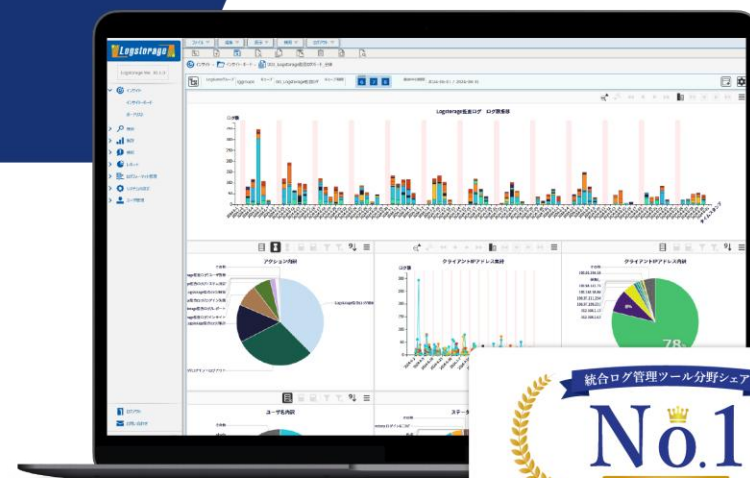


Logstorage

統合ログ管理システム「ログストレージ」

Logstorage SSDB監査 連携パック
参考資料



Logstorage 連携パックとは

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。

連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログのフォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。

「アップデートでログの保管先が変わった」

「出力されるログの内容が変わった」

「保管するログのサイズが増えた」

「仕様変更でログの種類が増えた」

「独自の収集プログラムが
仕様変更で作り直し」



技術者のリソースが
ログ管理に取られすぎる



パッケージ内容

Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

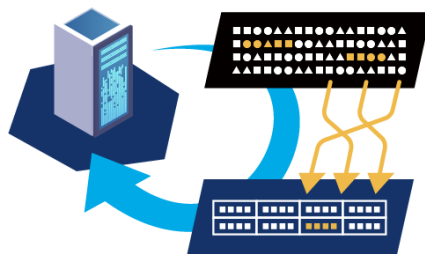
ログ収集モジュール



製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

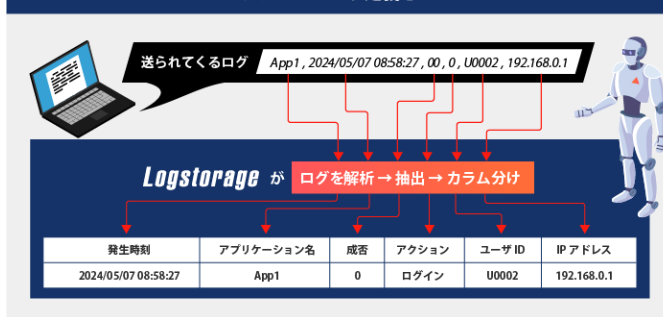
※製品によっては収集モジュールが不要の場合もございます。
その場合、パッケージに含まれませんので、ご了承ください。

