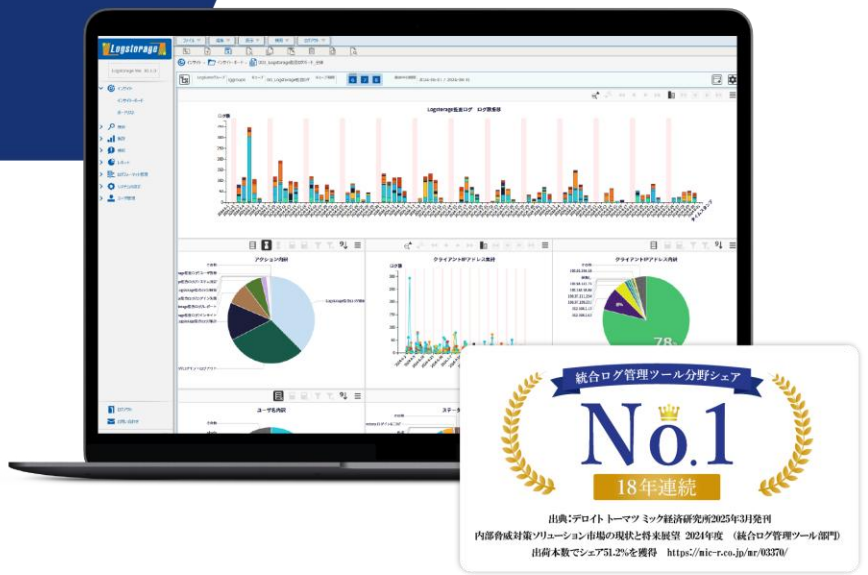
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage 秘文 連携パック
参考資料



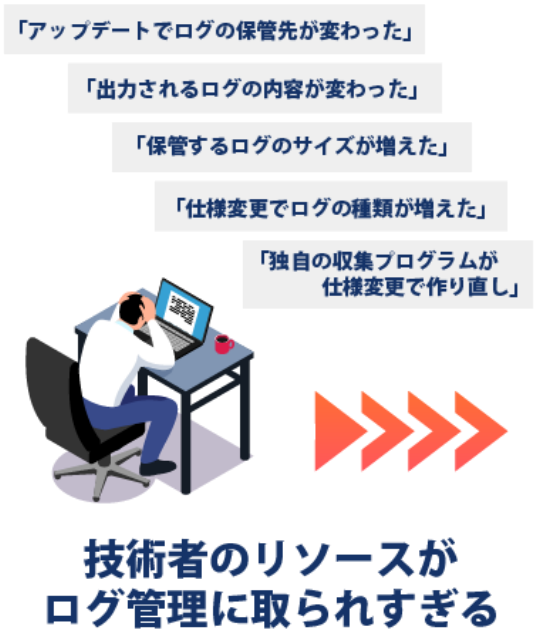
Infoscience
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

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

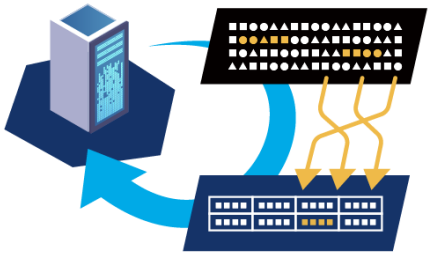
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

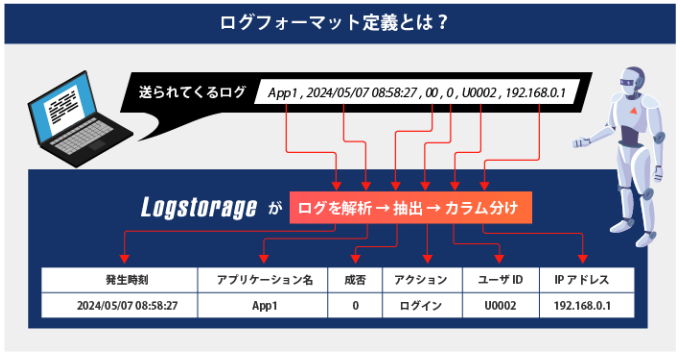
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※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



