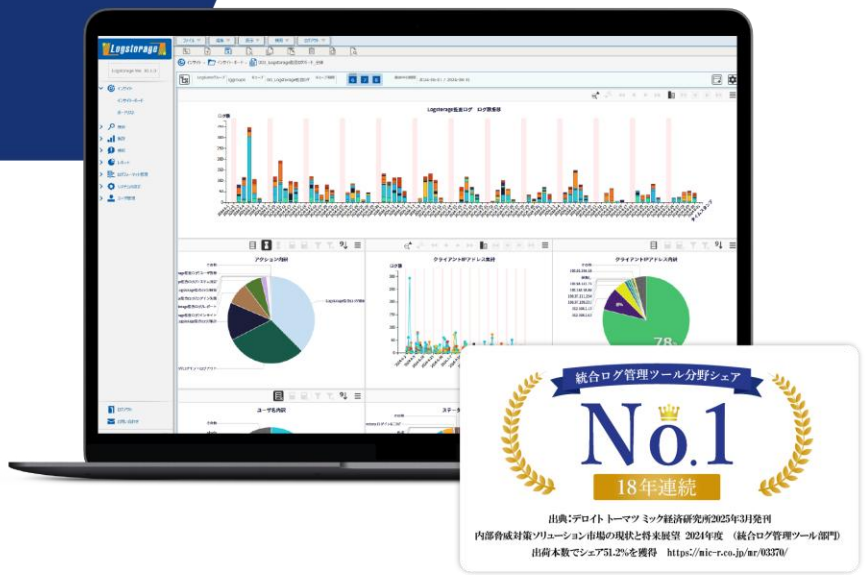
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage PISO 連携パック
参考資料



Infoscience

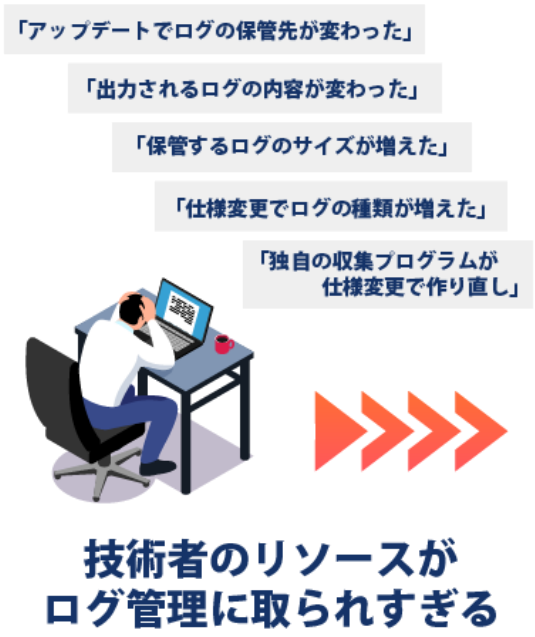
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

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。



パッケージ内容

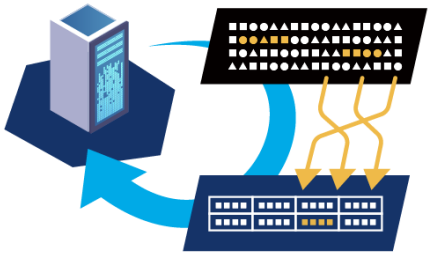
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

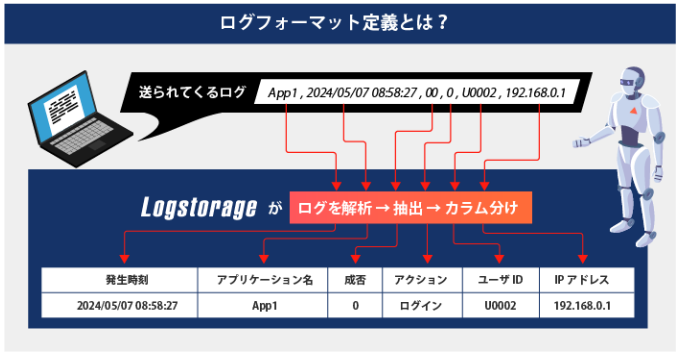
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※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