ログフォーマット定義ファイル



連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。

ログフォーマット定義とは？

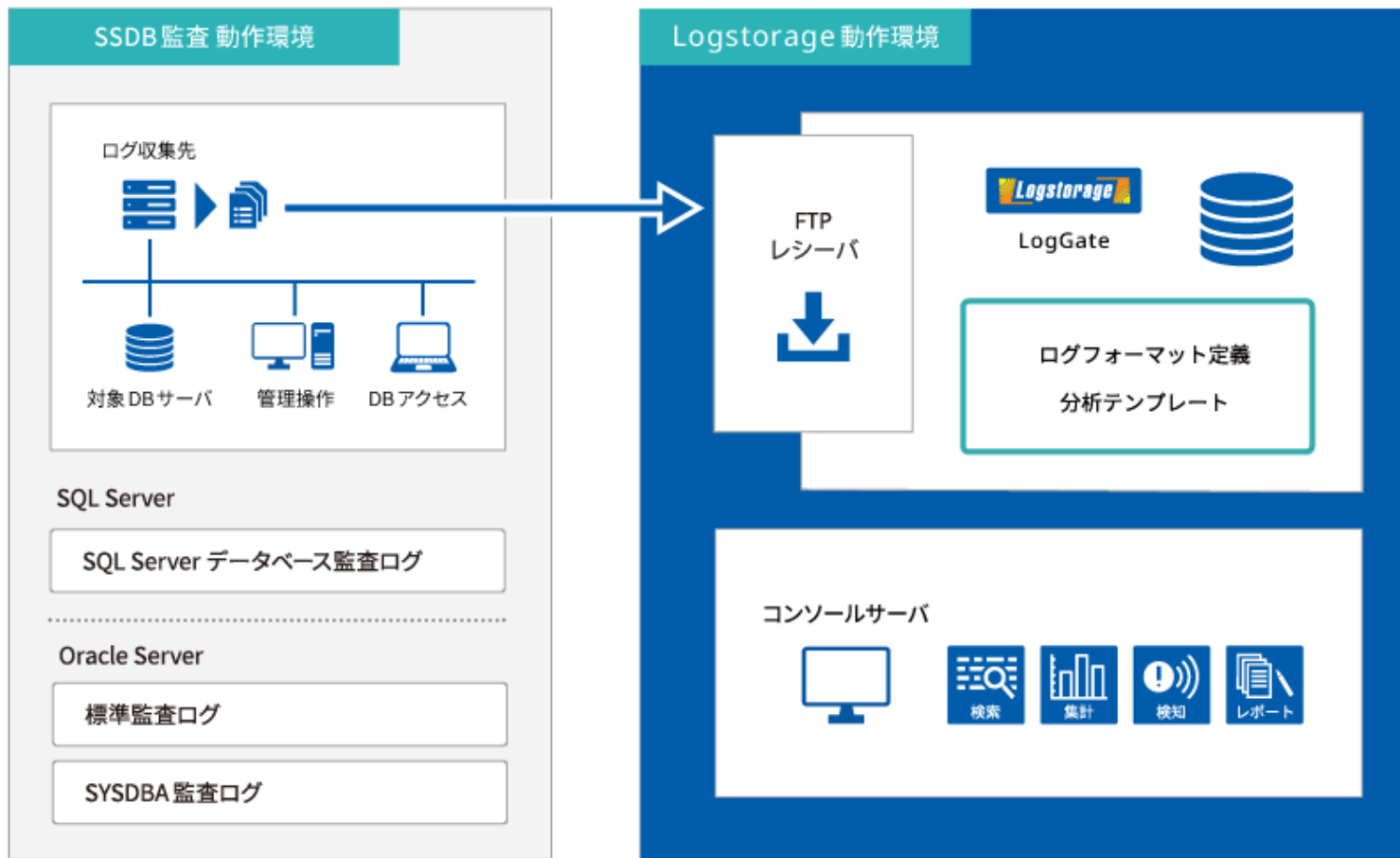


分析テンプレート



各製品から出力される多数のログの中から、どのログを検索すればよいのか・何を集計したらよいのか・どんなレポートを出力すればよいのか、ログ分析をサポートする分析テンプレートをご提供いたします。

システム構成



Logstorage SSDB監査 連携パック SQL Serverログの検索テンプレートは以下の通りです。

検索条件テンプレート名	概要
ログアウト	ログアウトログの検索
ログイン失敗	ログイン失敗ログの検索
ログイン成功	ログイン成功ログの検索
全ログ検索	SSDB監査の全ログ検索
操作一覧検索	全操作
操作一覧検索（SQL文無し）	全操作（SQL文無し）
操作別検索(作成/変更/取消/権限付与/権限剥奪/権限拒否)	作成/変更/取消/権限付与/権限剥奪/権限拒否
操作別検索(参照/挿入/更新/削除 等)	参照/挿入/更新/削除/切捨て/実行
権限操作検索	作成/変更/取消/権限付与/権限剥奪/権限拒否

