常検出の概要

1-1 ランサムウェアに対抗するAIによる異常検出とは

バックアップ時の異常をAI/機械学習にて検出、お知らせ



NetBackupに搭載したAIアルゴリズムで異常検出

- 過去の実績から正常パターンを解析
- 自動モニタリング&レポート
- 複数の基準に基づいたレポート
- 攻撃に対する早期の対処

* AIはDBSCANアルゴリズムによって実現されています。

1. 異常検出の概要

1-1 ランサムウェアに対抗するAIによる異常検出とは

バックアップ時の異常の検出動作について

■ 「異常」の基準

バックアップポリシー × クライアント × スケジュール

* この単位ごとに **ベースライン** を構成します。

フル、増分、差分

最低30回分のジョブを観測

* 近いデータを集めてクラスタを形成

* クラスタは14日ごとに調整

■ 検出の動作

1. バックアップを取得

2. メタデータ（カタログ情報）を収集

* 異常検出用の内部データベースで管理します。

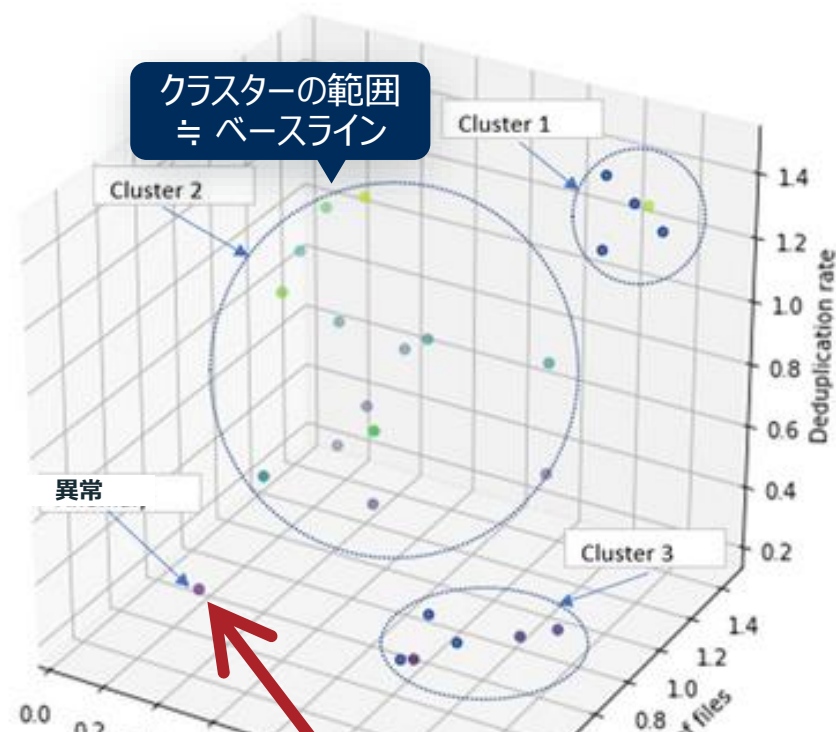
3. ベースラインと比較

* デフォルト設定では15分間隔です。

* クラスタからの逸脱具合によって、リスクスコアを算出します。

* リスクスコアの数値により、重大度を判定します。

4. 通知（Web UI、Syslog、外部監視システム）



どのクラスタからも離れているもの、これを「異常」として検出します。

* この例では、重複排除率、ファイル数、イメージサイズによりグラフ化しています。

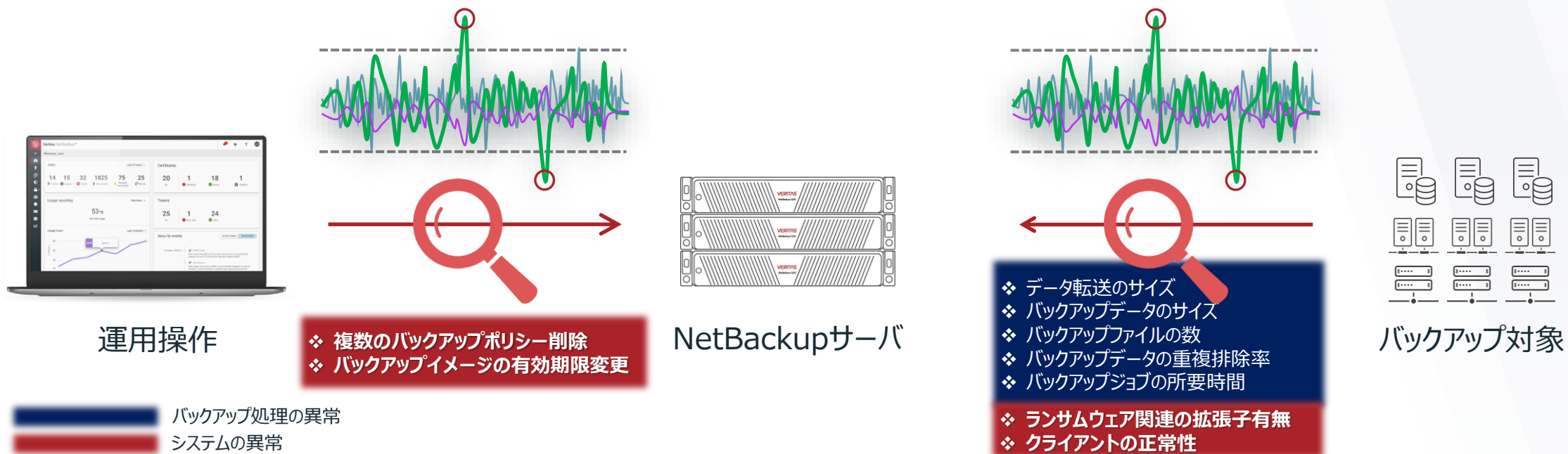
(参考) Backup Anomaly detection in NetBackup

<https://vox.veritas.com/t5/NetBackup/Backup-Anomaly-detection-in-NetBackup/td-p/895002>

1. 異常検出の概要

1-2 そのほかの異常検出

システムへの異常なアクションの検出機能（V10.3より）



バックアップ時の異常検出に加えて、バックアップシステムへの異常なアクションを早期に検出し、通知することができます。

1. 異常検出の概要

1-2 そのほかの異常検出

システムへの異常なアクションの検出機能（続き）

ルールに基づく異常検出機能（V10.3より）

各ルールに該当することが検出された際に、メッセージにはそれぞれこちらの重大度にて通知されます。

ルール名	説明	重大度
Storage configuration deleted ストレージ構成の削除	Detects if storage unit, disk pool or storage server is deleted. ストレージユニット、ディスクプール、またはストレージサーバーが削除されたかどうかを検出します。	高
SLP copy operation modified / removed SLPのコピー操作を変更または削除	Detects if an SLP replication or duplication is deleted in the given timeframe. SLPのコピー操作を変更または削除されたかどうかを検出します。	中
Reissue token detected 再発行トークンの検出	Detects token reissued in the given timeframe. 再発行されたトークンを検出します。	中
Multiple policies deleted or deactivated by user ユーザーによる複数ポリシーの削除または無効化	Detects if multiple policies are deleted or deactivated in the given timeframe. 指定された時間枠内に複数のポリシーが削除または無効化されたかどうかを検出します。	中
Multiple SLPs deleted or deactivated by user ユーザーによる複数SLPの削除または無効化	Detects if multiple SLPs are deleted or deactivated. 複数のSLPが削除されたか、無効化されたかを検出します。	中
Disk pool brought down by user ユーザーによるディスクプールのダウン	Detects if the disk pool state is changed to 'DOWN'. ディスクプールの状態が「DOWN」に変更されたかどうかを検出します。	中
Clients removed from the policy ポリシーの設定（クライアント）から設定を削除	One or more clients are removed from the policy 1つ以上のクライアントがポリシーから削除されたかどうかを検出します。	高
Backup coverage is reduced ポリシーの設定（バックアップ対象）から設定を削除	One or more file list or directories are removed from backup selection. 1つまたは複数のファイルリストまたはディレクトリがバックアップの選択から削除されたかどうかを検出します。	高

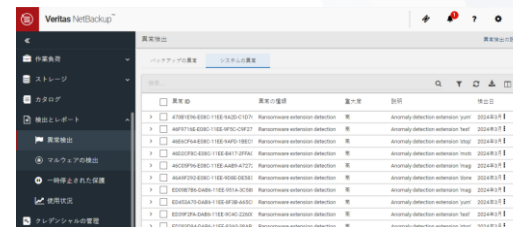
- ルールを登録し、そのルールに該当するふるまいが検出された場合には異常として検出、通知します。
- ルールはベリタスの[ダウンロードセンター](#)からダウンロードし、NetBackupに登録します。

