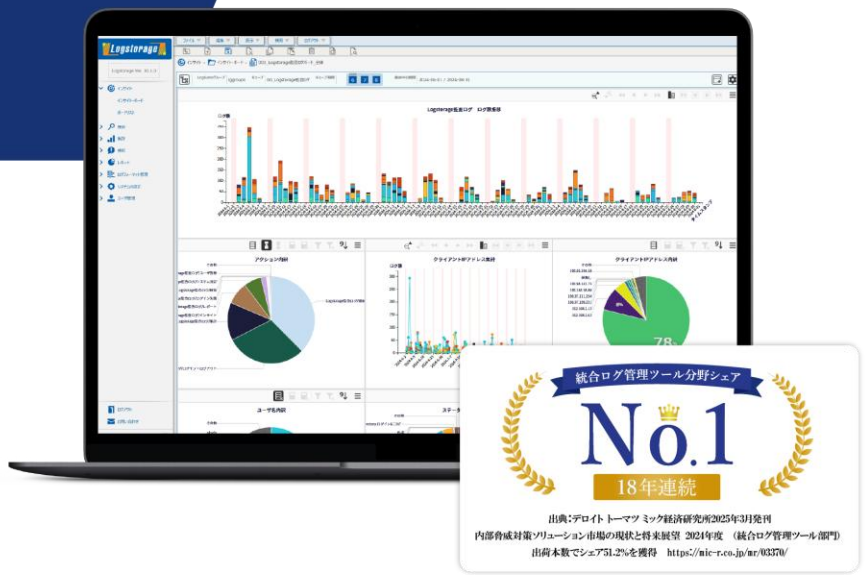
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage CWAT 連携パック
参考資料



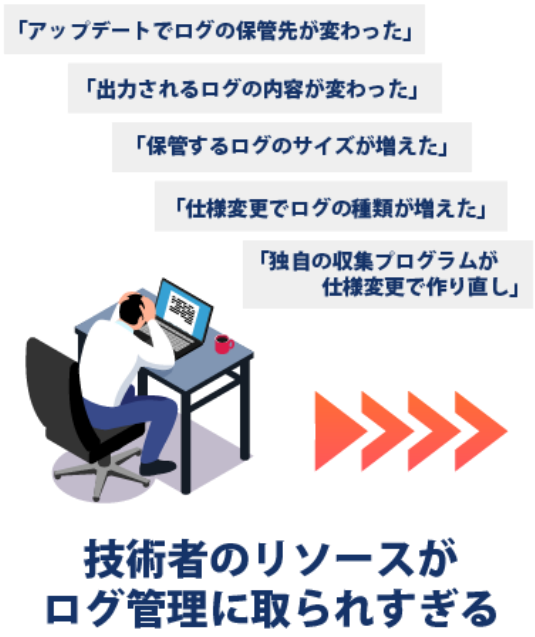
Infoscience
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

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

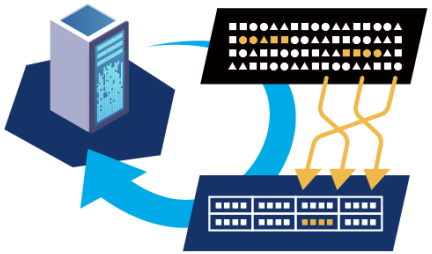
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

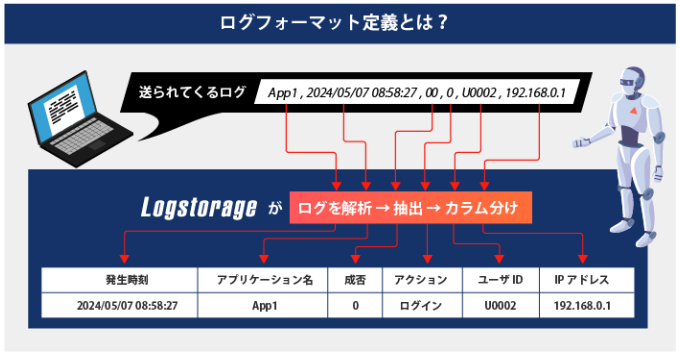
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※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