SQL Serverログ・テンプレート一覧

集計

Logstorage SSDB監査 連携パック SQL Serverログの集計テンプレートは以下の通りです。

集計条件テンプレート名	概要
SQLユーザ毎 操作別集計(作成、変更、取消、権限操作 等)	SQLユーザ毎 操作別集計（作成、変更、取消、権限操作 等）
SQLユーザ毎 操作別集計(参照、挿入、更新、削除 等)	SQLユーザ毎 操作別集計（参照、挿入、更新、削除 等）
サーバ別ログイン集計(ユーザ毎)	ユーザ別のログイン数の集計
ユーザ毎操作別集計	ユーザ毎、操作別の件数を集計
ユーザ毎権限操作別集計	ユーザ毎、権限操作別の件数を集計
ログイン失敗集計(ユーザ別)	ユーザ別のログイン失敗の集計
ログイン集計(サーバ別)	サーバ毎のログイン成功／失敗数を集計
ログイン集計(ユーザ別)	ユーザ別のログイン数の集計
ログイン集計(日別)	日別のログイン数の集計
操作別集計(テーブル操作)	ユーザ毎の作成、変更、取消、権限付与、権限剥奪、権限拒否の操作別の件数を集計
操作別集計(レコード操作)	ユーザ毎の参照、挿入、更新、削除 等の操作別の件数を集計

SQL Serverログ・テンプレート一覧

レポート

Logstorage SSDB監査 連携バック SQL Serverログのレポートテンプレートは以下の通りです。

レポート条件テンプレート名	概要
ログイン集計レポート（サーバ別・ユーザ毎）	サーバ別のSQLユーザのログイン成功と失敗をレポートします。
ログイン集計レポート（サーバ別）	サーバ別にユーザのログイン成功と失敗をレポートします。
ログイン集計レポート（ユーザ別）	SQLユーザ毎にログインの成功と失敗をレポートします。
操作一覧レポート	操作を一覧でレポートします。
操作一覧レポート（SQL文無し）	操作を一覧でレポートします。
操作一覧レポート（権限操作）	権限操作を一覧でレポートします。
操作別集計レポート（テーブル操作）	ユーザ毎の作成、変更、取消、権限付与、権限剥奪、権限拒否 の操作集計をレポートします。
操作別集計レポート（レコード操作）	ユーザ毎の参照、挿入、更新、削除 等の操作集計をレポートします。
ログイン集計レポート（サーバ別・ユーザ毎）	サーバ別のSQLユーザのログイン成功と失敗をレポートします。
ログイン集計レポート（サーバ別）	サーバ別にユーザのログイン成功と失敗をレポートします。
ログイン集計レポート（ユーザ別）	SQLユーザ毎にログインの成功と失敗をレポートします。

Oracleログ・テンプレート一覧

検索

Logstorage SSDB監査 連携パック Oracleログの検索テンプレートは以下の通りです。

ファイル名	検索条件テンプレート名	概要
SYSDBA監査	SYSDBA監査 ログイン失敗	SYSDBA監査のログイン失敗ログの検索
SYSDBA監査	SYSDBA監査 ログイン成功	SYSDBA監査のログイン成功ログの検索
SYSDBA監査	SYSDBA監査 全ログ検索	DBAUのSYSDBA監査の全ログ検索
SYSDBA監査	SYSDBA監査 参照走査検索	SYSDBA監査の参照
SYSDBA監査	SYSDBA監査 定義操作別検索	SYSDBA監査の作成/変更/取消/権限付与/権限剥奪
SYSDBA監査	SYSDBA監査 情報操作別検索	SYSDBA監査の挿入/更新/削除/切捨て/実行
SYSDBA監査	SYSDBA監査 操作一覧検索	SYSDBA監査の全操作
SYSDBA監査	SYSDBA監査 操作一覧検索（SQL文無し）	SYSDBA監査の全操作（SQL文無し）
標準監査	ログアウト	ログアウトログの検索
標準監査	ログイン失敗	ログイン失敗ログの検索
標準監査	ログイン成功	ログイン成功ログの検索
標準監査	全ログ検索	SSDBLOの全ログ検索
標準監査	参照操作検索	参照
標準監査	定義操作別検索	作成/変更/取消/権限付与/権限剥奪
標準監査	情報操作別検索	挿入/更新/削除/切捨て/実行
標準監査	操作一覧検索	全操作
標準監査	操作一覧検索（SQL文無し）	全操作（SQL文無し）