1. 異常検出の概要

1-3 異常検出からの通知

異常検出後の通知について

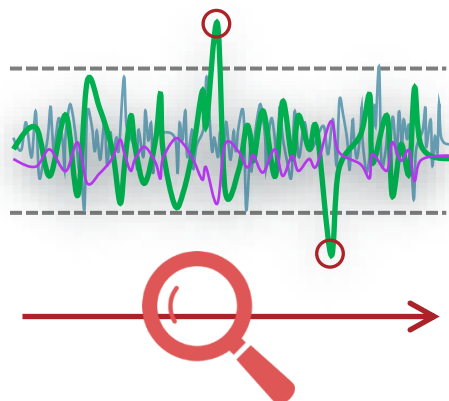
Web UI上での表示
(デフォルトで表示)



異常ID	異常の種類	発生時刻	検出	発生時刻
47826784-68611EE-A42D-11E9	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00
48071148-68611EE-9F5C-C9F2	Retention extension detection	2024/11/11 10:00:00	異常検出	2024/11/11 10:00:00



クラウド上やオンプレ
のバックアップ対象



NetBackupサーバ

通知

監査イベントとして
シスログへ書き込み



SIEM/SOARといった統合セキュ
リティ監視システムへのログ転送



設定方法は
当ガイド内に
後述します。

異常が検出された結果、3つの方法で通知を行うことが可能です。

1. 異常検出の概要

1-4 異常検出を行うメリット

バックアップから異常を早期検出することのメリット

異常に気付かず、
バックアップ保持世代を過ぎると、
正常なデータが無くなってしまふ



データの異常を早期に検出

=> バックアップをすぐに停止

=> 正常な過去のバックアップデータを多く確保

=> 正常なバックアップから復旧が可能！



- あらゆる場所のあらゆるデータのバックアップの異常を検出可能であり、バックアップデータを確実に保護
- **当機能の利用にあたっては新たな仕組みや特別なライセンスを導入しなくても、異常の検出は可能！**

1.異常検出の概要

1-5 NetBackupの異常検出の特徴

NetBackupの異常検出機能の特徴



ほぼリアルタイムな検出が可能のため、早期の検出を実現し、攻撃の影響を低減



異常検出を利用するための特別な追加ライセンスは不要であり、コストメリット大！



あらゆるワークロードのバックアップから異常検出が可能であり、スケジュールが異なっても（フル、増分）異常検出は可能！



AI/機械学習エンジンは内蔵しており、インターネット接続のないオフライン環境での利用も可能！

1. 異常検出の概要

1-6 システム構成

異常検出機能利用時のシステム構成について

- 異常検出機能がサポートされるNetBackupはV9.1以上
 - 当ガイドではV10.3.0.1にて実装されている機能を前提に内容を記載します。
 - 各バージョンに実装されている機能は、「セキュリティおよび暗号化ガイド」を参照ください。
- デフォルトではプライマリサーバーのみで稼働（デフォルトでは未稼働）、設定変更によってメディアサーバーで稼働させることも可能
 - 当ガイドではプライマリサーバーにて稼働させる手順にてご紹介します。
 - メディアサーバーで稼働させる場合は[こちらのマニュアル](#)をご参照ください。
- 検出の動作によるシステム負荷も小さいため、特別なサーバーリソースの追加は不要
- プライマリサーバー、メディアサーバーがサポートされるプラットフォームをすべてサポート（詳細は[こちらのコンパチビリティリスト](#)を参照）、検出可能なワークロードも特別な制限はなし

2. 異常検出の設定手順

2-1. バックアップ時の異常検出の設定

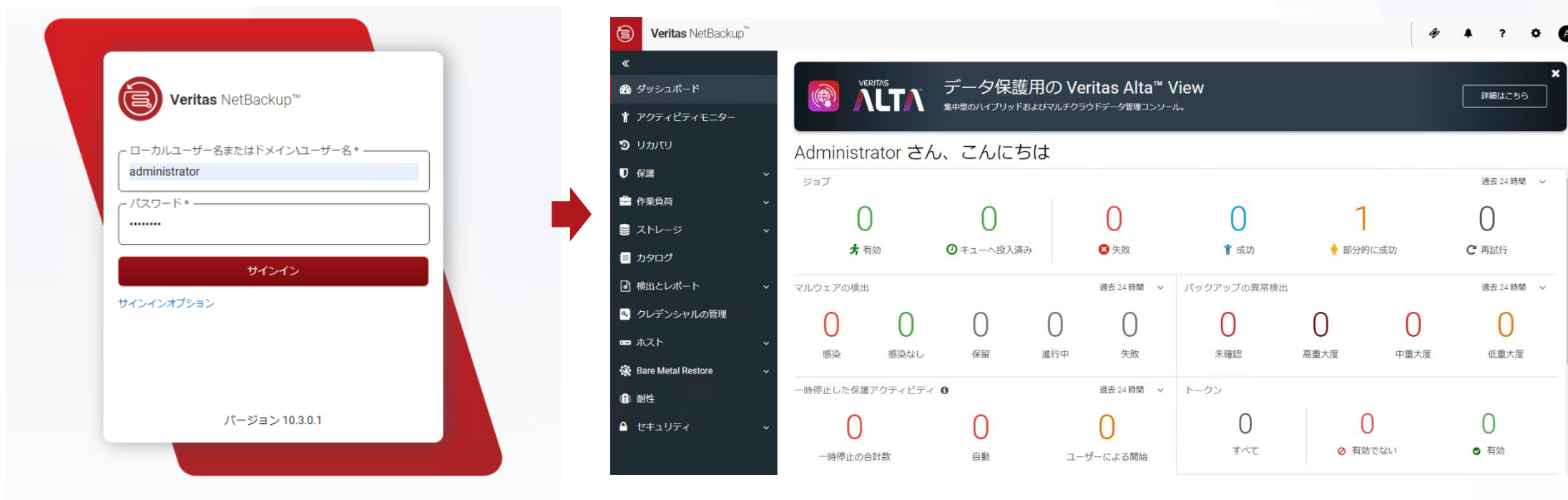
2-2. システムへの異常なアクションの検出の設定

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出の開始

- NetBackup Web UI へ接続します

- ① ブラウザから「https://プライマリサーバ名/webui」を指定し、Web UIのログイン画面を表示します。
- ② 管理者のアカウント情報を入力してサインインを行います

