



～ 統合ログ管理システム ～

Logstorage MylogStar 連携パック のご紹介

Infoscience

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

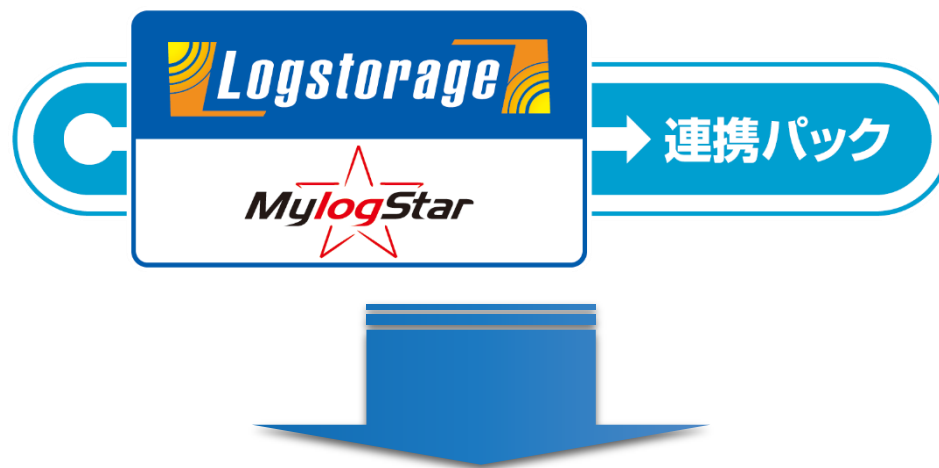
Logstorage MylogStar 連携パック



統合ログ管理シェアNo.1 のLogstorage が MylogStar に特化!!

国内シェアNo.1の Logstorage に MylogStar が記録するPC操作ログの活用に必要な全機能を搭載し、パッケージ化しました。

素早く・簡単にログを活用することができ、他システムのログも統合した分析を可能とします。



統合ログ管理は全て「Logstorage」が解決！！

他のシステム・機器のログとの統合

「Logstorage」ではインフォサイエンスが特許を持つログフォーマット定義機能により、異なるフォーマットを持つログの違いを吸収し、ログを統合的・横断的に分析する事が可能です。

例えば「MylogStar」で収集したPC操作ログと、入退出管理システム、複合機等の物理デバイスのログも統合し、フロアへの出入り、サーバー上での操作、紙の印刷など、ITシステム上での全てのアクティビティを、ログから時系列で追跡・分析する事が可能になります。

ログの長期保管・高速検索・原本性の証明

「MylogStar」にて記録したログを自動収集し圧縮することで長期保管を可能にします。また、収集したログに対してインデックスを作成し、より高速な検索を実現しています。

さらに、保管しているログに対して電子署名を生成する機能により、ログの改竄検出や原本性の証明が可能となります。

柔軟なレポーティング機能

「Logstorage MylogStar連携パック」は、「MylogStar」が記録したログに対するレポートテンプレートを用意しているほか、レポート内容をGUI上で自由に設定・カスタマイズする機能があります。レポートテンプレートをベースに、自社のセキュリティポリシーに合った、様々な角度からのレポート出力が可能となるため、セキュリティ・インシデントの予見、防止につながります。

ログの検索～絞り込み

検索条件
検索結果
カラムセットアサイン

LogGateグループ: Group12 ☐アーカイブ検索

期間指定: 今日 昨日 先週 先月

2010年 2月 3日 0時 0分 0秒 から
 2010年 2月 3日 23時 59分 59秒 まで

● アプリケーション

アプリケーション: MylogStar --

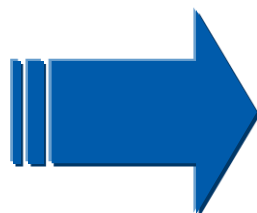
アクション: 全て

- 全て
- Eメール
- FTP
- TCPセッション
- アプリケーション
- イベント
- インターネット
- ウィンドウタイトル
- クリップボード
- ステータス
- スナップショット
- ドキュメント
- ファイル操作
- プリンタ
- メッセージャ
- ユーザ

