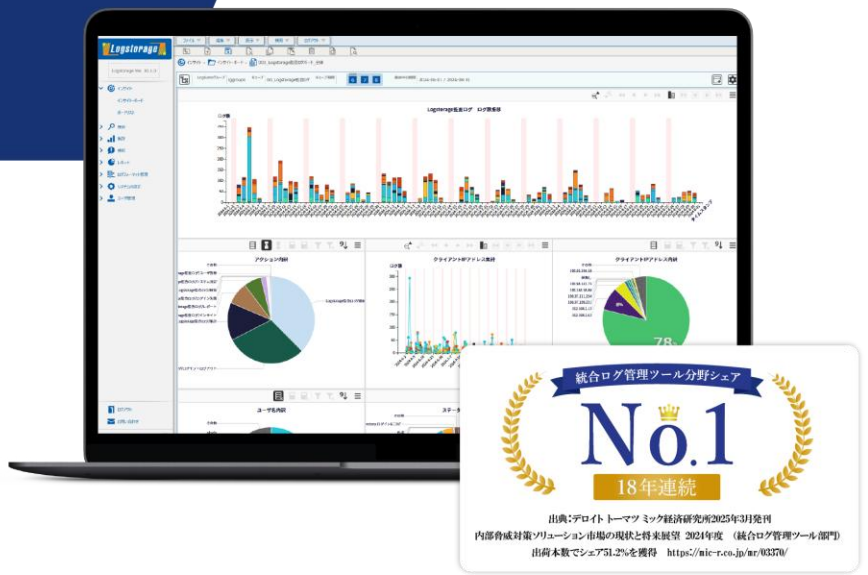
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage LANSCOPE 連携パック
参考資料



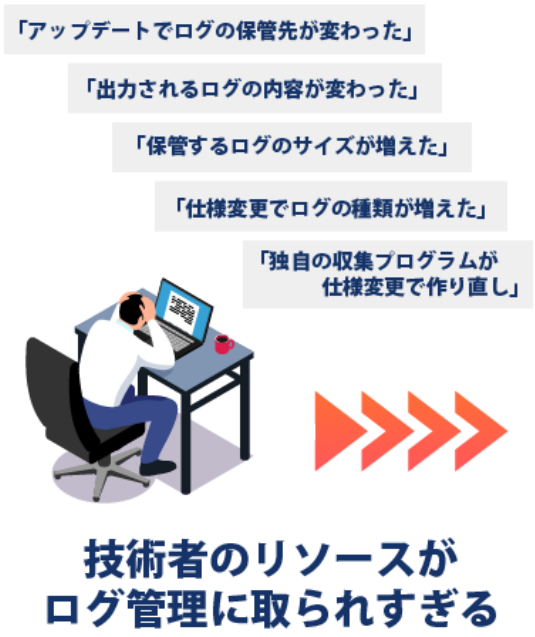
Infoscience
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

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。



Infoscience Copyright © Infoscience Corporation All Rights Reserved.

パッケージ内容

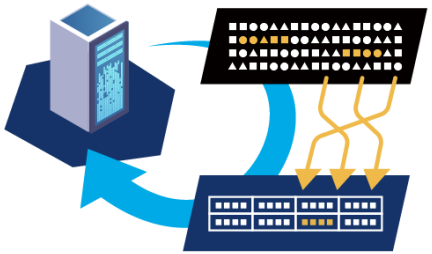
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

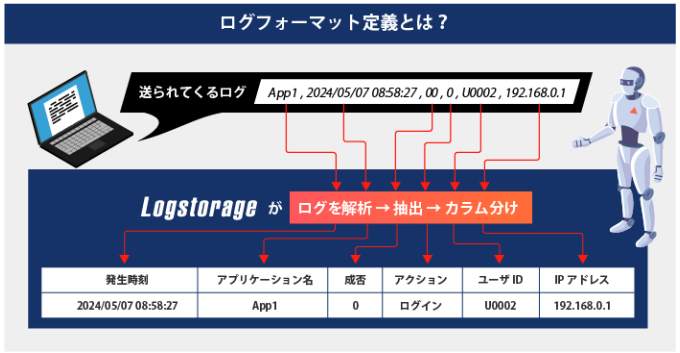
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※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。