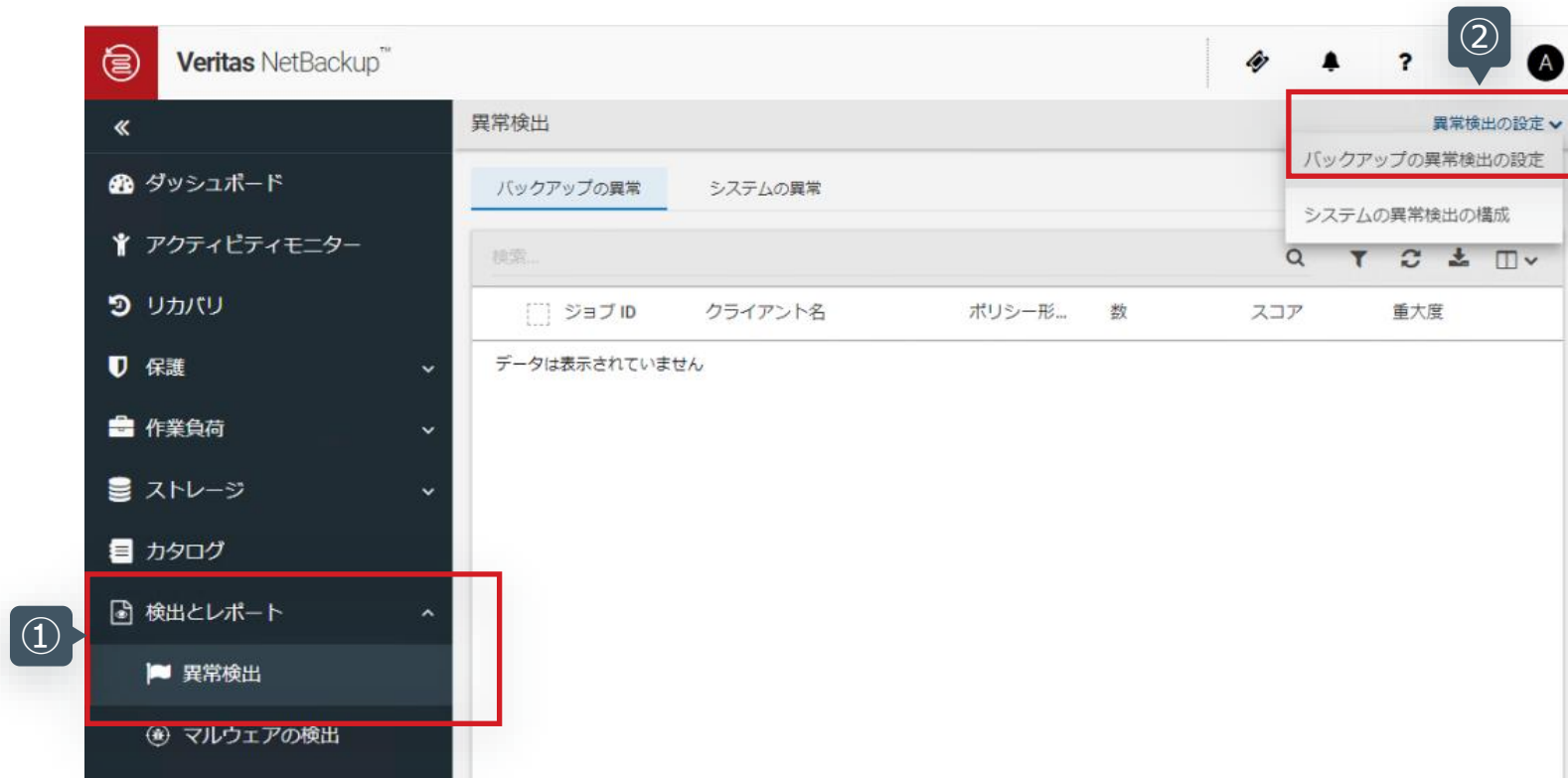


2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出の開始

- 異常検出の設定画面を表示します。

- ① 左メニューの「検出とレポート」 > 「異常検出」 をクリックします。
- ② 「異常検出の設定」 > 「バックアップの異常検出の設定」 をクリックします。



2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出の開始

- バックアップ時の異常検出の設定を変更、保存します。

- 「異常検出アクティビティを有効にする」の編集ボタンをクリックします。
- 「異常データの収集、検出サービス、イベントを有効にする」をチェックし、保存ボタンをクリックします。

バックアップの異常検出の設定

異常検出

異常検出アクティビティを有効にする
異常データの収集が有効です。

基本設定

異常検出の感度
0

データ保持の設定
12 カ月

データ収集の設定
間隔: 15 分

異常検出を有効にする

すべて無効にする
異常データの収集を有効にする
異常データの収集と検出サービスを有効にする
異常データの収集、検出サービス、イベントを有効にする

キャンセル 保存

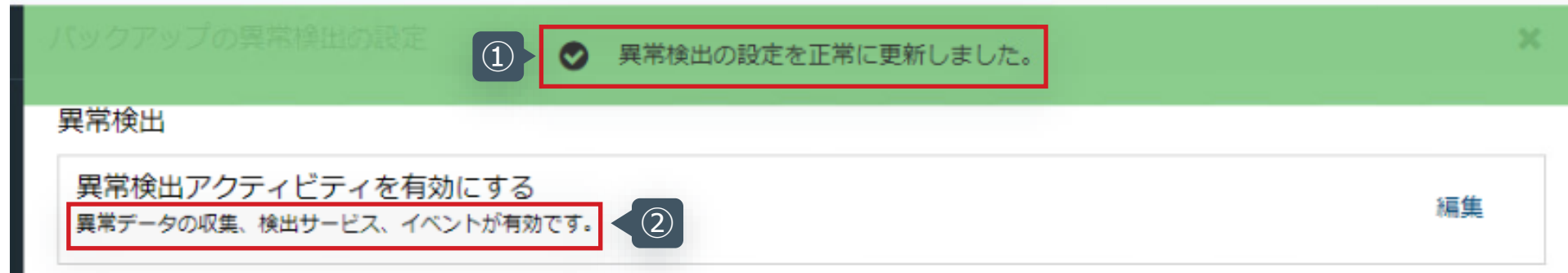
設定	NetBackupの動作
すべて無効にする	-
異常データの収集を有効にする	異常検出データベースへのデータ蓄積を行います * デフォルトの設定はこちらです。
異常データの収集と検出サービスを有効にする	異常検出データベースの情報をもとに異常検出を行います * ログを覗くと、検出結果が確認できます。
異常データの検出、検出サービス、イベントを有効にする	検出された異常を通知します * Web UIの表示やシスログ連携を行う場合はこちらです。

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出の開始

- バックアップ時の異常検出の開始を確認します。

- ① 「異常検出の設定を正常に更新しました」と表示されたメッセージを確認します。
- ② 「異常データの収集、検出サービス、イベントが有効です。」への表示の変更を確認します。



以上の手順で、バックアップ時の異常検出は開始されます。
以降のスライドでは運用中のパラメータ調整等について記載します。

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出時のログ用フォルダーの作成

- 異常検出時のログの書き込み用フォルダを作成します。
- ログの出力先は以下になります。

OS	出力先
Windows	C:¥Program Files¥Veritas¥NetBackup¥logs¥nbanomalydetect
Linux	/usr/opensv/netbackup/logs/nbanomalydetect/

* ログの出力を行うには、事前に「nbanomalydetect」フォルダを作成しておく必要があります。（mklogdir でも作成されます）

（例）Linux環境の場合

```
[root@nbu1011-lin ~]# ls /usr/opensv/netbackup/logs/nbanomalydetect/
SERVICE_USER.011723_00001.log SERVICE_USER.012023_00001.log
SERVICE_USER.013023_00001.log
SERVICE_USER.011823_00001.log SERVICE_USER.012323_00001.log
SERVICE_USER.013123_00001.log
SERVICE_USER.011923_00001.log SERVICE_USER.012523_00001.log
[root@nbu1011-lin ~]#
```

* ログは1日ごとにローテーションされます。

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出のパラメータ調整

- 必要に応じて検出のパラメータ「基本設定」を変更します(通常はデフォルトで運用可)。

- ① 「基本設定」の編集ボタンをクリックします。
- ② 必要に応じてパラメータを変更し、最後に保存をクリックします。

バックアップの異常検出の設定

異常検出

異常検出アクティビティを有効にする
異常データの収集、検出サービス、イベントが有効です。

編集

基本設定

異常検出の感度
0

データ保持の設定
12 か月

データ収集の設定
間隔: 15 分

異常プロキシサーバーの設定



基本設定

異常検出の感度
この設定を使用して異常検出の感度を調整します。

異常イベントの数が
増えます。 異常イベントの数が
減ります。

低 中 高

データ保持の設定
この設定を使用してデータベースの情報を保持する期間を指定します。

12 月 間

データ収集の設定
この設定を使用してデータ収集をトリガする間隔を指定します。

間隔 15 分 間

異常プロキシサーバーの設定
この設定を使用して、異常を処理する NetBackup メディアサーバーを指定します。指定しない場合、処理はプライマリサーバーで実行されます。

異常プロキシサーバー名
ホストの入力
メディアサーバー名を入力してください。

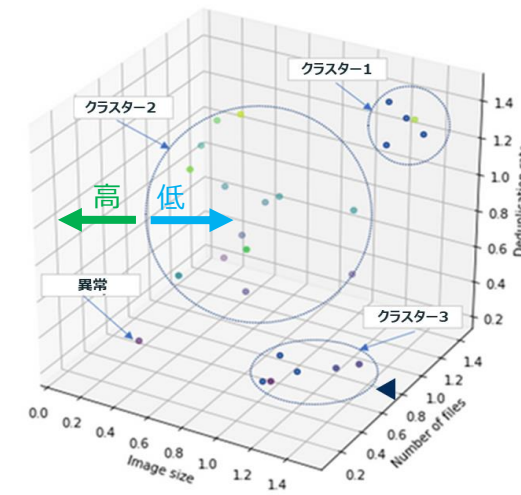
キャンセル 保存

以降のスライドで
パラメータについて
説明します。

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出のパラメータ調整

- 検出の基本設定のパラメータの内容は以下のとおりです。



基本設定

異常検出の感度
この設定を使用して異常検出の感度を調整します。

異常イベントの数が増えます。 異常イベントの数が減ります。

低 中 高

データ保持の設定
この設定を使用してデータベースの情報を保持する期間を指定します。

12 月間

データ収集の設定
この設定を使用してデータ収集をトリガする間隔を指定します。

間隔 15 分間

異常プロキシサーバーの設定
この設定を使用して、異常を処理する NetBackup メディアサーバーを指定します。指定しない場合、処理はプライマリサーバーで実行されます。