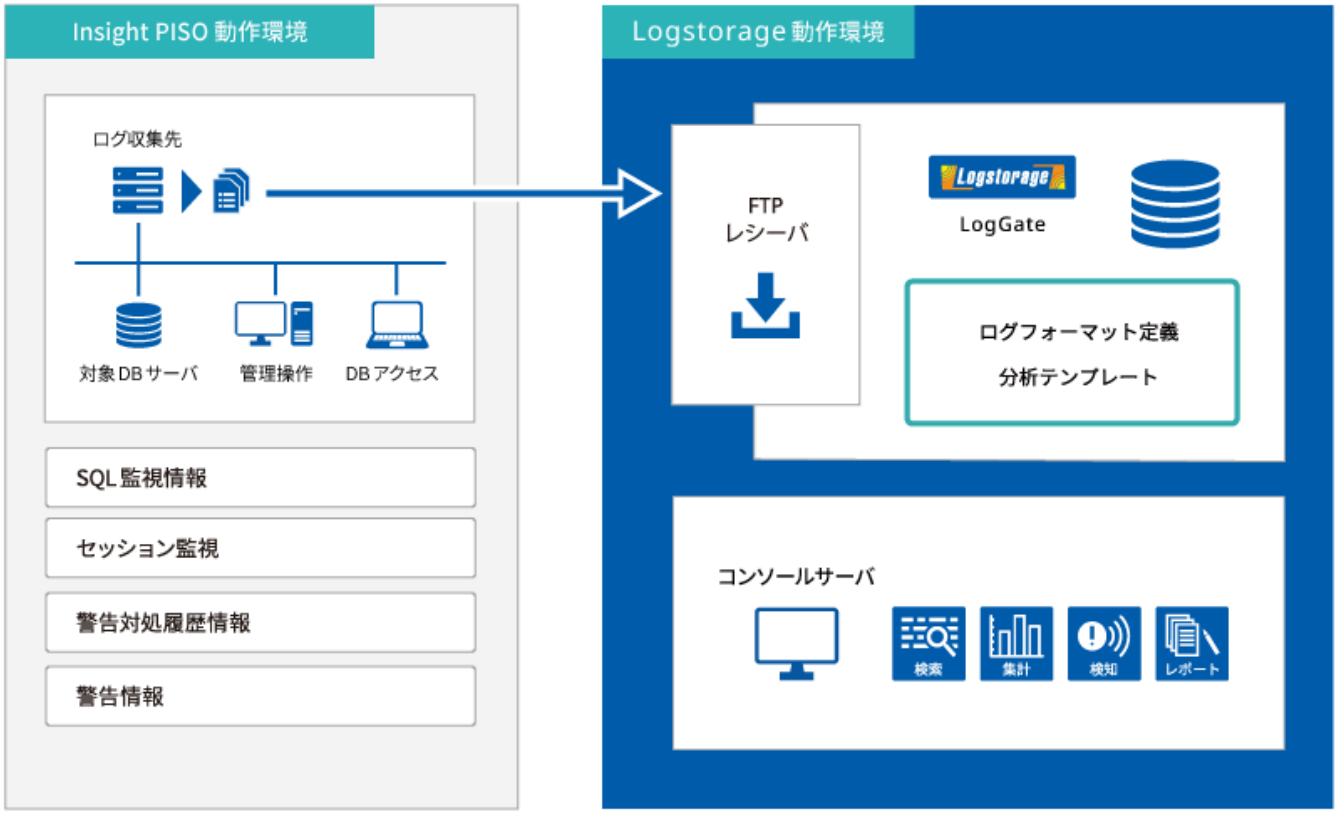
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