Oracleログ・テンプレート一覧

集計

Logstorage SSDB監査 連携パック Oracleログの集計テンプレートは以下の通りです。

ファイル名	集計条件テンプレート名	概要
SYSDBA監査	SYSDBA監査 DBユーザ毎 操作別集計（作成、変更、取消、権限操作 等）	SQLユーザ毎 操作別集計（作成、変更、取消、権限操作 等）（OSファイル）
	SYSDBA監査 DBユーザ毎 操作別集計（参照、挿入、更新、削除 等）	SQLユーザ毎 操作別集計（参照、挿入、更新、削除 等）（OSファイル）
	SYSDBA監査 ユーザ毎操作別集計	ユーザ毎、操作別の件数を集計（OSファイル）
	SYSDBA監査 ユーザ毎権限操作別集計	ユーザ毎、権限操作別の件数を集計（OSファイル）
	SYSDBA監査 操作別集計（テーブル操作）	ユーザ毎の作成、変更、取消、権限付与、権限剥奪、権限拒否の操作別の件数を集計（OSファイル）
	SYSDBA監査 操作別集計（レコード操作）	ユーザ毎の参照、挿入、更新、削除 等の操作別の件数を集計（OSファイル）

Oracleログ・テンプレート一覧

レポート-1

Logstorage SSDB監査 連携パック Oracleログのレポートテンプレートは以下の通りです。

ファイル名	レポート条件テンプレート名	概要
SYSDBA監査	SYSDBA監査 DBユーザ毎 操作別集計（作成、変更、取消、権限操作等）	SQLユーザ毎 操作別集計（作成、変更、取消、権限操作等）（OSファイル）
SYSDBA監査	SYSDBA監査 DBユーザ毎 操作別集計（参照、挿入、更新、削除等）レポート	SQLユーザ毎 操作別集計（参照、挿入、更新、削除等）（OSファイル）
SYSDBA監査	SYSDBA監査 ユーザ毎操作別集計レポート	ユーザ毎、操作別の件数を集計（OSファイル）
SYSDBA監査	SYSDBA監査 ユーザ毎権限操作別集計レポート	ユーザ毎、権限操作別の件数を集計（OSファイル）
SYSDBA監査	SYSDBA監査 ログイン失敗一覧レポート	SYSDBA監査のログイン失敗ログの一覧
SYSDBA監査	SYSDBA監査 ログイン成功一覧レポート	SYSDBA監査のログイン成功ログの一覧
SYSDBA監査	SYSDBA監査 定義操作別一覧レポート	SYSDBA監査の作成/変更/取消/権限付与/権限剥奪
SYSDBA監査	SYSDBA監査 情報操作別一覧レポート	SYSDBA監査の挿入/更新/削除/切捨て/実行
SYSDBA監査	SYSDBA監査 操作別集計（テーブル操作）レポート	ユーザ毎の作成、変更、取消、権限付与、権限剥奪、権限拒否の操作別の件数を集計（OSファイル）
SYSDBA監査	SYSDBA監査 操作別集計（レコード操作）レポート	ユーザ毎の参照、挿入、更新、削除等の操作別の件数を集計（OSファイル）