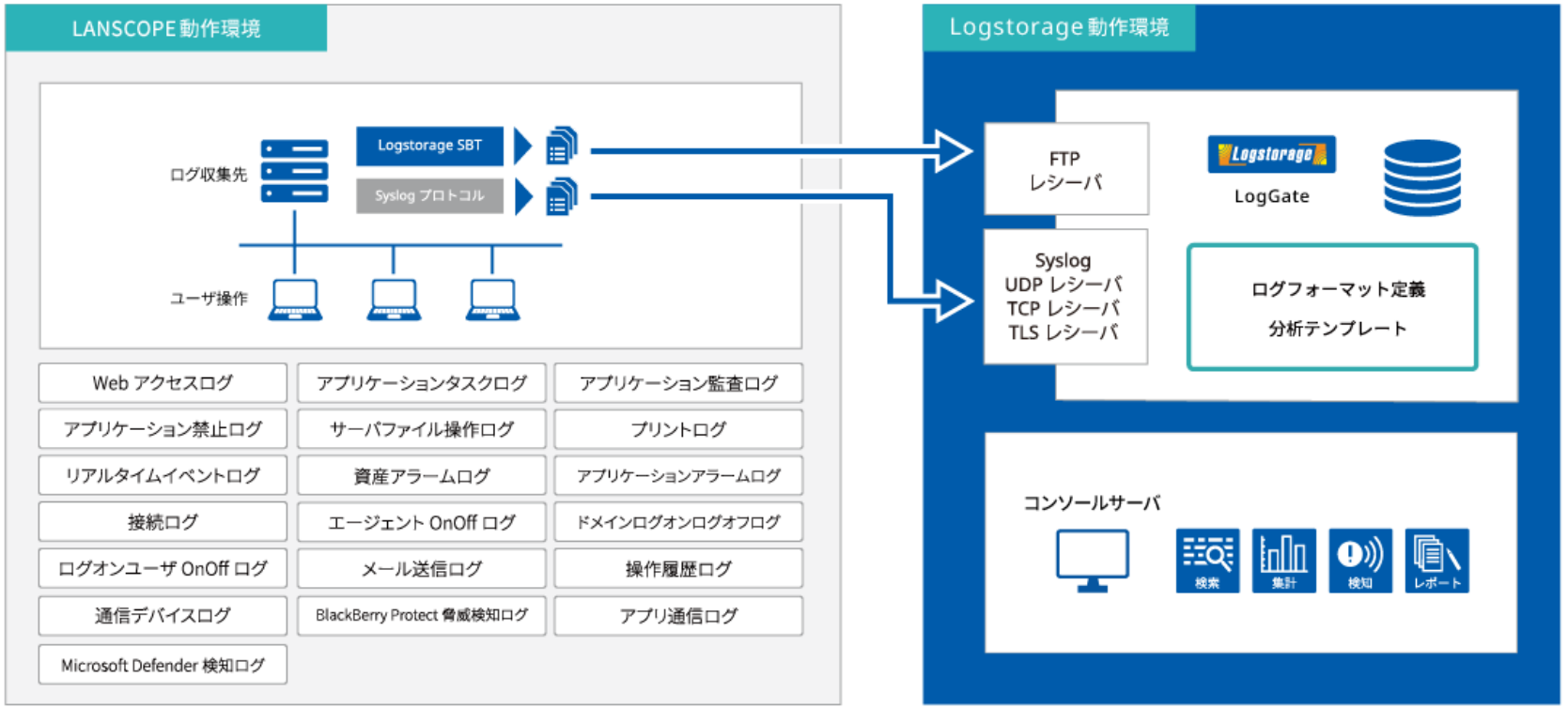


分析テンプレート

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。

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

システム構成



Infoscience Copyright © Infoscience Corporation All Rights Reserved.