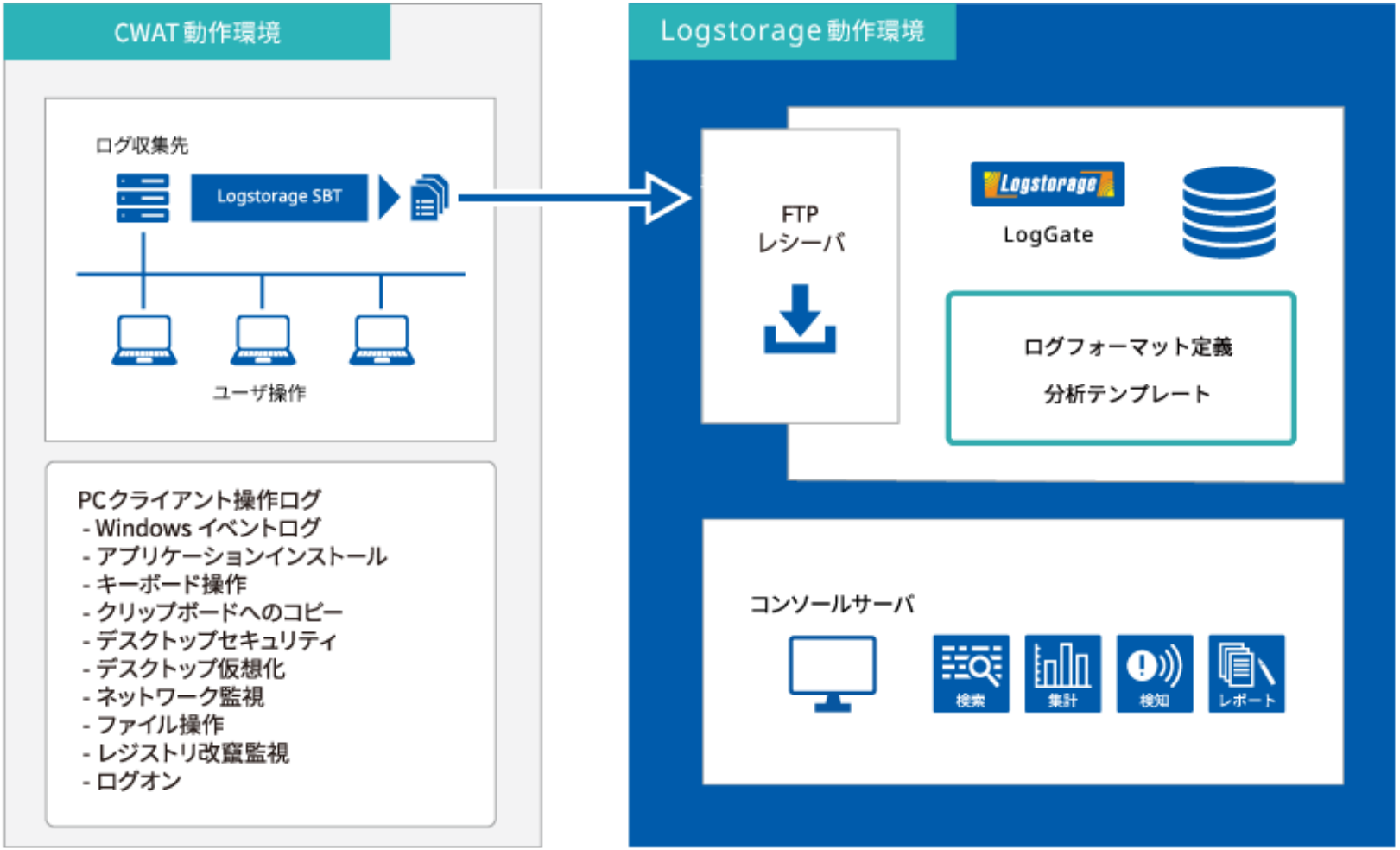
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



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 CWAT 連携パック の検索テンプレートは以下の通りです。