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



検索テンプレート一覧

Logstorage PISO 連携パック 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
DB更新SQL限定レポート	DBに対するユーザーの更新(SELECT文以外)の詳細を時系列で確認できます。
PISO SQL監視情報	-
PISO セッション監視情報	-
PISO 警告対処履歴情報	-
PISO 警告情報	-
アカウント変更管理	Oracleのアカウントの作成、権限変更を確認できます。
アクセス経路別レポート	アクセス経由ごとの実行回数、処理件数を確認できます。
システム変更管理	Oracleの初期化パラメータの変更などのシステム変更を確認できます。
スキーマ変更管理	Oracleのスキーマに対する変更を確認できます。
データベースの起動・停止	システム名、データベース名ごとにデータベースの起動、停止状況を確認できます。
ログオンログ一覧	-
特権ユーザーのアプリケーションテーブルへの不正アクセス	特権ユーザー(SYS,SYSTEMおよび/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)がアプリケーションテーブルに不正にアクセスした際の詳細情報を確認できます。(事前に"特権ユーザー監視DDL","特権ユーザー監視DML"という文字列を含む警告ルールを設定しておく必要があります。)
特権ユーザー利用状況チェック	特権ユーザー(SYS,SYSTEM)の利用状況を確認して特権ユーザーが複数人で使用されていないかを確認できます。(SYS,SYSTEM以外の特権ユーザがいる場合は、追加してください。)
特権ユーザー監視（DDL）	特権ユーザー（SYS,SYSTEM,/ AS SYSDBA,/ AS SYSOPER）がDDLを実施した際の警告情報と警告対処履歴を一覧表示します。（事前に"DDL"という文字列を含む警告ルールを設定しておく必要があります。）

集計テンプレート一覧

Logstorage PISO 連携パック 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
ログオンログ一覧	-
未許可アクセスレポート	-
特権ユーザーアクティビティ	特権ユーザー(SYS,SYSTEM,および/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)の発行コマンドの累計を確認できます。
特権ユーザー監視警告回数	特権ユーザー専用の警告ルールごとの警告発生件数を示します。（事前に"特権ユーザー監視"という文字列を含む警告ルールを設定しておく必要があります。）
警告ルール別検知回数	警告ルールごとの警告発生件数を示します。

レポートテンプレート一覧

Logstorage PISO 連携パック 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
DB更新SQL限定レポート	DBに対するユーザーの更新（SELECT文以外）の詳細を時系列で確認できます。
アカウント変更管理	Oracleのアカウントの作成、権限変更を確認できます。
アクセス経路別レポート	アクセス経路ごとの実行回数、処理件数を確認できます。
システム変更管理	Oracleの初期化パラメータの変更などのシステム変更を確認できます。
スキーマ変更管理	Oracleのスキーマに対する変更を確認できます。
データベースの起動・停止	システム名、データベース名ごとにデータベースの起動、停止状況を確認できます。
ログオンログ一覧	日付、ユーザ、データベース毎の1日当たりのデータベースログイン件数を確認できます。
未許可アクセスレポート	正規アクセスパターン以外のアクセス経路を確認できます。
特権ユーザーのアプリケーションテーブルへの不正アクセス	特権ユーザー(SYS,SYSTEMおよび/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)がアプリケーションテーブルに不正にアクセスした際の詳細情報を確認できます。(事前に"特権ユーザー監視DDL","特権ユーザー監視DML"という文字列を含む警告ルールを設定しておく必要があります。)
特権ユーザーアクティビティ	特権ユーザー(SYS,SYSTEM,および/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)の発行コマンドの累計を確認できます。
特権ユーザー利用状況チェック	特権ユーザー(SYS,SYSTEM)の利用状況を確認して特権ユーザーが複数人で使用されていないかを確認できます。(SYS,SYSTEM以外の特権ユーザがいる場合は、追加してください。)
特権ユーザー監視警告回数	特権ユーザー専用の警告ルールごとの警告発生件数を示します。（事前に"特権ユーザー監視"という文字列を含む警告ルールを設定しておく必要があります。）
特権ユーザー監視（DDL）	特権ユーザー（SYS,SYSTEM,/ AS SYSDBA,/ AS SYSOPER）がDDLを実施した際の警告情報と警告対処履歴を一覧表示します。（事前に"DDL"という文字列を含む警告ルールを設定しておく必要があります。）
警告ルール別検知回数	警告ルールごとの警告発生件数を示します。

レポート例 1

データベース・アクティビティレポート

データベースの起動・停止

概要　システム名、データベース名ごとにデータベースの起動、停止状況を確認できます。
作成日　2008-08-14 13:06:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　2件

システム名	データベース名	実行日時	アクション	DBユーザー	OSユーザー	端末
Server132 + Ora102	ora102	2008-06-27 00:00:00	SHUTDOWN	SCOTT	piso102	pts/1
Server132 + Ora102	ora102	2008-06-27 00:00:00	STARTUP	SCOTT	piso102	pts/1