☒ ログを改行しない
☐ 降順

検索
キャンセル

MylogStarのログが持つ、全てのイベント、項目での検索が可能

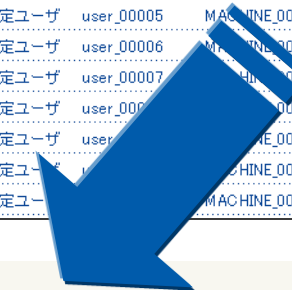


検索条件
検索結果
カラムセットアサイン

1 - 100件目表示(822件) 1 2 3 4 5 6 7 8 9 | NEXT ▶

タイムスタンプ	アクション	ユーザ識別子	部門名	ログイン名	マシン名	IPアドレス
2010-02-03 00:46:30	インターネット	MACHINE_00004	未設定ユーザ	user_00004	MACHINE_00004	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00000	未設定ユーザ	user_00000	MACHINE_00000	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00001	未設定ユーザ	user_00001	MACHINE_00001	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00003	未設定ユーザ	user_00003	MACHINE_00003	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00005	未設定ユーザ	user_00005	MACHINE_00005	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00006	未設定ユーザ	user_00006	MACHINE_00006	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00007	未設定ユーザ	user_00007	MACHINE_00007	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00008	未設定ユーザ	user_00008	MACHINE_00008	192.168.0.
2010-02-03 00:46:30	インターネット	MACHINE_00009	未設定ユーザ	user_00009	MACHINE_00009	192.168.0.
2010-02-03 02:33:33	ドキュメント	MACHINE_00004	未設定ユーザ	user_00004	MACHINE_00004	192.168.0.
2010-02-03 02:33:33	ドキュメント	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.

クリック



検索条件
検索結果
カラムセットアサイン

1 - 25件目表示(25件) 1

タイムスタンプ	アクション	ユーザ識別子	部門名	ログイン名	マシン名	IPアドレス
2010-02-03 00:46:30	インターネット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 02:33:33	ドキュメント	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 03:01:11	アプリケーション	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 03:20:29	スナップショット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 04:18:18	アプリケーション	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 04:46:10	インターネット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 04:47:44	ドキュメント	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 08:00:18	TCPセッション	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 08:28:24	スナップショット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.
2010-02-03 09:41:33	FTP	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0.

絞り込み結果

クリックしたログインユーザ名で絞り込まれた

ログの横断分析

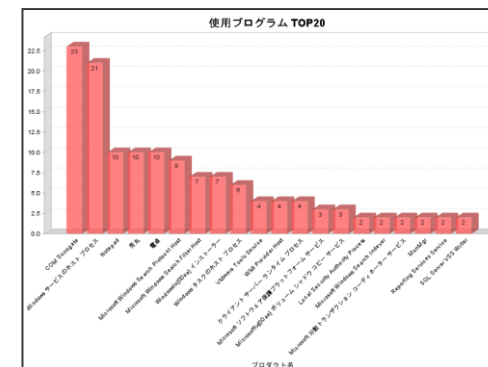
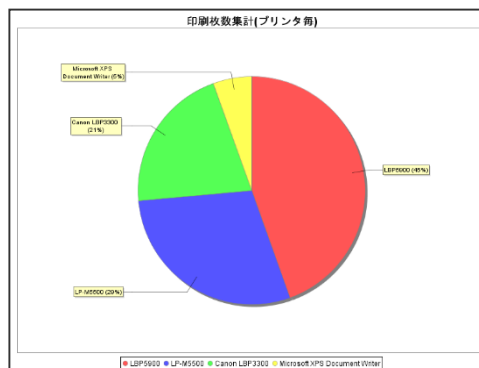
Logstorage の機能により、異なるフォーマットを持つログの違いを吸収し、統合的・横断的に扱う事が可能となります。

例えば、MylogStarで記録したPC操作ログと、入退室管理システム、複合機等の物理装置のログや、各種システムの認証ログなどを統合することにより、横断的な検索や分析を行うことができます。

検索条件		検索結果	コラムセッタサイン		ユーザID「yamada」での横断検索	
1 - 41 件目表示 (41 件)						
タイムスタンプ	ユーザID	アプリケーション	アクション	対象	ログメッセ	
2009-02-15 08:56:00	yamada	e-SG	カード認証OK(入室)	01011001(扉1-1)	e-SG: 9	
2009-02-15 08:58:27	yamada	SmartOn	Windows ログオン成功	PC01	SmartOn	
2009-02-15 09:17:23	yamada	ApeosPort-II	コピー		ApeosPort-II	
2009-02-15 10:24:37	yamada	SmartOn	コンピュータロック	PC01	SmartOn	
2009-02-15 10:25:00	yamada	e-SG	カード認証OK(退室)	01011001(扉1-1)	e-SG: 8	
2009-02-15 10:29:00	yamada	e-SG	カード認証OK(入室)	01011001(扉1-1)	e-SG: 9	
2009-02-15 10:30:00	yamada	SmartOn	コンピュータロック解除	PC01	SmartOn	
2009-02-15 10:30:12	yamada	ALogコンバータ	ファイル読み込み	C:\共有フォルダ\持出厳禁\顧客名簿2009.doc	ALogコンバータ	
2009-02-15 10:30:32	yamada	ALogコンバータ	ファイル読み込み	C:\共有フォルダ\持出厳禁\顧客名簿.doc	ALogコンバータ	
2009-02-15 10:31:00	yamada	MylogStar	ファイル操作	顧客名簿.doc	MylogStar	
2009-02-15 11:29:42	yamada	MylogStar	プリンタ	PDT0613C.pdf	MylogStar	
2009-02-15 11:29:42	yamada	ApeosPort-II	プリント	PDT0613C.pdf	ApeosPort-II	
2009-02-15 12:02:09	yamada	SmartOn	コンピュータロック	PC01	SmartOn	
2009-02-15 12:03:00	yamada	e-SG	カード認証OK(退室)	01011001(扉1-1)	e-SG: 8	
2009-02-15 12:49:00	yamada	e-SG	カード認証OK(入室)	01011001(扉1-1)	e-SG: 8	
2009-02-15 12:57:00	yamada	SmartOn	コンピュータロック解除	PC01	SmartOn	