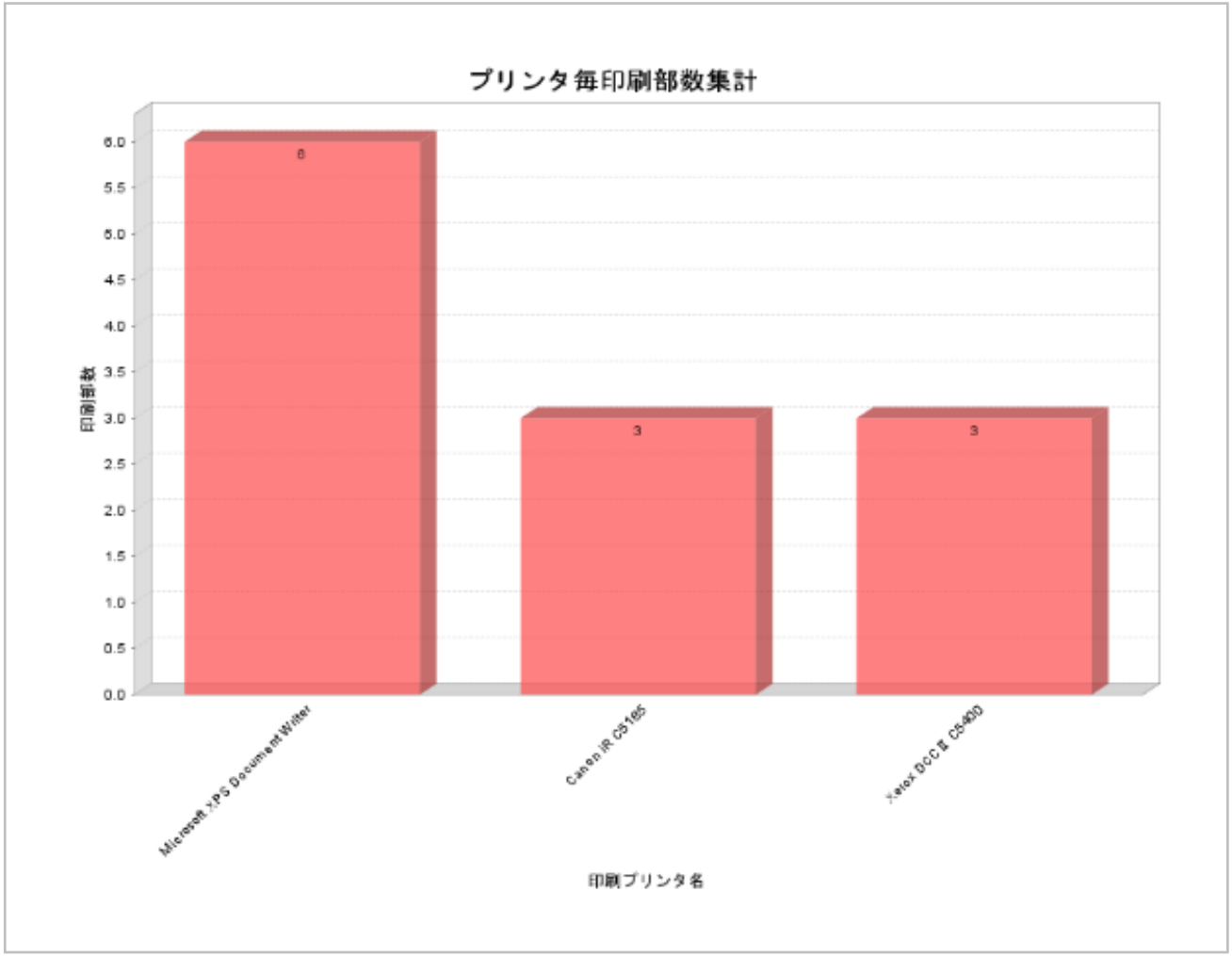
検索条件テンプレート名	
CWAT CDWriter	デスクトップセキュリティ
DeviceMonitor	デスクトップ仮想化
Exchange メール送信	ネットワーク監視
IE HTTP	ファイル操作
Messenger(MSN・QQ)	レジストリ改竄監視
OPDC の停止	ログオン
Read/WriteBlock	他CD Writer によるファイル書き出し遮断
SMTP メール送信	印刷
Windows イベントログ	時間管理
アプリケーション	暗号
アプリケーションインストール	未登録端末検知
キーボード操作	監査ログ書き込み容量不足
クリップボードへのコピー	-