検索テンプレート一覧

検索

Logstorage LANSCOPE 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
BlackBerry Protect脅威検知ログ
Microsoft Defender検知ログ
Webアクセスログ
アプリケーションアラームログ
アプリケーションタスクログ
アプリケーション監査ログ
アプリケーション禁止ログ
アプリ通信ログ
サーバファイル操作ログ
ドメインログオンログオフログ
プリントログ
メール送信ログ
ユーザ別ファイル操作ログ一括出力（アラーム出力）
リアルタイムイベントログ
ログオンユーザOnOffログ
接続ログ
資産アラームログ
通信デバイスログ

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

集計・レポートテンプレート一覧

集計-1 レポート-1

Logstorage LANSCOPE 連携パック の集計及びレポートテンプレートは以下の通りです。

ファイル名	集計・レポート条件テンプレート名
WEBアクセス	WEBアクセス稼働時間集計
WEBアクセス	アラームキーワード別回数
WEBアクセス	エージェント別 ダウンロード/アップロード回数
WEBアクセス	エージェント別 禁止/警告のアラーム回数
WEBアクセス	タイトル別WEBアクセス回数
アプリケーション禁止	禁止アプリケーション別起動回数
アプリケーション稼働	アプリケーションタスク稼働時間集計
アプリケーション稼働	アプリケーション別起動回数
サーバファイル操作	クライアントユーザ別アラーム
サーバファイル操作	クライアント別ファイルアクセス
サーバファイル操作	クライアントユーザ別ファイル操作失敗回数
プリント	エージェント別印刷枚数集計
プリント	ドキュメント別集計
プリント	プリンタ別集計
リアルタイムイベント	PC別ログオンユーザ一覧
リアルタイムイベント	デバイス使用回数推移
リアルタイムイベント	リアルタイムイベント稼働時間集計
リアルタイムイベント	外部持ち出しファイル一覧
リアルタイムイベント	時間外操作回数

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

集計・レポートテンプレート一覧

集計-2

レポート-2

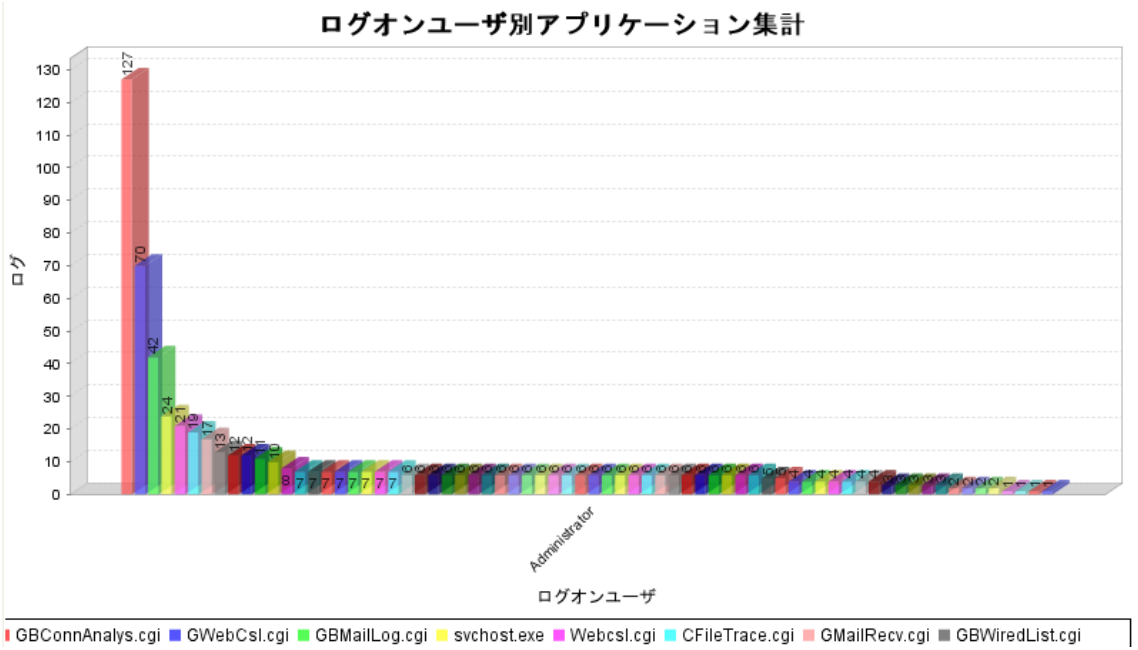
ファイル名	集計・レポート条件テンプレート名
不正PC検知	セグメント別MR稼働台数集計
不正PC検知	セグメント別アラームノード一覧
不正PC検知	セグメント別アラームノード推移
不正PC検知	不正接続アラーム推移
アラーム別件数推移	-