多彩なレポート機能

マシン名	OS バージョン	クライアント バージョン	ログ 件数
MACHINE_00000	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00001	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00002	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00003	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00004	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00005	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00006	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00007	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00008	Windows XP Professional SP2	12.5.1.101	1
MACHINE_00009	Windows XP Professional SP2	12.5.1.101	1
WIN-1 R24AMG47GL	Windows 7 Ultimate	12.5.1.101	2
総 合 計			12



レポートの**定期・自動出力**
(日次、週次、月次、1時間毎レポート)

随時更新される豊富な
レポートテンプレート

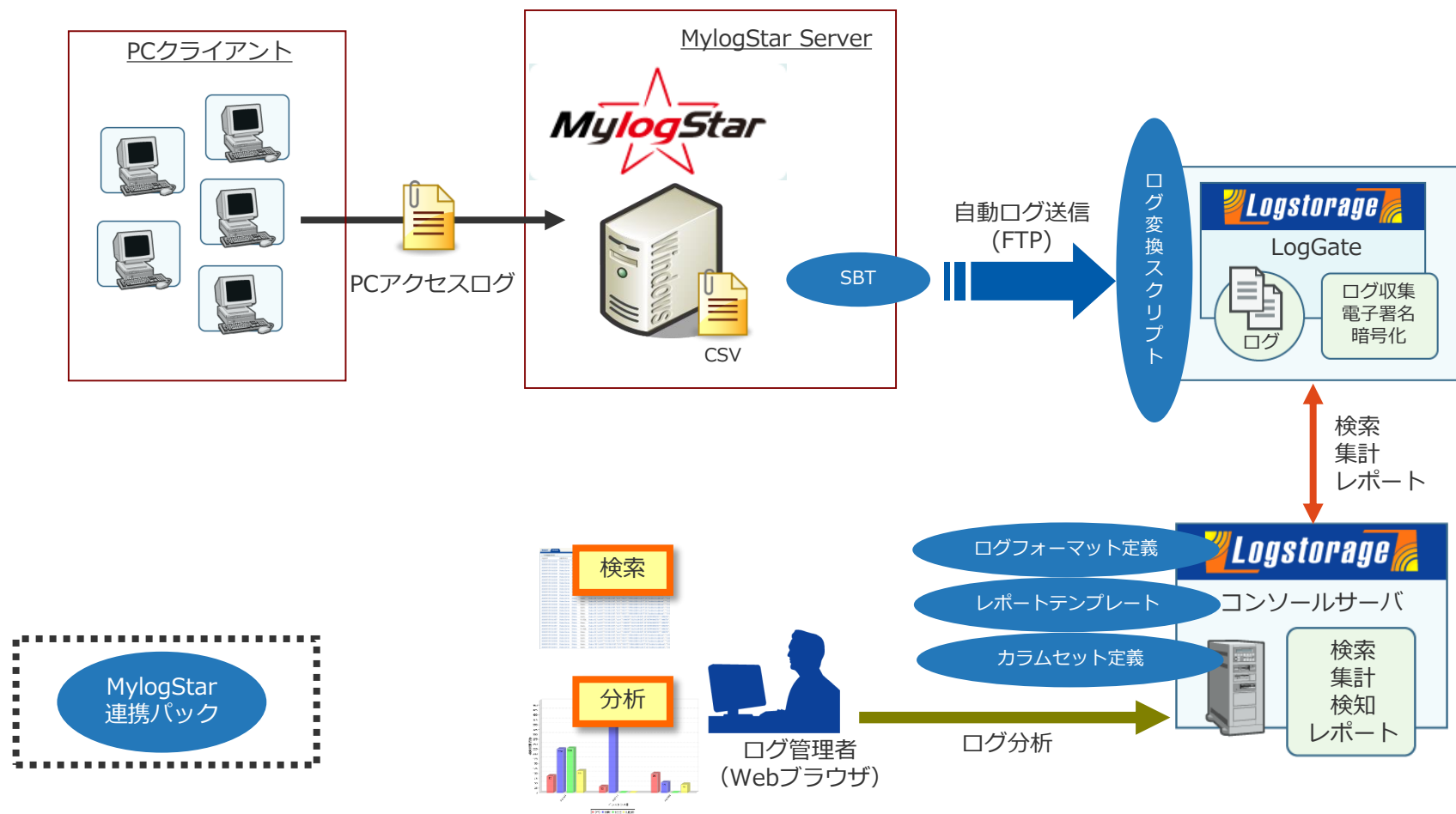
直感的なGUI画面より、お客様自身が自由
にテンプレート作成可能

多様なフォーマットで出力可能
他システムとの連携が容易

Logstorage + MylogStar システム構成



システム構成



※LogGateとコンソールサーバは同一筐体内でも動作可能です

Logstorage MylogStar 連携パック内容	
SBT	MylogStarから出力されたログを、Logstorage に自動送信するプログラム
ログ変換スクリプト	MylogStarのログをLogstorage フォーマットに自動変換して保存。 自動変換スクリプトを標準設定
ログフォーマット定義	MylogStarのログフォーマット定義（全項目）を標準設定
カラムセット定義	MylogStarの検索結果画面を標準設定
レポートテンプレート	MylogStarのレポートテンプレートを標準設定

検索条件						
検索結果						
カラムセットアサイン						
1 - 100件目表示(822件) 1 2 3 4 5 6 7 8 9 NEXT ▶						
タイムスタンプ	アクション	ユーザ識別子	部門名	ログイン名	マシン名	IPアドレス
2010-02-03 00:46:30	インターネット	MACHINE_00004	未設定ユーザ	user_00004	MACHINE_00004	192.168.0
2010-02-03 00:46:30	インターネット	MACHINE_00002	未設定ユーザ	user_00002	MACHINE_00002	192.168.0
2010-02-03 00:46:30	インターネット	MACHINE_00000	未設定ユーザ	user_00000	MACHINE_00000	192.168.0
2010-02-03 00:46:30	インターネット	MACHINE_00001	未設定ユーザ	user_00001	MACHINE_00001	192.168.0

カラムセット定義
(検索結果画面)

● アプリケーション

アプリケーション: MylogStar

アクション: FTP

メッセージパラメータ: 全て

全て
FTPコマンド
IPアドレス
MACアドレス
アラーム警告
コマンドデータ
マシン名
ユーザ識別子
ログイン名
ログ生成時刻
ログ種別名
取得時刻
検索条件名
送信元アドレス
送信元ポート
送信先アドレス
送信先ポート
部門名