異常プロキシサーバー名

ホストの入力

メディアサーバー名を入力してください。

❖ 異常検出の感度

クラスターの境界幅を調整し、「異常」判定の範囲を設定します。

低：クラスターの境界が狭くなります ➡ 検出イベントの増加

高：クラスターの境界が広がります ➡ 検出イベントの減少

❖ データ保持の設定

異常検出用のデータベースに対する、データの保持期間が調整できます。デフォルトは12か月。1か月～12か月で調整できますが、基本的に変更は不要です。

❖ データ収集の設定

データ収集を実施する間隔(検出間隔)が調整できます。デフォルトは15分。15分～120分で設定は可能ですが、基本的に変更は不要です。

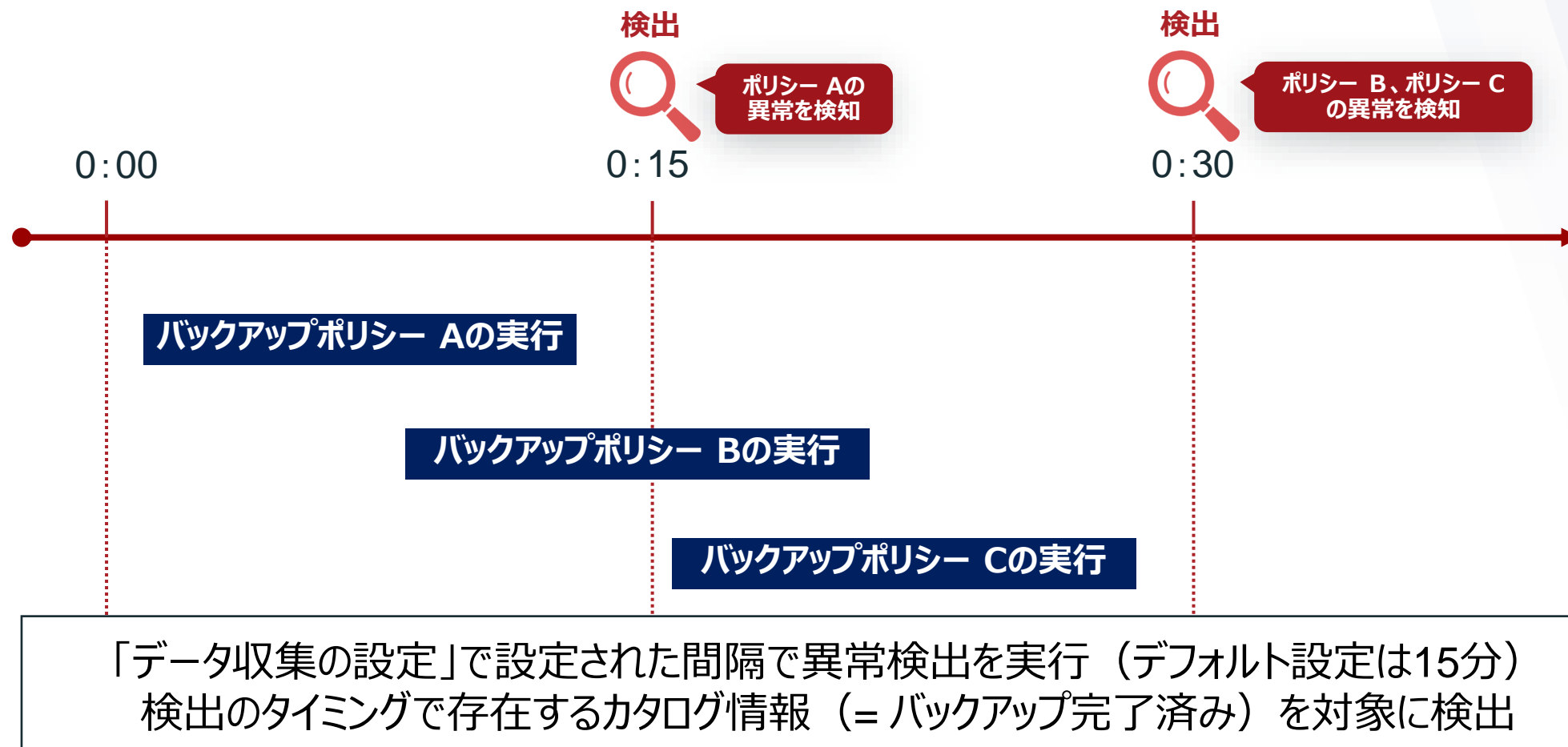
❖ 異常プロキシサーバーの設定

メディアサーバで異常検知の処理を行うことができます。デフォルトはプライマリサーバ。プライマリサーバの負荷が気になる環境で調整します。

2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出のパラメータ調整

- 検出の基本設定のパラメータの内容は以下のとおりです。



2. 異常検出の設定手順

2-1 バックアップ時の異常検出の設定：異常検出のパラメータ調整

- 必要に応じて検出のパラメータ「詳細設定」を変更します(通常はデフォルトで運用)。

① 「詳細設定」の編集ボタンをクリックし、必要に応じて**検出対象から除外したい対象を選択**し、最後に保存をクリックします。

The image illustrates the configuration steps for anomaly detection in Veritas backup software. It shows three main panels:

- 詳細設定 (Detailed Settings):** A panel with two sections. The first section, 'クライアントの異常設定を無効にする' (Disable anomaly detection for clients), has a red box around the '編集' (Edit) button. The second section, '機械学習でポリシー形式または特定の機能を無効にする' (Disable policy format or specific functions with machine learning), also has a red box around its '編集' (Edit) button.
- クライアントの異常設定を無効にする (Disable anomaly detection for clients):** A dialog box with a search field for 'クライアント名' (Client name) and a '検索' (Search) button. Below is a table of clients. A red box highlights the 'リストに追加' (Add to list) button for the client 'nbusvrw06'. A blue callout bubble points to this button with the text: '除外したいクライアントがあればリストから選択' (Select from the list if there are clients to be excluded).
- 機械学習でポリシー形式または特定の機能を無効にする (Disable policy format or specific functions with machine learning):** A dialog box with a search field and a table of policy formats. A red box highlights the 'Standard' row. A blue callout bubble points to this row with the text: '除外したい特定のポリシーや特定の観点があれば選択' (Select if there are specific policies or specific viewpoints to be excluded).

At the bottom right, there are 'キャンセル' (Cancel) and '保存' (Save) buttons.

2. 異常検出の設定手順

2-1. バックアップ時の異常検出の設定

2-2. システムへの異常なアクションの検出の設定

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「システムの異常検出」について

異常なアクションの検出「システムの異常検出」について

ここでは以下の2つの異常検出「システムの異常検出」の設定方法について手順を説明します。

❖ 「疑わしいエラーコードがあり、オフラインのクライアントを検出する」について

NetBackupのバックアップ対象がサイバー攻撃によって暗号化され、バックアップ時に疑わしい状況でオフラインになっている場合に異常であることを通知します。

※ベリタスの専用ラボにおけるランサムウェア攻撃のシミュレーションの結果から、ランサムウェアからの攻撃を受けたクライアントのバックアップを実行すると特定のステータスで失敗終了することがわかっており、特定のステータスコードやクライアントのオフラインの状態等から判断をして、攻撃が発生しているうたがいがあることを通知します。

❖ 「イメージの有効期限操作の異常を検出する」について

一定期間に行われた有効期限切れや変更の回数を機械学習し、ユーザーごとの正常な行動を形成しながら、通常にはないバックアップイメージの有効期限切れや変更が行われた場合には異常と判断し、通知します。