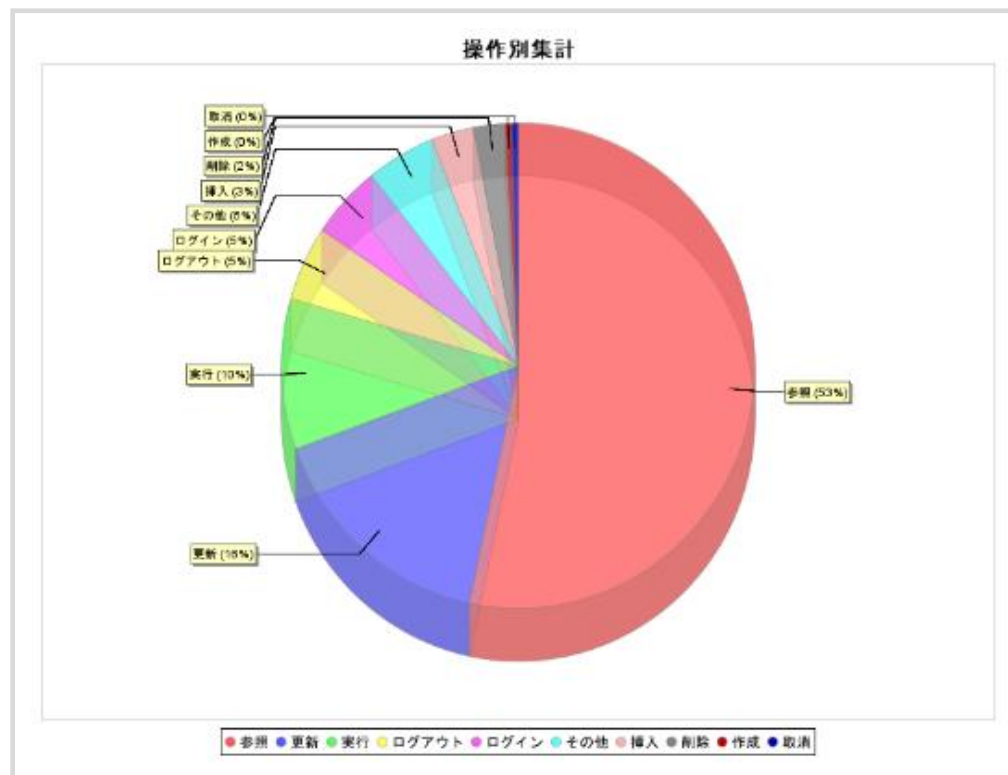
Oracleログ・テンプレート一覧

レポート-2

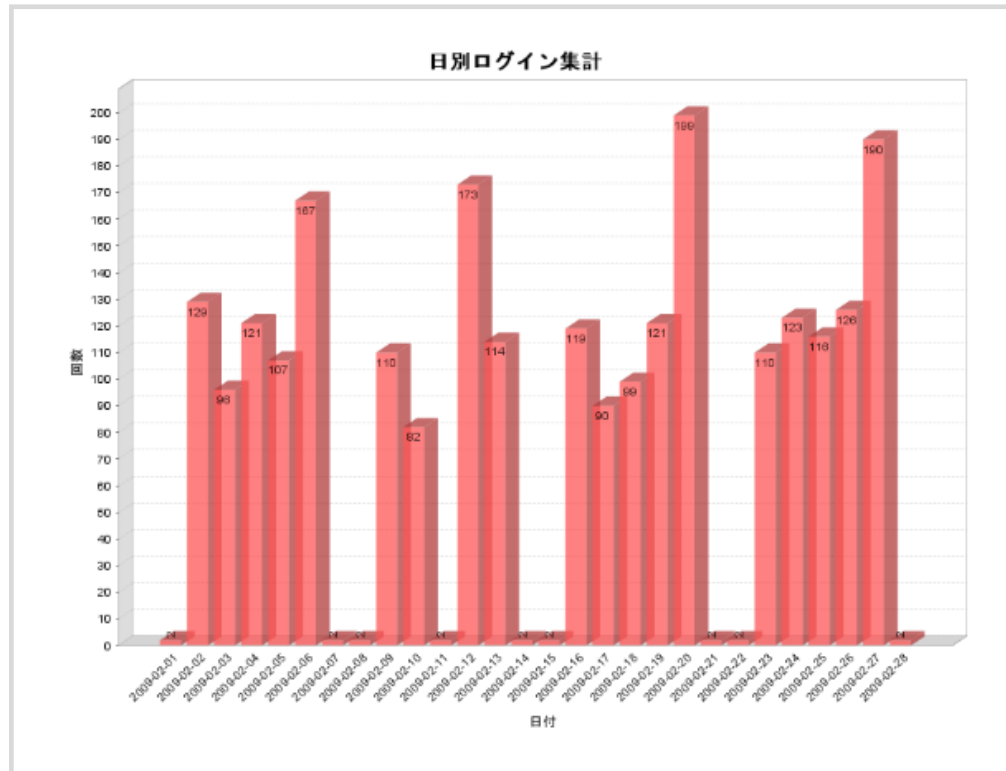
Logstorage SSDB監査 連携パック Oracleログのレポートテンプレートは以下の通りです。