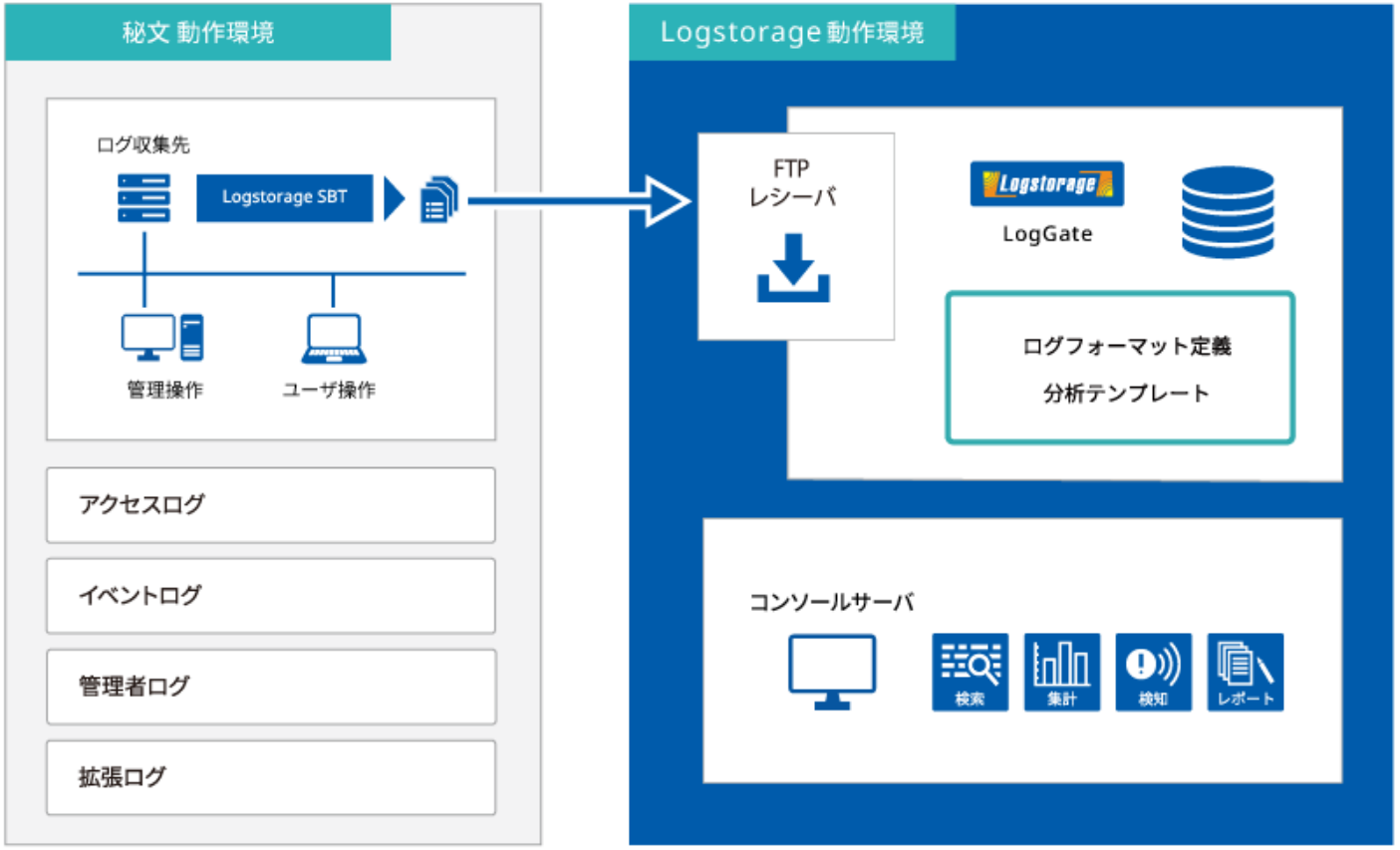
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



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

検索-1

Logstorage 秘文 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
秘文機密ファイルの作成一覧
組織外持ち出し一覧
CD/DVDによる暗号書込一覧
CD/DVDによる組織外書込一覧
ファイル保護機能によるアクセス制御(許可プログラム)一覧
ファイル保護機能によるアクセス制御(禁止プログラム)一覧
ファイル保護機能によるアクセス制御(ファイルアクセス許可ツール利用)一覧
ファイル保護機能によるネットワーク通信制御(許可)一覧
ファイル保護機能によるネットワーク通信制御(禁止)一覧
ディスクの管理領域への書き込み保護一覧
プログラムのロード一覧
共有機密フォルダへのファイル持ち出し一覧
秘文フォーマットメディアへの持ち出し一覧
通常フォーマットメディアへの持ち出し一覧
通常フォーマットメディアへの持ち出し(オフライン時)一覧
平文持ち出し一覧
CD/DVDによる平文書込一覧
共有フォルダへのファイル持ち出し一覧
印刷一覧
デバイス接続ログ一覧
ネットワーク接続制御(社内無線LAN接続)一覧
ネットワーク接続制御(社外有線LAN接続)一覧
ネットワーク接続制御(社内有線LAN接続)一覧