集計テンプレート一覧

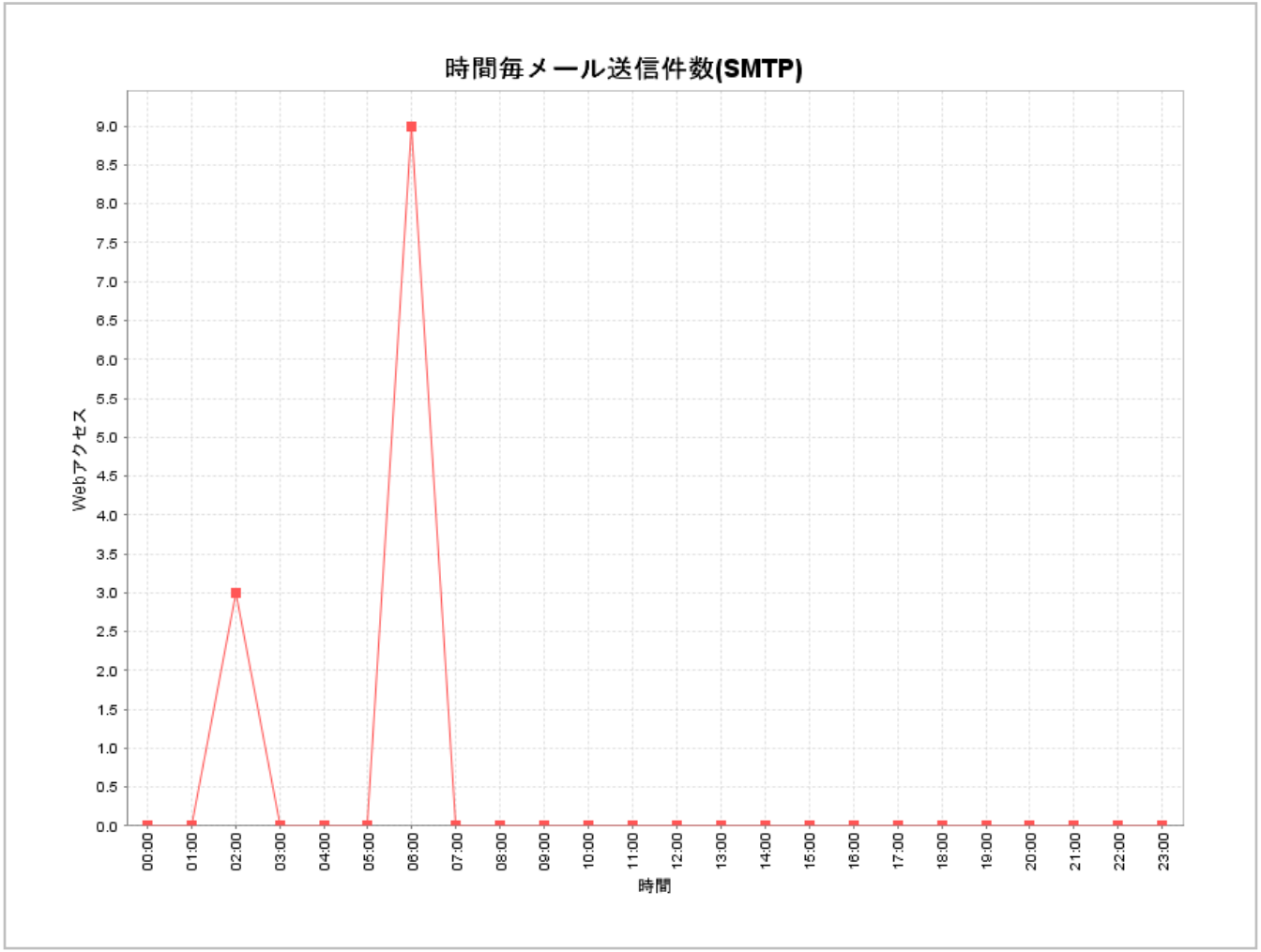
Logstorage CWAT 連携パック の集計テンプレートは以下の通りです。

集計条件テンプレート名
プリンタ毎印刷部数集計
ユーザ毎メール送信件数(SMTP)
ユーザ毎メール送信件数(Webメール)
ユーザ毎印刷部数集計
時間毎メール送信件数(SMTP)
時間毎メール送信件数(Webメール)

レポート例 1



レポート例 2



レポート例 3

アプリケーションインストール履歴

概要

作成日	2010-09-14 11:12:34
対象期間	2010-08-01 00:00:00 - 2010-08-31 23:59:59

検索条件名	アプリケーションインストール履歴
概要	
件数	6件

ﾀｲﾑｽﾀﾝﾌﾟ	端末ホスト名	端末IP アドレス	端末MAC アドレス	イベント紐付きユーザ名	インストールアプリケーショ	イベント紐付きプロセス名
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe
2010-08-31 09:10:03	cmst-bd90184e90	192.168.1.3	00-0C-29-3F-18-D2	cmst	Virus Chaser	C:\PROGRA~1\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe

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