ファイル名	レポート条件テンプレート名	概要
標準監査	DBユーザ毎 操作別集計（作成、変更、取消、権限操作 等） レポート	SQLユーザ毎 操作別集計（作成、変更、取消、権限操作 等）（監査テーブル）
標準監査	DBユーザ毎 操作別集計（参照、挿入、更新、削除 等） レポート	SQLユーザ毎 操作別集計（参照、挿入、更新、削除 等）（監査テーブル）
標準監査	サーバ別ログイン集計（ユーザ毎） レポート	ユーザ別のログイン数の集計
標準監査	ユーザ毎操作別集計レポート	ユーザ毎、操作別の件数を集計（監査テーブル）
標準監査	ユーザ毎権限操作別集計レポート	ユーザ毎、権限操作別の件数を集計（監査テーブル）
標準監査	ログイン失敗一覧レポート	ログイン失敗ログの一覧
標準監査	ログイン失敗集計（ユーザ別） レポート	ユーザ別のログイン失敗の集計（監査テーブル）
標準監査	ログイン成功一覧レポート	ログイン成功ログの一覧
標準監査	ログイン集計（サーバ別） レポート	サーバ毎のログイン成功／失敗数を集計（監査テーブル）
標準監査	ログイン集計（ユーザ別） レポート	ユーザ別のログイン数の集計（監査テーブル）
標準監査	ログイン集計（日別） レポート	日別のログイン数の集計（監査テーブル）
標準監査	定義操作別一覧レポート	作成/変更/取消/権限付与/権限剥奪 一覧
標準監査	情報操作別一覧レポート	挿入/更新/削除/切捨て/実行 一覧
標準監査	操作別集計（テーブル操作） レポート	ユーザ毎の作成、変更、取消、権限付与、権限剥奪、権限拒否の操作別の件数を集計（監査テーブル）
標準監査	操作別集計（レコード操作） レポート	ユーザ毎の参照、挿入、更新、削除 等の操作別の件数を集計（監査テーブル）

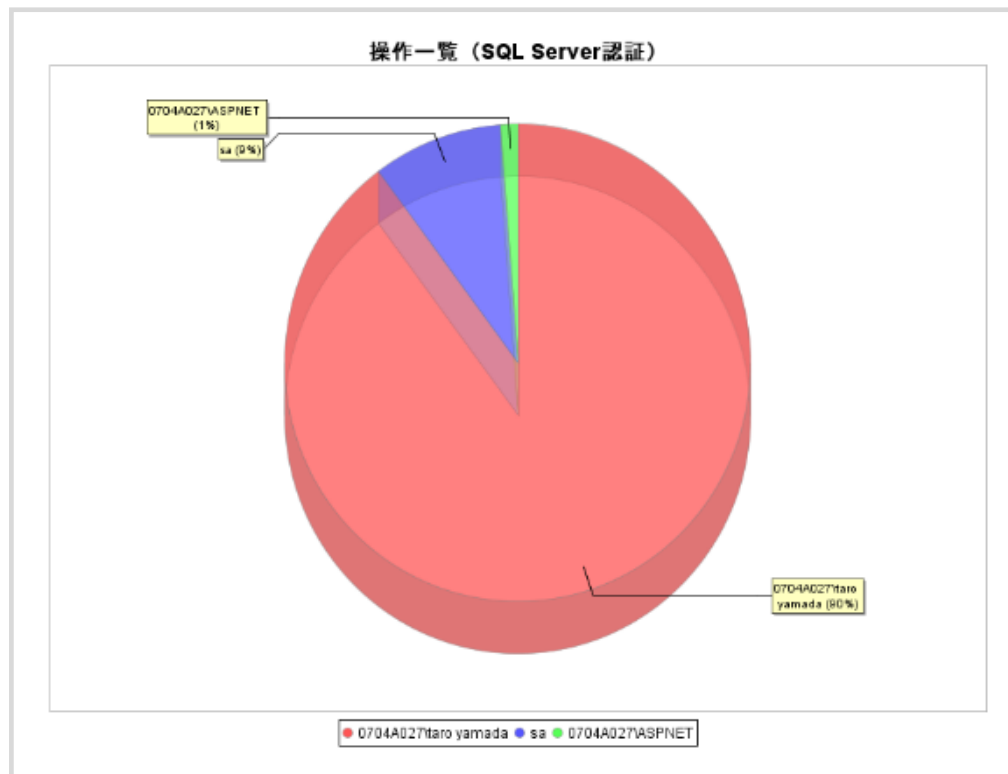
レポート例 1



レポート例 2



レポート例 3



お問い合わせ

ご不明点、ご相談につきましては、下記お問い合わせ先からご連絡ください。

電話でのお問い合わせ

03-5427-3503

【受付】 平日 9:00～17:30

メールでのお問い合わせ

info@logstorage.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください

当社のホームページでも資料請求・お問い合わせができます。

<https://logstorage.com>