※例えば、この検出を有効化した後にバックアップを取得し、カタログから10～15個のバックアップイメージを有効期限切れにすると、期限切れの異常として通知されます。

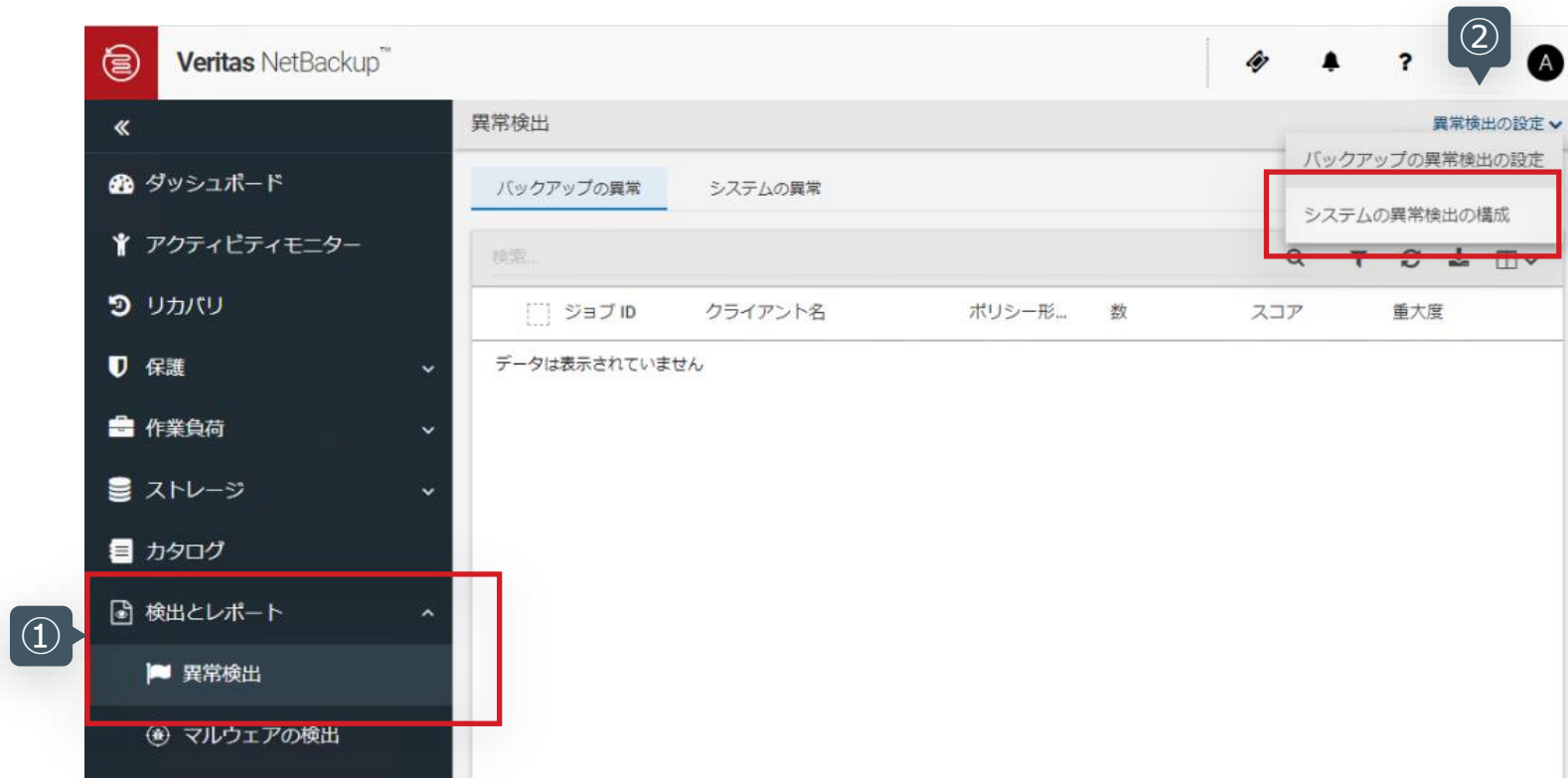
2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「システムの異常検出」の開始

- 異常検出の設定画面を表示します。

① 左メニューの「検出とレポート」 > 「異常検出」をクリックします。

② 「異常検出の設定」 > 「システムの異常検出の構成」をクリックします。



2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「システムの異常検出」の開始

- システムの異常検出の構成を変更します。

- ① 「システムの異常検出」 のダウンボタンをクリックします。
- ② 「疑わしいエラーコードがあり・・・」 と 「イメージの有効期限操作の異常を検出する」 をチェックします。
- ③ 編集ボタンをクリックします。



②の選択は、どちらか必要な検出の一方のチェックをするだけでも特に問題ありません。

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「システムの異常検出」の開始

- システムの異常検出の構成を有効化します。
 - ① 必要に応じて「NetBackupがイメージの有効期限の」をチェックします。
 - ② 保存ボタンをクリックします。

システムの異常検出の構成

システムの異常検出 2/2 のオプションが有効です

- 疑わしいエラーコードがあり、オフラインのクライアントを検出する ⓘ
NetBackup によって、クライアントが疑わしい状態でオフラインになっていることが検出された場合に、異常アラートを生成します。
- イメージの有効期限操作の異常を検出する ⓘ
イメージの有効期限に関して通常と異なる活動が発生したときに異常を生成します。
- NetBackup がイメージの有効期限の異常を検出した場合に、マルチパーソン認証を有効にする ⓘ
マルチパーソン認証では、「デフォルトのマルチパーソン認証 (MPA) の承認者」の役割を持つ2人目のユーザーが要求された操作を先に承認することが求められます。NetBackup CLI および NetBackup 管理コンソールは MPA を使用する操作には使用できません。

データを保持する週数 *
52

現在のデータ内の異常を検出するために過去のデータを保持する週数。30 ~ 52 の範囲内の値を選択してください。

キャンセル 保存

❖ 「NetBackupがイメージの有効期限の異常を検出した場合にマルチパーソン認証を有効にする」をチェックするケース

このチェックボタンをチェックすると、日常みられないような異常なバックアップイメージの有効期限の変更を検出した場合、2人目のユーザーが認証しないと変更が実施できないように指定を変更します。デフォルトはOffです。

マルチパーソン認証については、以下のドキュメントをご参照ください。

[NetBackup™ セキュリティおよび暗号化ガイド](#)

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「システムの異常検出」の開始

- システムの異常検出の構成の画面を確認します。

① 以下の画面の状態になっていることを確認します。

システムの異常検出の構成

システムの異常検出 2/2 のオプションが有効です

- 疑わしいエラーコードがあり、オフラインのクライアントを検出する
NetBackup によって、クライアントが疑わしい状態でオフラインになっていることが検出された場合に、異常アラートを生成します。
- イメージの有効期限操作の異常を検出する
イメージの有効期限に関して通常と異なる活動が発生したときに異常を生成します。
✔ NetBackup がイメージの有効期限の異常を検出した場合に、マルチパーソン認証を有効にする

データを保持する週数 52 編集

ルールに基づく異常検出

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」について

異常なアクションの検出「ルールに基づく異常検出」について

ここでは以下の「ルールに基づく異常検出」の設定方法について手順を説明します。

❖ NetBackup 異常検出ルールを使用して異常を検出

シンプルなルールを登録し、そのルールに設定した特定のしきい値を超えたら異常として通知します。そのルールはJSON形式のフォーマットでベリタスのダウンロードセンターからダウンロードして入手し、そのルールファイルをWeb UIからアップロードおよび有効化することが可能です。

なお、ルールファイルのダウンロードは以下のベリタスのダウンロードサイトから可能です。ダウンロードするためにはユーザー登録が必要ですが、ログインのためのユーザーIDが分からない場合には、ライセンスの販売窓口にお問合せください。

Veritasダウンロードセンター NetBackup V10.3のダウンロード

https://www.veritas.com/support/ja_JP/downloads/detail.REL135241#item2

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」の開始

- ダウンロードセンターにアクセスし、ルールファイルをダウンロードします。

- ① ブラウザにて[ダウンロードセンター](#)にアクセス、ログインし、検索欄に「rule」と入力します。
- ② 抽出された「NetBackup_Rule_Engine_1.0_0007.zip」を選択します。
- ③ 画面右上の「ダウンロード」をクリックし、ファイルをダウンロードします。



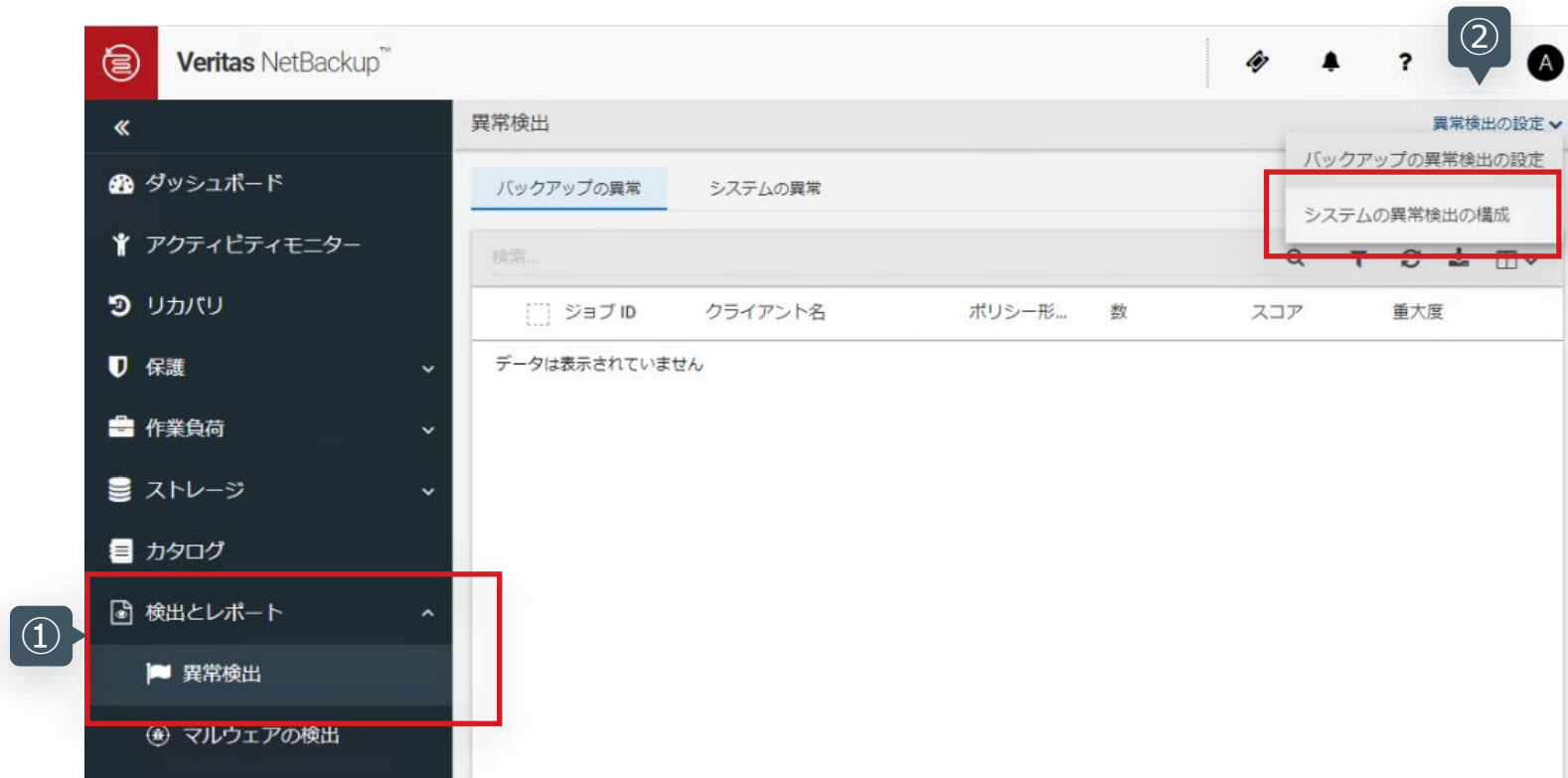
※ダウンロードしたファイルはZip形式になっていますので、ダウンロード後にZipを解凍しておいてください。