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例 1

アプリケーション稼働ログ

ログオンユーザ	アプリケーション	ログ件数
Administrator	GBConnAnalys.cgi	127
	GWebCsl.cgi	70
	GBMailLog.cgi	42
	svchost.exe	24
	Webcsl.cgi	21
	CFileTrace.cgi	19
	GMailRecv.cgi	17
	GBWiredList.cgi	13
	LSPSRVANY.EXE	12
	LSPSRVG.EXE	12
	LSPQUEST.EXE	11
	MPU.exe	10
	WinMgmt.exe	8
	CLaunch.exe	7
	Explorer.EXE	7
	Winampa.exe	7
	ctfmon.exe	7
	hkcmd.exe	7
	igfxpers.exe	7
	[illegible]	7

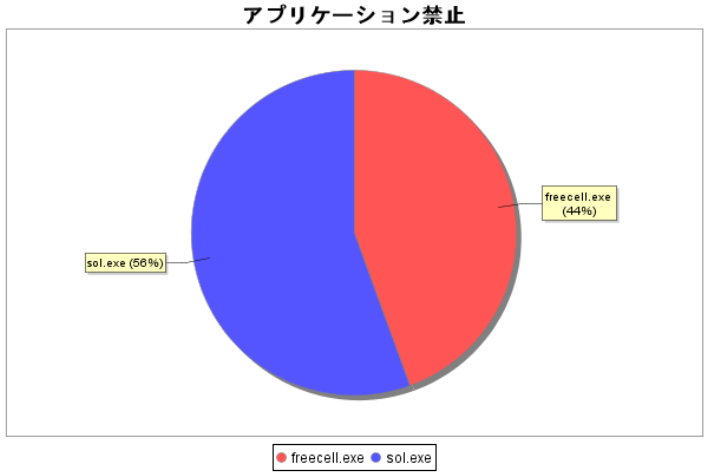


ログオンユーザ別アプリケーション集計

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例 2

アプリケーション禁止ログ



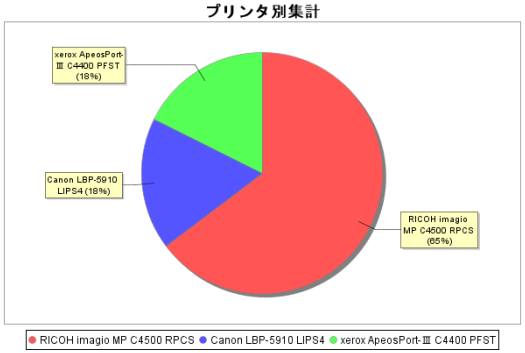
エージェント	禁止アプリケーション	起動件数
須藤　隆	sol.exe	5
	freecell.exe	0
内田　健太	freecell.exe	4
	sol.exe	0
総合計		9