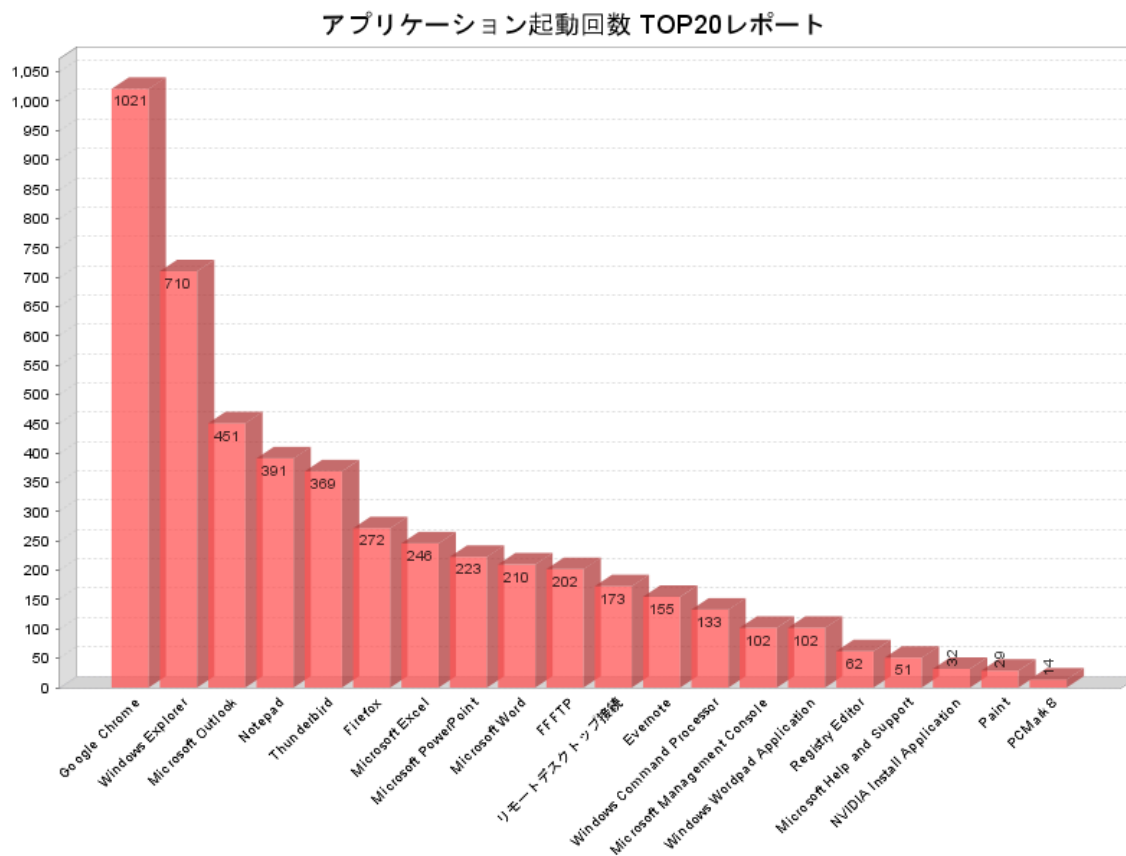
ログを改行しない ☐ 降順検索

キャンセル