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」の開始

- 異常検出の設定画面を表示します。

- ① 左メニューの「検出とレポート」 > 「異常検出」 をクリックします。
- ② 「異常検出の設定」 > 「システムの異常検出の構成」 をクリックします。



2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」の開始

- **ルールに基づく異常検出の設定をします。**

- ① 「ルールに基づく異常検出」 のダウンボタンをクリックします。
- ② 「ルールをアップロードする」 をクリックします。



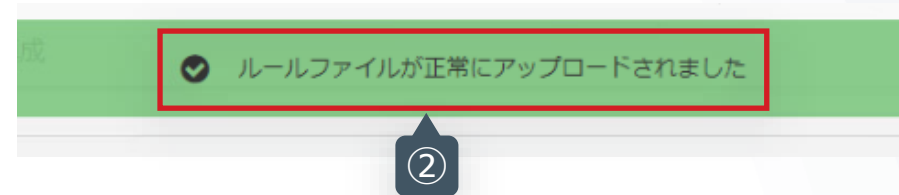
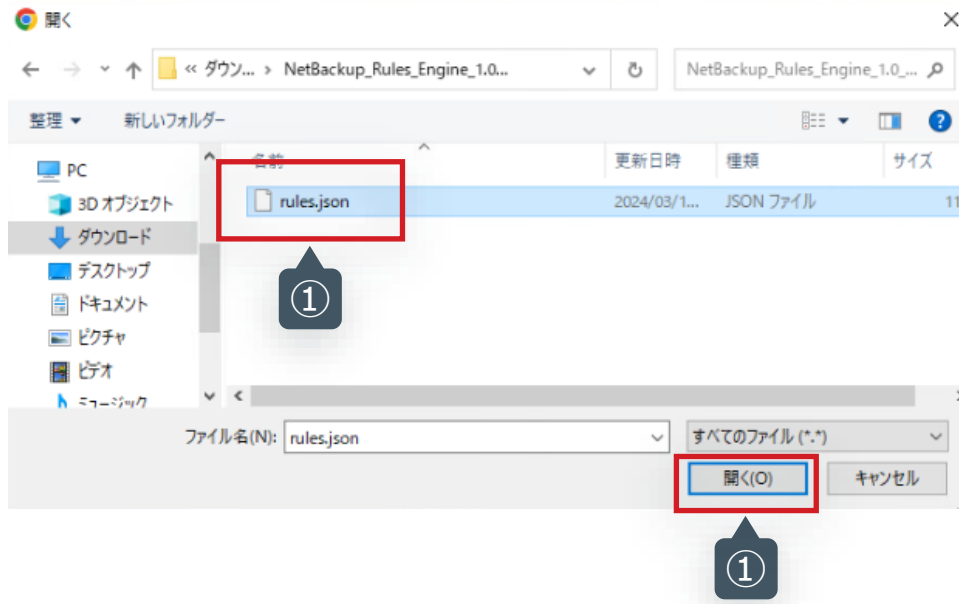
2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」の開始

- ルールファイルをアップロードします。

① 「rule.json」 を選択し、開くをクリックします。

② ルールが登録され、「ルールファイルが正常にアップロードされました」と表示されたメッセージを確認します。



2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：「ルールに基づく異常検出」の開始

• アップロードされたルールを有効化します。

- ① 「NetBackup異常検出ルールを使用して異常を検出します」 をチェックします。
- ② 設定したいルールを選択し、有効化をクリックします。
- ③ 表示されたメッセージを確認し、該当のルールが有効化されたことを確認します。

The screenshot shows the 'ルールに基づく異常検出' (Anomaly Detection Based on Rules) configuration page. The top status bar indicates '1/8 のルールが有効です' (1 of 8 rules are active). A red box highlights the checkbox for 'NetBackup 異常検出ルールを使用して異常を検出します' (Use NetBackup anomaly detection rules to detect anomalies), which is checked. Below this is a table of 8 rules, all of which are selected. A red box highlights the '有効化' (Activate) button. A red arrow points to a green notification box that says '状態を正常に変更しました' (Status changed to normal). Below that, a grey notification box shows '8/8 のルールが有効です' (8 of 8 rules are active).

ルール名	説明	重大度	バージョン
Rule: Storage configuration delet...	Detects if storage unit, disk pool or storage ...	高	1
Rule: Disk pool brought down by ...	Detects if the disk pool state is changed to '...	中	1
Rule: SLP copy operation modifie...	Detects if an SLP replication or duplication I...	中	1
Rule: Multiple policies deleted or ...	Detects if multiple policies are deleted or de...	中	1
Rule: Backup coverage is reduced	One or more file list or directories are remov...	高	1
Rule: Clients removed from the p...	One or more clients are removed from the p...	高	1
Rule: Reissue token detected	Detects token reissued in the given timefra...	中	1
Rule: Multiple SLPs deleted or de...	Detects if multiple SLPs are deleted or deac...	中	1

有効化したルールが表示されます。

- デフォルトで、「Multiple policies deleted or deactivated by user」は有効化されています。
- ダウンロードしたルールの内容については、P9を参照してください

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：デフォルトで有効化されている異常検出

デフォルトで有効化されている異常検出について①

NetBackupインストール後にデフォルトで有効化されている2つの異常検出について説明します。

❖ バックアップ対象に含まれるランサムウェアに関連する拡張子を持つファイルの検出

- あらかじめランサムウェアに関連するファイルの拡張子と登録されている拡張子を持つファイルがバックアップ対象に含まれていた場合、異常として検出、通知します。
- 当異常検出はデフォルトで有効化されています。
- バックアップ実行後にファイル名を解析し、以下のファイル内に指定されている拡張子を持つファイルが含まれている場合に通知されます。
 - Linux : /usr/opensv/var/global/extensions.txt
 - Windows: c:¥Program Files¥Veritas¥NetBackup¥var¥global¥extensions.txt

2. 異常検出の設定手順

2-2 システムへの異常なアクションの検出の設定：デフォルトで有効化されている異常検出

デフォルトで有効化されている異常検出について②

❖ ユーザーによる複数ポリシーの削除または無効化の検出

- 一定の時間枠内に複数のポリシーが削除または無効化する操作を行った場合、異常として検出、通知します。
- 当検出はルールとしてあらかじめ登録されており、デフォルトで有効化されています。
- デフォルトでは複数のポリシーが10分間に2回削除されたり、変更された場合には、通知されます。

3. 異常検出の通知

3-1. Web UIへの通知

3-2. 監査イベントへの通知とSyslogへの転送

3-3. バックアップ時の異常検出のサンプル

3. 異常検出の通知

3-1 Web UIへの通知

- 検出の結果を確認し、検出動作にフィードバックします。

- ① 左メニューの「検出とレポート」 > 「異常検出」 をクリックします。
- ② 「バックアップの異常」タブか、「システムの異常」タブをクリックします。
- ③ 表示された異常の一覧から、確認したい異常を選択します。

Veritas NetBackup™

異常検出

バックアップの異常 システムの異常

検索...