検索テンプレート一覧

検索-2

検索条件テンプレート名
オフラインログイン(秘文DCログイン)
DCログアウト(秘文DCログイン時)
ウィンドウアクティブ一覧
ログ取得エンジン開始/終了一覧
ファイルの作成一覧
ファイルのコピー一覧
ファイルの移動一覧
ファイル名変更一覧
ファイル削除一覧
ファイルオープン（Office製品）一覧
ファイル上書き保存（Office製品）一覧
ドライブの追加または削除一覧
プログラムの起動/終了一覧
PCの起動/終了一覧
Windowsのログオン/ログオフ一覧
マルウェア検知一覧
メモリ保護およびスクリプト禁止一覧
オフラインログイン用のパスワード発行一覧
オフラインログイン用のiKey発行一覧
秘文_アクセスログ
秘文_イベントログ
秘文_拡張ログ
秘文_管理者ログ

集計テンプレート一覧

集計

Logstorage 秘文 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
[アクセスログ集計] ユーザ毎ファイルアクセス警告・エラー集計
[アクセスログ集計] ユーザ毎操作警告・エラー集計
[アクセスログ集計] ユーザ毎操作集計
[アクセスログ集計] ユーザ毎警告・エラー回数集計

レポートテンプレート一覧

レポート-1

Logstorage 秘文 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
秘文機密ファイルの作成一覧
組織外持ち出し一覧
CD/DVDによる暗号書込一覧
CD/DVDによる組織外書込一覧
ファイル保護機能によるアクセス制御(許可プログラム)一覧
ファイル保護機能によるアクセス制御(禁止プログラム)一覧
ファイル保護機能によるアクセス制御(ファイルアクセス許可ツール利用)一覧
ファイル保護機能によるネットワーク通信制御(許可)一覧
ファイル保護機能によるネットワーク通信制御(禁止)一覧
ディスクの管理領域への書き込み保護一覧
プログラムのロード一覧
共有機密フォルダへのファイル持ち出し一覧
秘文フォーマットメディアへの持ち出し一覧
通常フォーマットメディアへの持ち出し一覧
通常フォーマットメディアへの持ち出し(オフライン時)一覧
平文持ち出し一覧
CD/DVDによる平文書込一覧
共有フォルダへのファイル持ち出し一覧
印刷一覧
デバイス接続ログ一覧
ネットワーク接続制御(社内無線LAN接続)一覧
ネットワーク接続制御(社外有線LAN接続)一覧
ネットワーク接続制御(社内有線LAN接続)一覧

レポートテンプレート一覧

レポート-2

レポート条件テンプレート名
オフラインログイン(秘文DCログイン)
DCログアウト(秘文DCログイン時)
ウィンドウアクティブ一覧
ログ取得エンジン開始/終了一覧
ファイルの作成一覧
ファイルのコピー一覧
ファイルの移動一覧
ファイル名変更一覧
ファイル削除一覧
ファイルオープン（Office製品）一覧
ファイル上書き保存（Office製品）一覧
ドライブの追加または削除一覧
プログラムの起動/終了一覧
PCの起動/終了一覧
Windowsのログオン/ログオフ一覧
マルウェア検知一覧
メモリ保護およびスクリプト禁止一覧
オフラインログイン用のパスワード発行一覧
オフラインログイン用のiKey発行一覧
秘文_アクセスログ
秘文_イベントログ
秘文_拡張ログ
秘文_管理者ログ

レポートテンプレート一覧

レポート-3

レポート条件テンプレート名
[アクセスログ集計] ユーザ毎ファイルアクセス警告・エラー集計
[アクセスログ集計] ユーザ毎操作警告・エラー集計
[アクセスログ集計] ユーザ毎操作集計
[アクセスログ集計] ユーザ毎警告・エラー回数集計