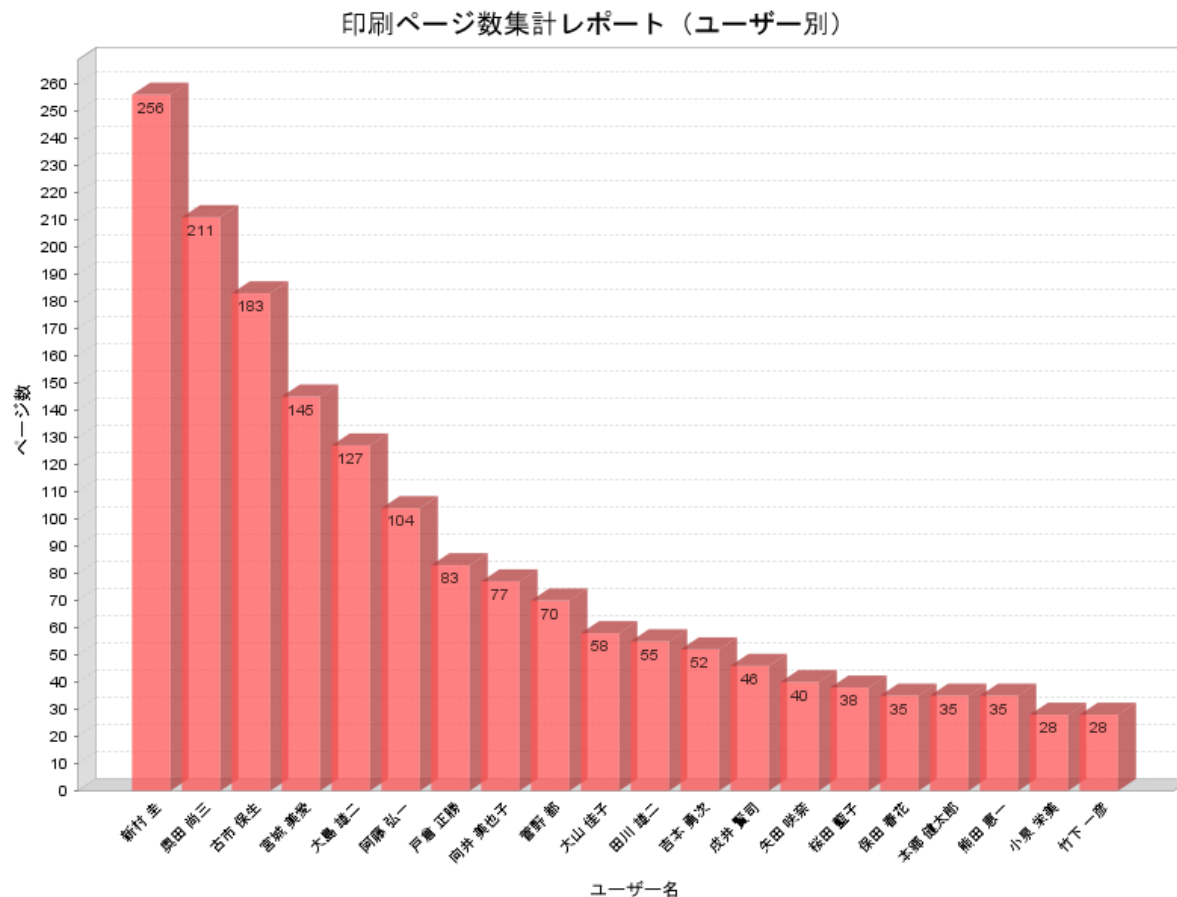
ログフォーマット定義
(検索条件画面例)