システム変更管理

概要　Oracleの初期化パラメータの変更などのシステム変更を確認できます。
作成日　2008-08-14 13:06:15
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　3件

システム名	データベース名	実行日時	アクション	DBユーザー	端末
Server132 + Ora102	ora102	2008-06-27 00:00:00	ALTER DATABASE	SCOTT	pts/1
Server132 + Ora102	ora102	2008-06-27 00:00:00	ALTER SYSTEM	SCOTT	pts/1
Server132 + Ora102	ora102	2008-06-27 00:00:00	SET SYSTEM PARAMETER	SCOTT	pts/1

アカウント変更管理

概要　Oracleのアカウントの作成、権限変更を確認できます。
作成日　2008-08-14 13:06:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　6件

システム名	データベース名	実行日時	アクション	DBユーザー
Server132 + Ora102	ora102	2008-06-27 00:00:00	CREATE USER	SCOTT
Server132 + Ora102	ora102	2008-06-27 00:00:00	DROP USER	SCOTT
Server132 + Ora102	ora102	2008-06-27 00:00:00	GRANT ROLE	SCOTT
Server132 + Ora102	ora102	2008-06-27 00:00:00	GRANT OBJECT	SCOTT
Server132 + Ora102	ora102	2008-06-27 00:00:00	ALTER USER	SCOTT
Server132 + Ora102	ora102	2008-06-27 00:00:00	GRANT	SCOTT

スキーマ変更管理

概要　Oracleのスキーマに対する変更を確認できます。
作成日　2008-08-14 13:06:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　29件

システム名	データベース名	アクション	実行日時	DBユーザー	マシン	端末
Server132 + Ora102	ora102	CREATE LIBRARY	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	CREATE JAVA	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP TABLE	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP CLUSTER	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP VIEW	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP PROCEDURE	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP MATERIALIZED VIEW	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP FUNCTION	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP PACKAGE	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP LIBRARY	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	DROP JAVA	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	ALTER TABLE	2008-06-27 00:00:00	SCOTT	server132	pts/1
Server132 + Ora102	ora102	ALTER CLUSTER	2008-06-27 00:00:00	SCOTT	server132	pts/1

警告ルール別検知回数

概要　警告ルールごとの警告発生件数を示します。
作成日　2008-08-14 13:07:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

集計条件名　警告ルール別検知回数
概要　警告ルールごとの警告発生件数を示します。

システム名	データベース名	メッセージ	件数
Server132 + Ora102	ora102	DDLセッション情報監視【ログオン監視】	1
		SQL情報監視【すべてのSQL】	10
		SQL監視情報【特権ユーザー監視DDL】	3
		セッション情報監視【ログオン監視】	10
		未許可アクセス監視	1

特権ユーザー利用状況チェック

概要　特権ユーザー(SYS,SYSTEM)の利用状況を確認して特権ユーザーが複数人で使用されていないかを確認できます。(SYS,SYSTEM以外の特権ユーザがいる場合は、追加してく
作成日　2008-08-14 13:07:14
対象期間2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　3件

システム名	データベース名	DBユーザー	OSユーザー	実行回数
Server132 + Ora102	ora102	SYS	piso102	2
Server132 + Ora102	ora102	SYSTEM	piso102	2
Server132 + Ora102	ora102	SYSTEM	piso102	2

レポート例 2

特権ユーザ管理レポート_1

特権ユーザー利用状況チェック

概要　　特権ユーザー(SYS,SYSTEMの利用状況を確認して特権ユーザーが複数人で使用されていないかを確認できます。(SYS,SYSTEM以外の特権ユーザがいる場合は、追加してく
作成日　2008-08-14 13:07:14
対象期間2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　3件

システム名	データベース名	DBユーザー	OSユーザー	実行回数
Server132 + Ora102	ora102	SYS	piso102	2
Server132 + Ora102	ora102	SYSTEM	piso102	2
Server132 + Ora102	ora102	SYSTEM	piso102	2

特権ユーザー監視(DDL)

概要　　特権ユーザー(SYS,SYSTEM,/ AS SYSDBA,/ AS SYSOPER)がDDLを実施した際の警告情報と警告対処履歴を一覧表示します。(事前に"DDL"という文字列を含む警告ルール
作成日　2008-09-10 17:44:47
対象期間2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　2件