ログオンユーザ別アプリケーション集計

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例３

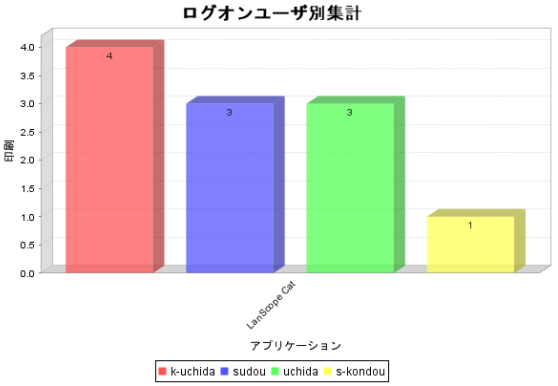
プリントログ



プリンタ	印刷
	件数
RICOH imagio MP C4500 RPCS	11
Canon LBP-5910 LIPS4	3
xerox ApeosPort-Ⅲ C4400 PFST	3
総合計	17

プリンタ別集計

ログオンユーザ	印刷
	件数
k-uchida	4
sudou	3
uchida	3
s-kondou	1
総合計	11



ログオンユーザ別集計

エージェント	印刷
	件数
内田　健太	7
近畑　慎一	1
須畑　陸	3
総合計	11

PC別集計

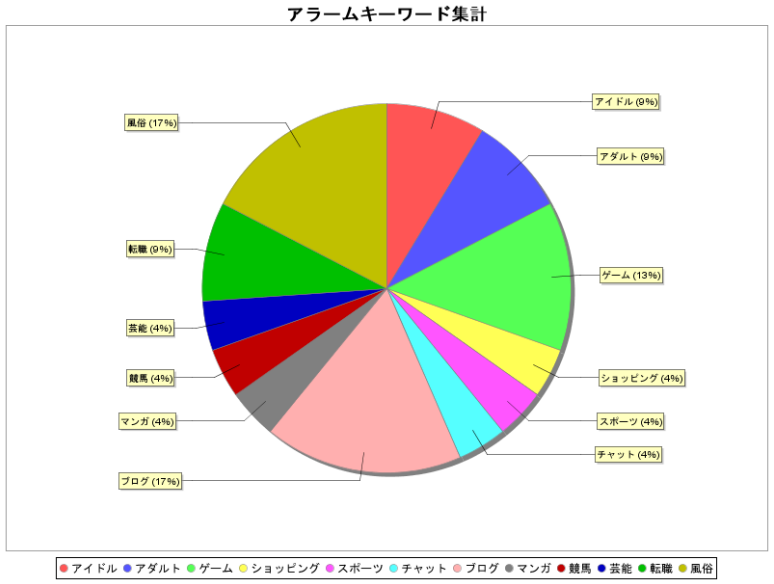
ドキュメント	印刷
	件数
2007年度分.doc	1
2008年度分.doc	1
名簿.txt - メモ帳	1
得意先.doc	1
採用地域リスト(東日本).txt - メモ帳	1
採用地域リスト(西日本).txt - メモ帳	1