レポートテンプレート名	内容
アプリケーション起動回数 TOP20 レポート	ユーザー指定/全体指定で、指定期間におけるアプリケーション起動回数のTOP20を表示。
印刷ページ数集計レポート（ユーザー別）	指定期間におけるユーザー毎/全体の印刷ページ数の集計をグラフ表示。 プリンターログの「ページ数」を集計表示。
印刷ページ数集計レポート（月別・日別）	ユーザー指定/全体指定で、指定期間における月毎・日毎の印刷ページ数推移をグラフ表示。 プリンターログの「ページ数」を集計表示。
Webアクセス先ホスト名 TOP20 レポート	ユーザー指定/全体指定で、指定期間におけるWebアクセスの多いホスト名順にレポート表示。 SSLでのアクセスも集計対象とすることが可能。Webログの「ホスト名」をキーにログ件数を集計。
リムーバブルメディアへのファイルコピー ユーザー TOP20 レポート	指定期間におけるリムーバブルメディアへのファイルコピーの多いユーザー順にレポート表示。 ファイルログの「操作」が「COPY」、「操作後パス」が「REMOVABLE」をキーにログ件数を集計。
USBメモリへのファイルコピー 回数推移レポート	指定期間におけるリムーバブルメディアへのファイルコピーログ数を月別/日別に表示。 ファイルログの「操作」が「COPY」、「操作後パス」が「REMOVABLE」をキーにログ件数を集計。
Eメール送信先ドメイン TOP20 レポート	ユーザー指定/全体指定で、指定期間におけるEメール送信先ドメインのTOP20を表示。 Eメールログの「TO」を集計表示。
Eメール送受信件数レポート （月別/日別）	ユーザー指定/全体指定で、指定期間におけるEメール送信/受信の件数を、月別/日別に表示。 Eメールログの「送信/受信」をキーに集計して表示。
Eメール送受信件数レポート （ユーザー別）	ユーザー指定/全体指定で、指定期間におけるEメール送信/受信の件数をユーザー別に表示。 Eメールログの「送信/受信」をキーに集計して表示。

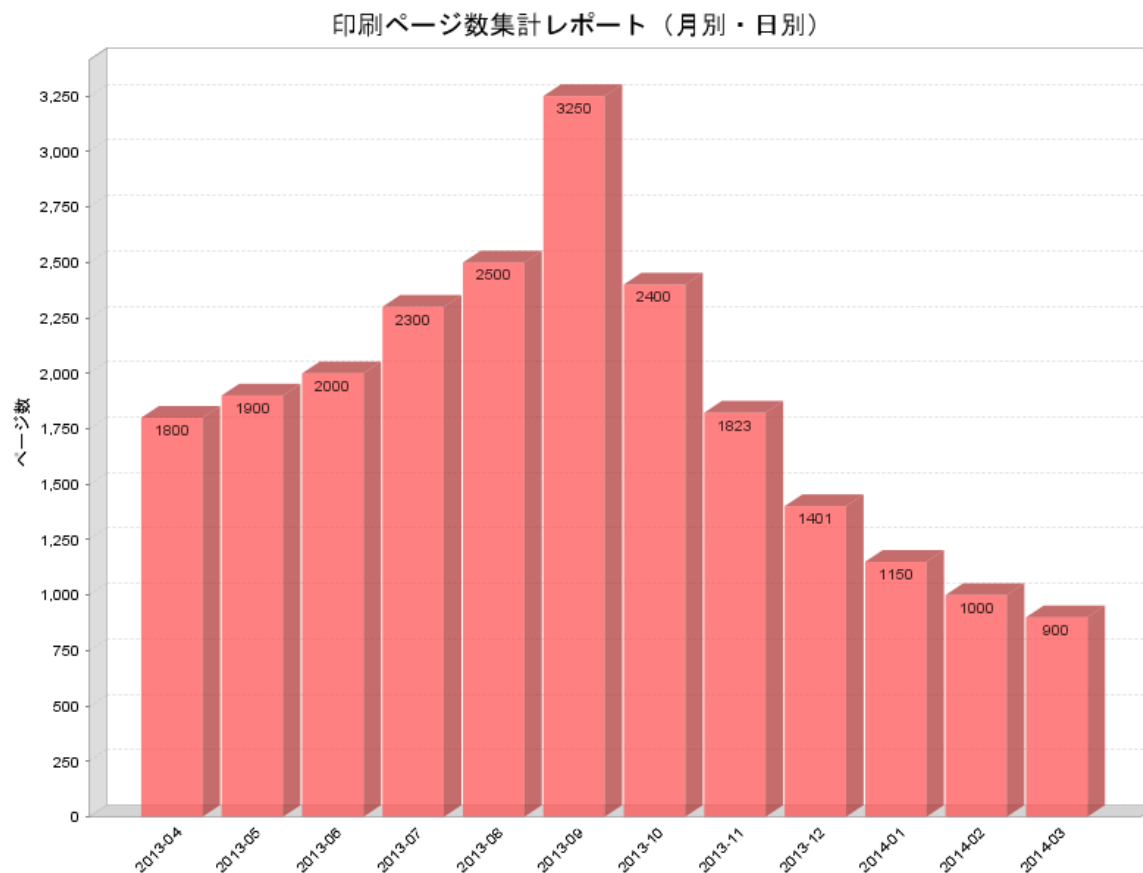
ユーザー指定/全体指定で、指定期間内におけるアプリケーション起動回数のTOP20を表示