<input type="checkbox"/>	異常 ID	異常の種類	重大度	説明	格
<input checked="" type="checkbox"/>	> 756447B5-9EC2-4041-9EA5-98D9E	Ransomware extension detection	高	Anomaly detection extension 'stop'	2 ⋮
<input checked="" type="checkbox"/>	> 4225EFD2-7E4E-48F9-953B-29C75	Ransomware extension detection	高	Anomaly detection extension 'yum'	2 ⋮

3. 異常検出の通知

3-1 Web UIへの通知

• 検出の結果を確認し、検出動作にフィードバックします。

- ① 重大度や発生元等の情報を確認します。
- ② 確認結果として、いずれかをクリックします（必須ではありません）。

スコアと異常の重大度

- ❖ クラスタからの逸脱度合いでスコアリング
- ❖ スコアと重大度の関係は以下のとおり

スコア	重大度
10 未満	低
10~15 未満	中
15以上	高

異常値フィードバック機能

検出結果にユーザ判断を加え、フィードバック！

フィードバック	
無視としてマーク	このデータをクラスタの構成データから除外します。 今後の異常検出のデータとしません。
異常として確認	確認状態を「異常」に変更します。 ※表示のみ変更されます。
誤検知として報告	ベースラインの見直しが行われます。 新しいクラスタが作成されるか、 既存のクラスタが再構成されます。

異常検出

バックアップの異常 システムの異常

検索...

異常 ID	異常の種類	重大度	説明	検出日	確認状態
756447B5-9EC2-4041-9EA5-98D9E	Ransomware extension detection	高	Anomaly detection extension 'stop'	2024年3月11日 00:04	未確認

異常の詳細

Backup id: nbusvrw06_1710082932

Client name: nbusvrw06

Details: Anomaly detection extension 'stop' for Ransomware is detected for job ID : 5

Policy name: anomaly_test

Ransomware extension stop

無視としてマーク 異常として確認 誤検知として報告

3. 異常検出の通知

3-1. Web UIへの通知

3-2. 監査イベントへの通知とSyslogへの転送

3-3. バックアップ時の異常検出のサンプル

3. 異常検出の通知

3-2 監査イベントへの通知とSyslogへの転送

● 監査イベントへの通知を確認し、Syslog転送を設定します。

- ① 左メニューの「セキュリティ」 > 「セキュリティイベント」をクリックします。
- ② 「監査イベント」タブをクリックし、表示されたイベントを確認します。
- ③ 「セキュリティイベントの設定」、確認したい異常を選択します。



3. 異常検出の通知

3-2 監査イベントへの通知とSyslogへの転送

- 監査イベントへの通知を確認し、Syslog転送を設定します。

- ① 「監査イベントをシステムログに送信する」 をチェックします。
- ② 「監査イベントカテゴリの選択」ボタンをクリックします。
- ③ 検索欄に「anomaly」と入力し、表示された異常検出に関連するカテゴリをすべて選択し、「保存」をクリックします。

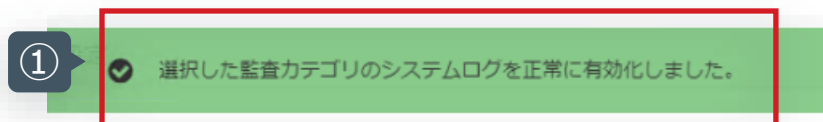


3. 異常検出の通知

3-2 監査イベントへの通知とSyslogへの転送

- 監査イベントへの通知を確認し、Syslog転送を設定します。

- ① 有効化に成功したというメッセージが表示されます。
- ② カテゴリの数値を確認し、選択個数に問題がないことを確認します。



※以下のSyslogに異常検出の監査イベントが転送されます。

OS	通知場所
Windows	Windowsイベントログ
Linux	/var/log/messages

**以上の手順で、監査イベントのSyslog転送の設定は完了です。
これ以降に異常が発生した場合は、Syslogへ転送されます。**

3. 異常検出の通知

3-1. Web UIへの通知

3-2. 監査イベントへの通知とSyslogへの転送

3-3. バックアップ時の異常検出のサンプル

3. 異常検出の通知

3-3 バックアップ時の異常検出のサンプル

• バックアップ時の異常検出を発生させるためのバックアップのシナリオ例

- ◆ NetBackupクライアントが導入されているサーバーのあるフォルダ(約21万ファイル、1.9GB)をバックアップするポリシーを30回、そのまま繰り返して実行
=>この作業にて、異常の基準（ベースライン）が作成されます。
- ◆ バックアップ対象のフォルダー内のファイルを一部削除（約110MBに削減）し、再度バックアップを実行
- ◆ バックアップ時の異常を検出した結果として、以下のように異常検出のWeb UIに表示

The screenshot displays the '異常検出' (Anomaly Detection) section of the NetBackup Web UI. It features a search bar and a table of detected anomalies. The table has columns for Job ID, Client Name, Policy Name, Count, Score, Severity, Summary, Receipt Date, and Confirmation Status. A specific anomaly is highlighted for Job ID 599, Client nbuprimary.lab.local, Policy Standard, with a count of 5 and a score of 10.18. Below the table, there is a section for '異常の詳細' (Anomaly Details) with buttons for '無視としてマーク' (Mark as Ignored), '異常として確認' (Confirm as Anomaly), and '誤検知として報告' (Report as False Positive). At the bottom, there are five summary statistics for the anomaly.

ジョブ ID	クライアント名	ポリシー形...	数	スコア	重大度	概略	受信日 ↓	確認状態
599	nbuprimary.lab.local	Standard	5	10.18	中	Anomaly image size, Backup file...	2024年3月20日 09:52	未確認

ジョブ ID	クライアント名	ポリシー名	ポリシー形式	スケジュール名	スケジュール形式	確認状態
599	nbuprimary.lab.local	Anomaly_Detection	Standard	FULL	FULL	未確認

バックアップ ID	異常 ID	異常の重大度
nbuprimary.lab.local_1710952711	599_1710952711	中

異常の詳細

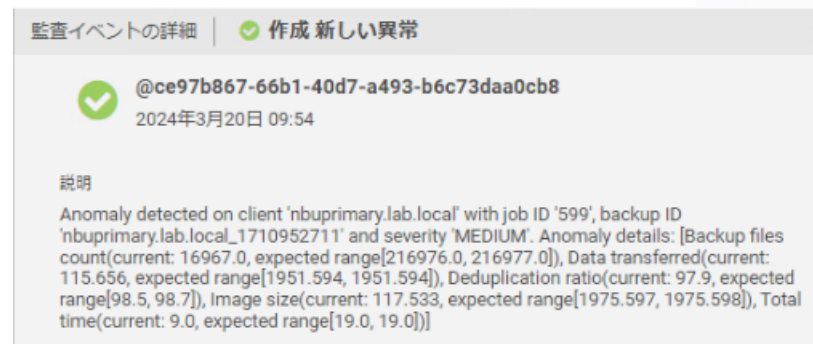
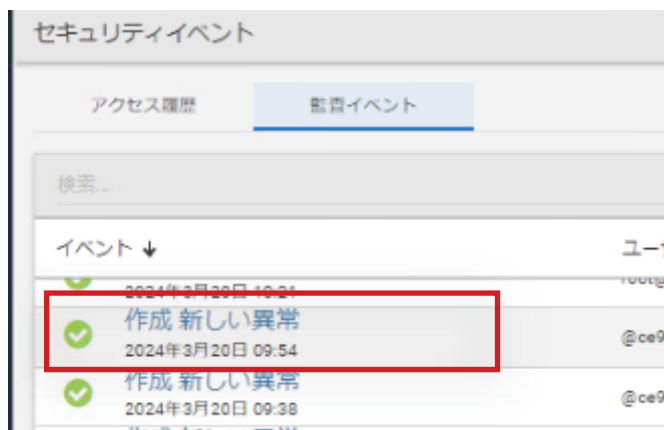
異常: Backup files count 16967 (通常: 216976 - 216977)	異常: Data transferred 115.656 MB (通常: 1951.594 MB - 1951.594 MB)	異常: Deduplication ratio 97.9 % (通常: 98.5 % - 98.7 %)	異常: Image size 117.533 MB (通常: 1975.597 MB - 1975.598 MB)	異常: Total time 9 Seconds (通常: 19 Seconds - 19 Seconds)
---	--	---	--	---