ドキュメント別集計

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例４

Webアクセスログ



アラームキーワード集計

ログオンユーザ	Webタイトル	アクセス件数
SYSTEM	芸能：MSN毎日 インタラクティブ - Microsoft Internet Explorer	10
	MSN Japan - Microsoft Internet Explorer	3
	速報：MSN毎日 インタラクティブ - Microsoft Internet Explorer	2
	MSN スポーツ - Microsoft Internet Explorer	1
	MSN-Mainichi INTERACTIVE 芸能 - Microsoft Internet Explorer	1
	MSN毎日 インタラクティブ - Microsoft Internet Explorer	1
	http://www.jp.msn.com/ - Microsoft Internet Explorer	1
	http://www.mainichi-msn.co.jp/entertainment/geinou/200603/graph/22_2/1.html - Microsoft Internet Explorer	1
	http://www.mainichi-msn.co.jp/entertainment/geinou/200607/graph/05_2/3.html - Microsoft Internet Explorer	1
	http://www.mainichi-msn.co.jp/entertainment/geinou/200607/graph/05_2/7.html - Microsoft Internet Explorer	1
	http://www.msn.co.jp/ - Microsoft Internet Explorer	1
	http://www.msn.co.jp/home.armx - Microsoft Internet Explorer	1
	今日の話題：MSN毎日 インタラクティブ - Microsoft Internet Explorer	1
	写真特集：MSN毎日 インタラクティブ - Microsoft Internet Explorer	1
	MS:巨額制裁金、日本の事業には影響なし－企業：MSN毎日 インタラクティブ - Microsoft Internet Explorer	1
総合計		27

ユーザ別Web使用回数集計

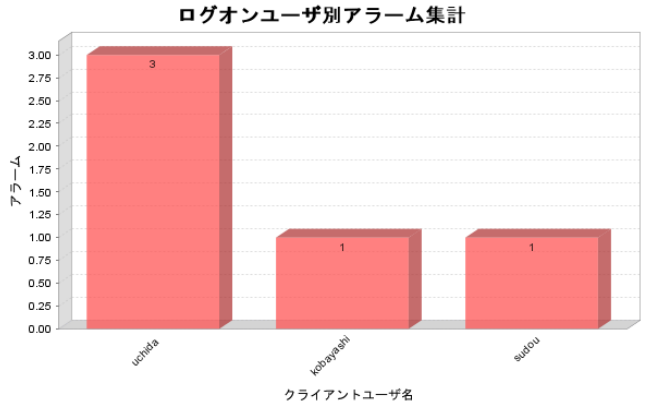
Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例 5

サーバ監視ログ

クライアントユーザ名	ファイルパス	アクセス 件数
uchida	C:¥【社外秘】営業部¥取引先住所データ.xls	2
	C:¥【社外秘】営業部¥営業1課用¥取引先住所データ.xls	2
	C:¥【社外秘】営業部¥営業1課用¥営業データ.xls	2
	C:¥【社外秘】営業部¥営業1課用¥得意先.doc	2
	C:¥【社外秘】営業部¥営業データ.xls	2
	C:¥【社外秘】営業部¥得意先.doc	2
	C:¥【社外秘】営業部¥データ確認用¥個人実績フォルダ¥【個人実績】2007年10月(仮).xls	1
	C:¥【社外秘】営業部¥データ確認用¥個人実績フォルダ¥【個人実績】2007年10月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥個人実績フォルダ¥【個人実績】2007年8月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥個人実績フォルダ¥【個人実績】2007年9月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥取引先住所データ.xls	1
	C:¥【社外秘】営業部¥データ確認用¥営業データ.xls	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥【実績】2007年10月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥【実績】2007年8月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥【実績】2007年9月.xls	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥【実績】2007年総計.xls	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥確認用¥2007年度分.doc	1
	C:¥【社外秘】営業部¥データ確認用¥実績フォルダ¥確認用¥2008年度分.doc	1
	C:¥【社外秘】営業部¥データ確認用¥得意先.doc	1
	C:¥【社外秘】営業部¥営業1課用	1
	C:¥【社外秘】営業部¥実績フォルダ¥確認用¥2007年度分.doc	1
	C:¥【社外秘】営業部¥新しいフォルダ	1
総合計		28