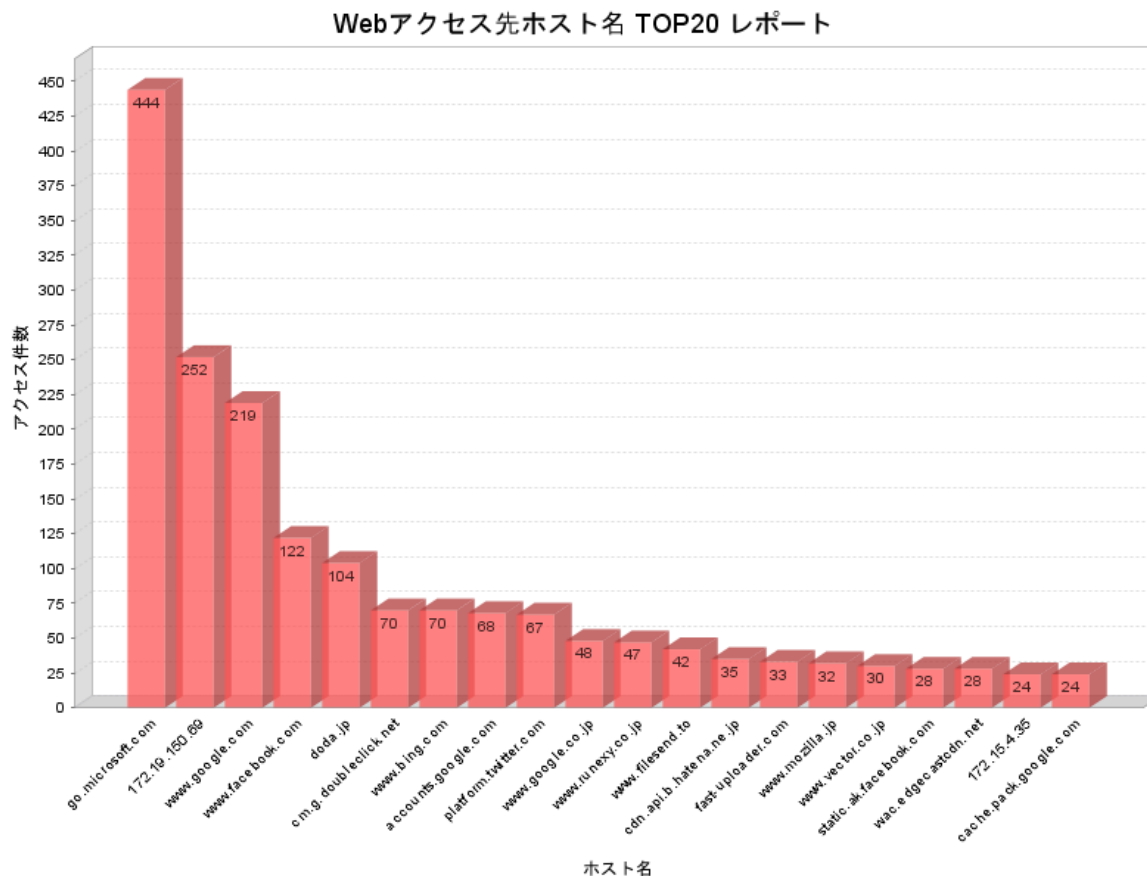
指定期間におけるユーザー毎/全体の印刷ページ数の集計をグラフ表示。
プリンターログの「ページ数」を集計表示。



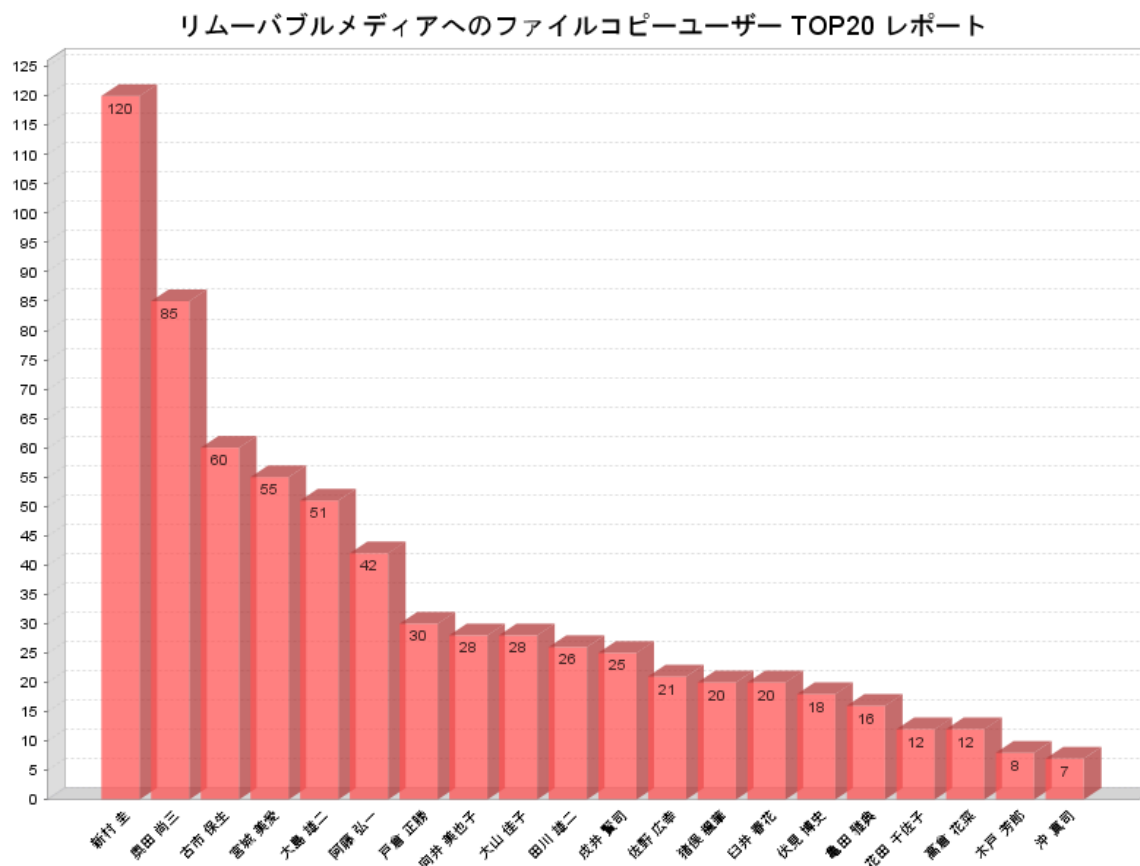
ユーザー指定/全体指定で、指定期間における月毎・日毎の印刷ページ数推移をグラフ表示。
プリンターログの「ページ数」を集計表示。