レポート例 1

不許可端末レポート

概要　不許可端末のMACアドレス、コンピュータ名などを出力します。
作成日　2015-09-03 09:39:45
対象期間　2015-07-15 00:00:00 - 2015-07-15 23:59:59

検索条件名　不許可端末レポート
概要
件数　1件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱｸｼｮﾝ	コンピューター名	IPアドレス	MACアドレス	アクセスPC	種別	ゲートウェイMACアドレス	ゲートウェイIPアドレス
2015-07-15 13:30:40	不許可端末	TEST-SERVER	192.168.0.100			ゲートウェイ検知	00-00-00-00-00-00	10.0.0.1

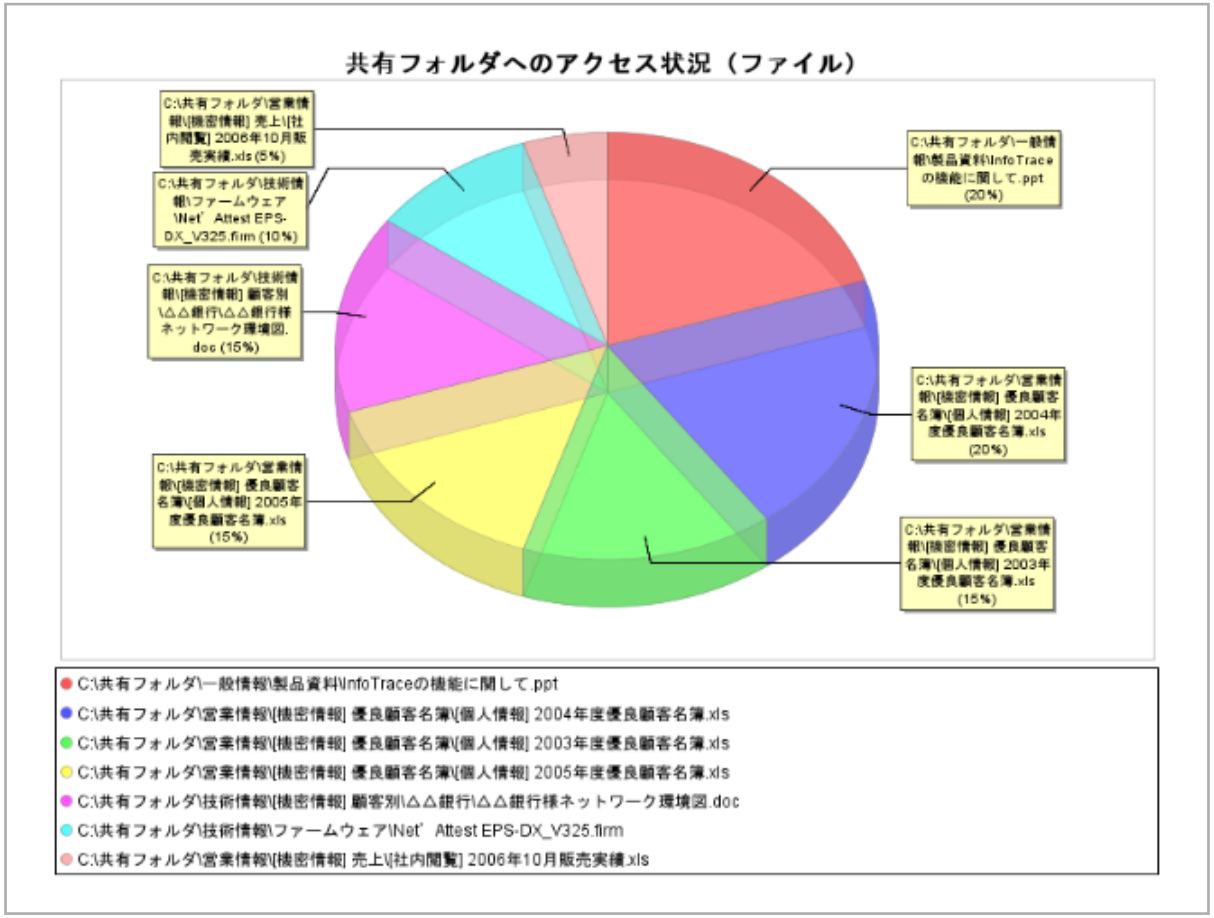
共有フォルダ作成レポート

概要　共有フォルダの作成履歴を出力します。
作成日　2015-09-03 09:41:45
対象期間　2015-08-05 00:00:00 - 2015-08-05 23:59:59