3. 異常検出の通知

3-3 バックアップ時の異常検出のサンプル

- バックアップ時の異常検出結果の監査イベントとSyslog転送結果

- ◆ 監査イベントには以下のように通知され、Syslogへもイベントが転送されます。



↓ Syslog転送結果

★異常検出

```
Mar 20 09:54:39 nbuprimary
nbaudit@nbuprimary.lab.local:application[NetBackup]: DESCRIPTION:
Anomaly detected on client 'nbuprimary.lab.local' with job ID '599',
backup ID 'nbuprimary.lab.local_1710952711' and severity 'MEDIUM'.
Anomaly details: [Backup files count(current: 16967.0, expected
range[216976.0, 216977.0]), Data transferred(current: 115.656,
expected range[1951.594, 1951.594]), Deduplication ratio(current: 97.9,
expected range[98.5, 98.7]), Image size(current: 117.533, expected
range[1975.597, 1975.598]), Total time(current: 9.0, expected
range[19.0, 19.0])]. | TIMESTAMP: 1710953679090 | DATETIME: 2024-03-
20T09:54:39.000-07:00 | USER: @ce97b867-66b1-40d7-a493-b6c73daa0cb8 |
CATEGORY: ANOMALY_NEW | ACTION: CREATE | REASON: | DETAILS: 0
attribute(s)
```

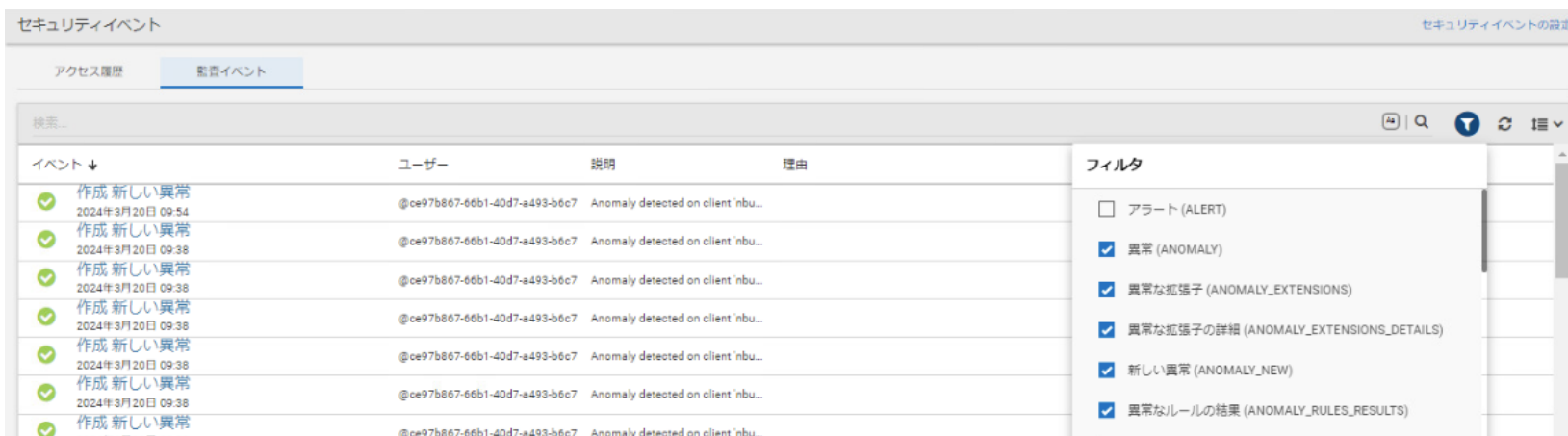
こちらのサンプルのSyslogはRedHatの
/var/log/messagesへの転送結果です。

4. 参考情報

4. 参考情報

4-1 監査イベントについて

監査イベントを確認することで、NetBackup環境でユーザが開始した処理を監査し、いつ誰が何を変更したかを把握できます。NetBackup Web UIより、48種類のカテゴリ（次ページ参照）の監査イベントを確認することができます。



(例) 異常検出

イベント ↓	ユーザー	説明
🔍 アクセス ログイン 2022年11月27日 20:36	user1@nbuprimary.lab.local	User 'user1@nbuprimary.lab.local' is logged out
✅ アクセス ログイン 2022年11月27日 20:36	user1@nbuprimary.lab.local	User 'user1' authenticated successfully
🔍 アクセス ログイン 2022年11月27日 20:36	root@nbuprimary.lab.local	User 'root@nbuprimary.lab.local' is logged out
✅ アクセス ログイン 2022年11月27日 20:35	root@nbuprimary.lab.local	User 'root' authenticated successfully
❌ アクセス ログイン 2022年11月27日 20:34	root@nbuprimary.lab.local	User 'root' authentication failed

(例) ログイン

- ✓ 監査はデフォルトで有効
- ✓ SOX法で要求されるガイドラインに準拠
- ✓ 監査レコードのバックアップは、カタログバックアップの一環で実施
- ✓ 監査レコードは、デフォルト90日間保持（0に設定し無期限にすることも可）
- ✓ Syslogへの送信 & Syslog転送が可能
- ✓ nbauditreportコマンドで監査ログを表示可能

NetBackup Web UI 管理者ガイド P211「セキュリティイベントと監査ログ」
<https://sort.veritas.com/DocPortal/pdf/152422053-162358156-1>

4. 参考情報

4-1 監査イベントについて

監査イベントのカテゴリと概要

監査イベントのカテゴリ (48種類) <-V10.3

アラート (ALERT)	インテリジェントグループ (ASSETGROUP)
異常 (ANOMALY)	ジョブ (JOB)
異常な拡張子 (ANOMALY_EXTENSIONS)	ライセンス (LICENSING)
新しい異常 (ANOMALY_NEW)	ログイン (LOGIN)
異常なルールの結果 (ANOMALY_RULES)	マルウェアの影響あり (MALWARE_IMPACTED)
資産 (ASSET)	マルウェアスキャンの状態 (MALWARE_SCAN_STATUS)
監査構成 (AUDITCFG)	マルウェアスキャンのトリガ (MALWARE_SCAN_TRIGGER)
監査データベース (AUDITDB)	ポリシー (POLICY)
監査サービス (AUDITSVC)	プール (POOL)
認証エラー (AZFAILURE)	保護計画 (PROTECTION_PLAN_SVC)
一時停止中のクライアント (PAUSED_CLIENTS)	保持レベル (RETENTION_LEVEL)
Bare Metal Restore (BMR)	セキュリティ構成 (SEC_CONFIG)
bp.conf (BPCONF)	ストレージライフサイクルポリシー (SLP)
カタログ (CATALOG)	ストレージサーバー (STORAGE_SRV)
証明書 (CERT)	ストレージユニット (STU)
構成 (CONFIG)	トークン (TOKEN)
接続 (CONNECTION)	ユーザー (USER)
クレデンシャル (CREDENTIALS)	Audit Log Forward (AUDIT_LOG_FORWARD)
クレデンシャルスキーマ (CREDENTIAL_SCHEMA)	Event Audit (EVENT_AUDIT)
データアクセス (DATAACCESS)	External CMS Server (ECMS)
検出 (DISCOVERY)	Isolated Recovery Environment (IRE)
イベントログ (EVENT_LOG)	など
保留 (HOLD)	
ホスト (HOST)	

監査される処理 (抜粋)

- ✓ NetBackup管理コンソール、Web UI、または、APIへのログオン試行の失敗または成功
- ✓ アクティビティモニター（ジョブステータス確認画面）にて、ジョブのキャンセル、中断、再開、再起動、ジョブ履歴の削除
- ✓ 異常検出、マルウェアスキャンの開始、完了、検出
- ✓ 異常を誤検知（偽陽性：false positive）として報告
- ✓ ジョブ設定（バックアップポリシー、保護計画）の作成、変更、削除
- ✓ バックアップイメージの期限切れ、リストアのためのカタログ検索
- ✓ リストアジョブの開始
- ✓ 資産のクリーンアップ処理の一環として、vCenter Serverなどの資産を削除（登録解除）
- ✓ セキュリティ構成設定に加えられた変更

4. 参考情報

4-2 参考資料

- NetBackup™ セキュリティおよび暗号化ガイド V10.3 （異常検出に関する設定等の情報）
<https://sort.veritas.com/DocPortal/pdf/32258597-162350087-1>
- NetBackup™ Web UI 管理者ガイド V10.3 （監査イベントの情報）
<https://sort.veritas.com/DocPortal/pdf/152422053-162358156-1>

The Veritas logo is positioned in the top right corner of the page. It consists of the word "VERITAS" in a white, uppercase, sans-serif font, with a small trademark symbol (TM) to its upper right. The background of the entire page is a low-angle shot of a modern glass skyscraper against a bright blue sky with scattered white clouds. A warm, golden light flare is visible in the upper left quadrant, suggesting the sun is low on the horizon. A large, semi-transparent red shape, resembling a stylized arrow or a corner of a page, is located on the right side of the image, containing the Japanese text "ありがとうございました！".

VERITAS™

ありがとうございました！

Copyright © 2024 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.