システム名	データベース名	DBユーザー	OSユーザー	ログオン日時	SQL文	メッセージ	最新ステータス	担当者	対処メッセージ
Server132 + Ora102	ora102	SYS	piso102	2008-06-27 00:00:00	select * from dept	DDLセッション情報監視 [ログオン監視]	CLOSED	ユーザ3	確認済み
Server132 + Ora102	ora102	SYS	piso102	2008-06-27 00:00:00	select * from dept	SQL監視情報[特権ユーザー監視DDL]	CLOSED	ユーザ3	確認済み

特権ユーザー監視警告回数

概要　　特権ユーザー専用の警告ルールごとの警告発生件数を示します。(事前に"特権ユーザー監視"という文字列を含む警告ルールを設定しておく必要があります。)
作成日　2008-08-14 13:08:14
対象期間 2008-06-27 00:00:00 - 2008-06-27 23:59:59

集計条件名　特権ユーザー監視警告回数
概要　　特権ユーザー専用の警告ルールごとの警告発生件数を示します。(事前に"特権ユーザー監視"という文字列を含む警告ルールを設定しておく必要があります。)

システム名	データベース名	DBユーザー	メッセージ	警告件数
				件数
Server132 + Ora102	ora102	SYS	SQL監視情報[特権ユーザー監視DDL]	3

特権ユーザーのアプリケーションテーブルへの不正アクセス

概要　　特権ユーザー(SYS,SYSTEMおよび/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)がアプリケーションテーブルに不正にアクセスした際の詳細情報を確認できます。(事前に
作成日　2008-09-10 17:30:47
対象期間2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　1件

システム名	データベース名	DBユーザー	SQL文	警告日時
Server132 + Ora102	ora102	SYS	select * from dept	2008-06-27 00:00:00

レポート例 3

特権ユーザ管理レポート_2

特権ユーザーアクティビティ

概要　特権ユーザー(SYS,SYSTEM,および/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)の発行コマンドの累計を確認できます。
作成日　2008-08-14 13:08:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

集計条件名　特権ユーザーアクティビティ
概要　特権ユーザー(SYS,SYSTEM,および/ AS SYSDBA,/ AS SYSOPERで接続したユーザー)の発行コマンドの累計を確認できます。

システム名	データベース名	アクション	DBユーザー	OSユーザー	コマンド発行回数
					件数
Server132 + Ora102	ora102	RDBDDLEX	SYSTEM	piso102	6

アクセス経路別レポート

概要　アクセス経路ごとの実行回数、処理件数を確認できます。
作成日　2008-08-14 13:07:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　15件

システム名	データベース名	DBユーザー	OSユーザー	マシン	端末	処理件数	実行回数
Server132 + Ora102	ora102	SYS	piso102	server132	192.168.200.16	28	2
Server132 + Ora102	ora102	SYSTEM	piso102	server132	192.168.200.16	28	2
Server132 + Ora102	ora102	SYSTEM	piso102	server132	192.168.200.16	28	2
Server132 + Ora102	ora102	SCOTT	piso102	server132	192.168.200.16	14	1
Server132 + Ora102	ora102	SCOTT	piso102	server132	192.168.200.16	28	2
Server132 + Ora102	ora102	SCOTT	piso102	server132	192.168.200.16	14	1

未許可アクセスレポート

概要　正規アクセスパターン以外のアクセス経路を確認できます。
作成日　2008-08-14 13:07:15
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

集計条件名　未許可アクセスレポート
概要

システム名	データベース名	DBユーザー	OSユーザー	マシン	端末	プログラム	警告件数
							件数
Server132 + Ora102	ora102	SYS	piso102	server132	192.168.200.16	sqlplus@server132 (TNS V1-V3)	1

DB更新SQL限定レポート

概要　DBに対するユーザーの更新(SELECT文以外)の詳細を時系列で確認できます。
作成日　2008-08-14 13:07:14
対象期間　2008-06-27 00:00:00 - 2008-06-27 23:59:59

検索結果　1件

システム名	データベース名	DBユーザー	OSユーザー	マシン	端末	プログラム	SQL開始日時	SQL文
Server132 + Ora102	ora102	SYSTEM	piso102	server132	192.168.200.16	sqlplus@server132 (TNS V1-V3)	2008-06-27 00:00:00	insert into .....

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