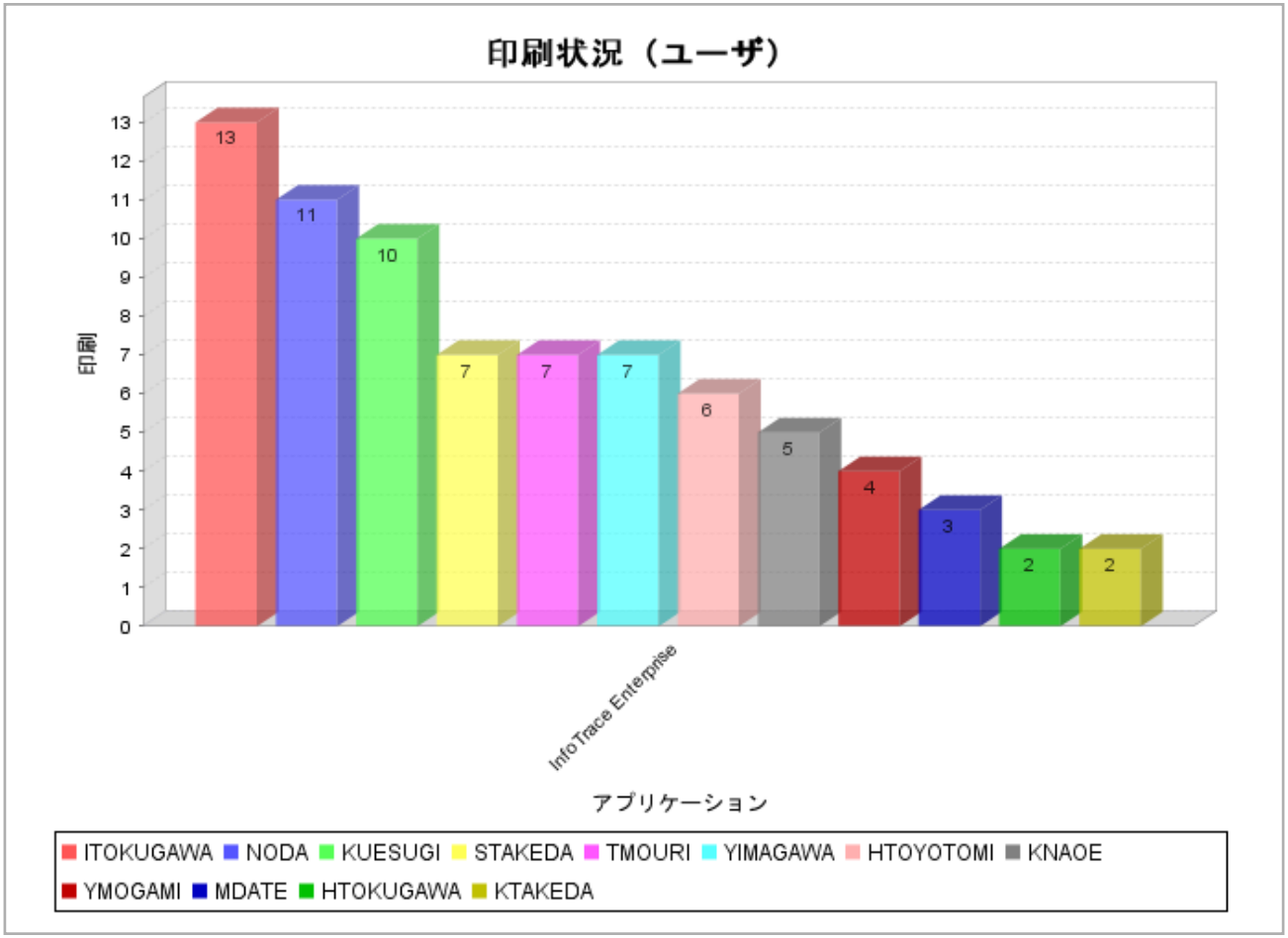
検索条件名　共有フォルダの作成レポート
概要
件数　1件

ﾀｲﾑｽﾀﾝﾌﾟ	ｱｸｼｮﾝ	コンピューター名	IPアドレス	ログイン名	パス / URL	操作種別	共有名
2015-08-05 13:50:45	フォルダ共有	YAMADA-WORK	192.168.0.1	yamada	C:¥Temp¥vmshare	作成	vmshare

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