ログオンユーザ別ファイルアクセス集計



クライアントユーザ名	操作	アラーム 件数
uchida	削除	3
kobayashi	削除	1
sudou	削除	1
総合計		5

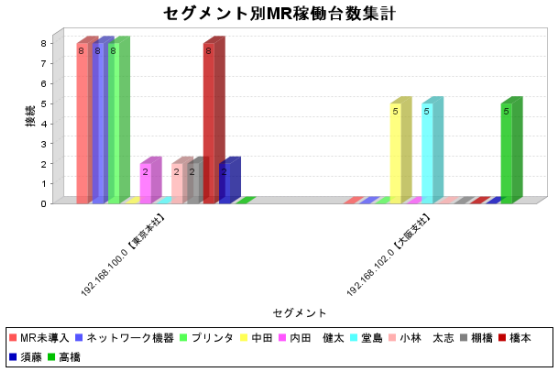
ログオンユーザ別アラーム集計

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例 6

不正PC検知ログ

セグメント	ノード	接続 件数
192.168.100.0【東京本社】	MR未導入	8
	ネットワーク機器	8
	プリンタ	8
	中田	0
	内田　健太	2
	堂島	0
	小林　太志	2
	棚橋	2
	橋本	8
	須藤	2
	高橋	0
192.168.102.0【大阪支社】	MR未導入	0
	ネットワーク機器	0
	プリンタ	0
	中田	5
	内田　健太	0
	堂島	5
	小林　太志	0
	棚橋	0
	橋本	0
	須藤	0
	高橋	5



セグメント別MR稼働台数集計

セグメント	ノード	接続 件数
192.168.100.0【東京本社】	0001 30FE8070	0
	000D56FD0E75	0
	000E7FAC554E	8
	0016D329F384	2
192.168.102.0【大阪支社】	0001 30FE8070	1
	000D56FD0E75	1
	000E7FAC554E	0
	0016D329F384	0

セグメント別MR未稼働台数集計

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

レポート例 7

リアルタイムイベントログ

ウィンドウタイトル	ログ件数
Program Manager	327
Shell_TrayWnd	284
送信済みアイテム - Microsoft Outlook	74
スタート メニュー	56
ホームページアラーム - Microsoft Internet Explorer	45
Outlook 送受信の進行度	39
MSN Japan - Microsoft Internet Explorer	36
サービス	35
Webアクセスアラーム設定	32
ファイルのダウンロード	32

ウィンドウタイトル別集計

ファイル	ログ件数
C:¥Documents and Settings¥motex¥デスクトップ¥新規Microsoft PowerPoint プレゼンテーション.ppt	5
C:¥Documents and Settings¥motex¥デスクトップ¥新事業計画案(仮)¥~$Microsoft Word 文書.doc	4
C:¥Documents and Settings¥sudou¥デスクトップ¥~$A会社資料.doc	4
C:¥Documents and Settings¥sudou¥デスクトップ¥新規Microsoft Word 文書.doc	4
C:¥Documents and Settings¥sudou¥デスクトップ¥新規テキストドキュメント.txt	4
C:¥Documents and Settings¥Administrator¥デスクトップ¥15期売り上げ.xls	3
C:¥Documents and Settings¥sudou¥My Documents¥My Music¥iTunes¥iTunes Music¥Marc Seales	3
C:¥Documents and Settings¥uchida¥Local Settings¥Application Data¥Microsoft¥CD Burning¥TEST	3
C:¥Documents and Settings¥uchida¥デスクトップ¥商品案内.xls	3
C:¥Documents and Settings¥uchida¥デスクトップ¥新規Microsoft Word 文書.doc	3

アクセスファイル別集計

エージェント	ログオンユーザ	ログ件数
内田 健太	Administrator	44
	SYSTEM	147
	k-uchida	96
	motex	0
	murata	174
	sudou	0
	uchida	1027
須藤 隆	Administrator	0
	SYSTEM	0
	k-uchida	0
	motex	0
	murata	0
	sudou	809
	uchida	0
小林 太志	Administrator	0
	SYSTEM	1
	k-uchida	0
	motex	203
	murata	0
	sudou	0
	uchida	0

PC別ログオンユーザー一覧

Infoscience Copyright © Infoscience Corporation All Rights Reserved.

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

Infoscience Copyright © Infoscience Corporation All Rights Reserved.