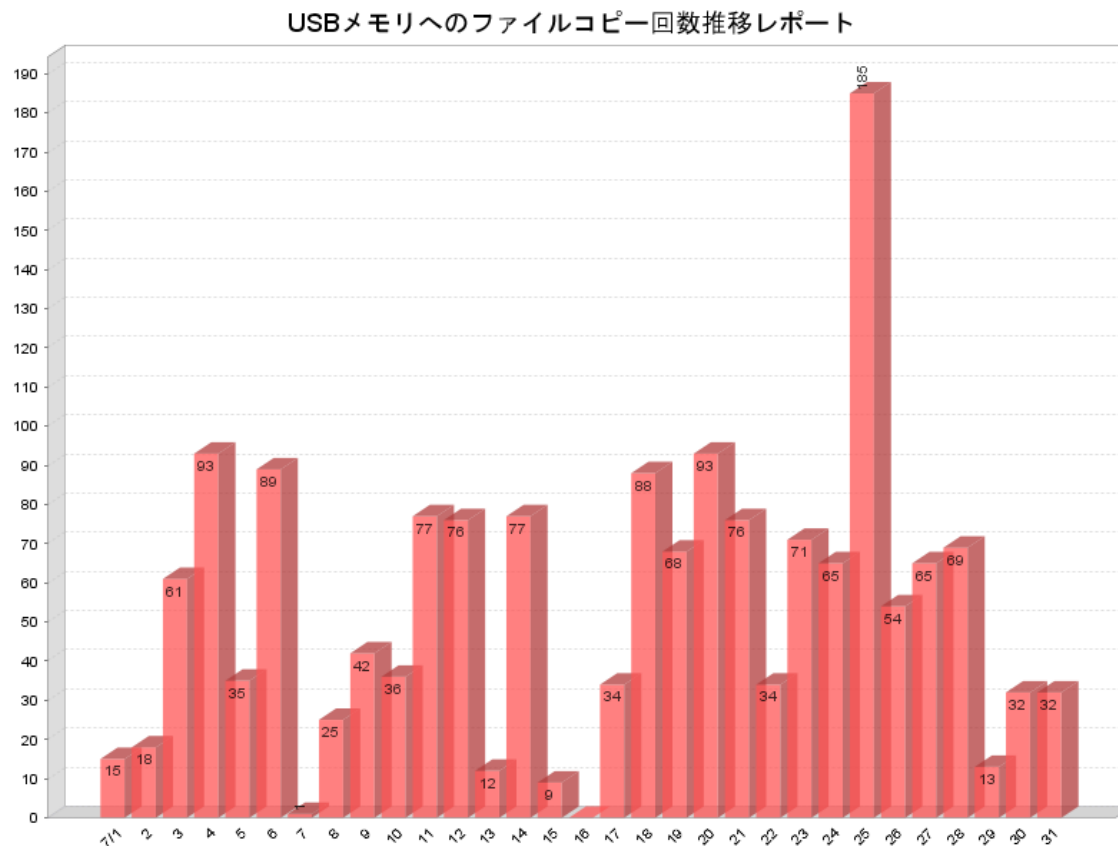
ユーザー指定/全体指定で、指定期間におけるWebアクセスの多いホスト名順にレポート表示。SSLでのアクセスも集計対象とすることが可能。Webログの「ホスト名」をキーにログ件数を集計。



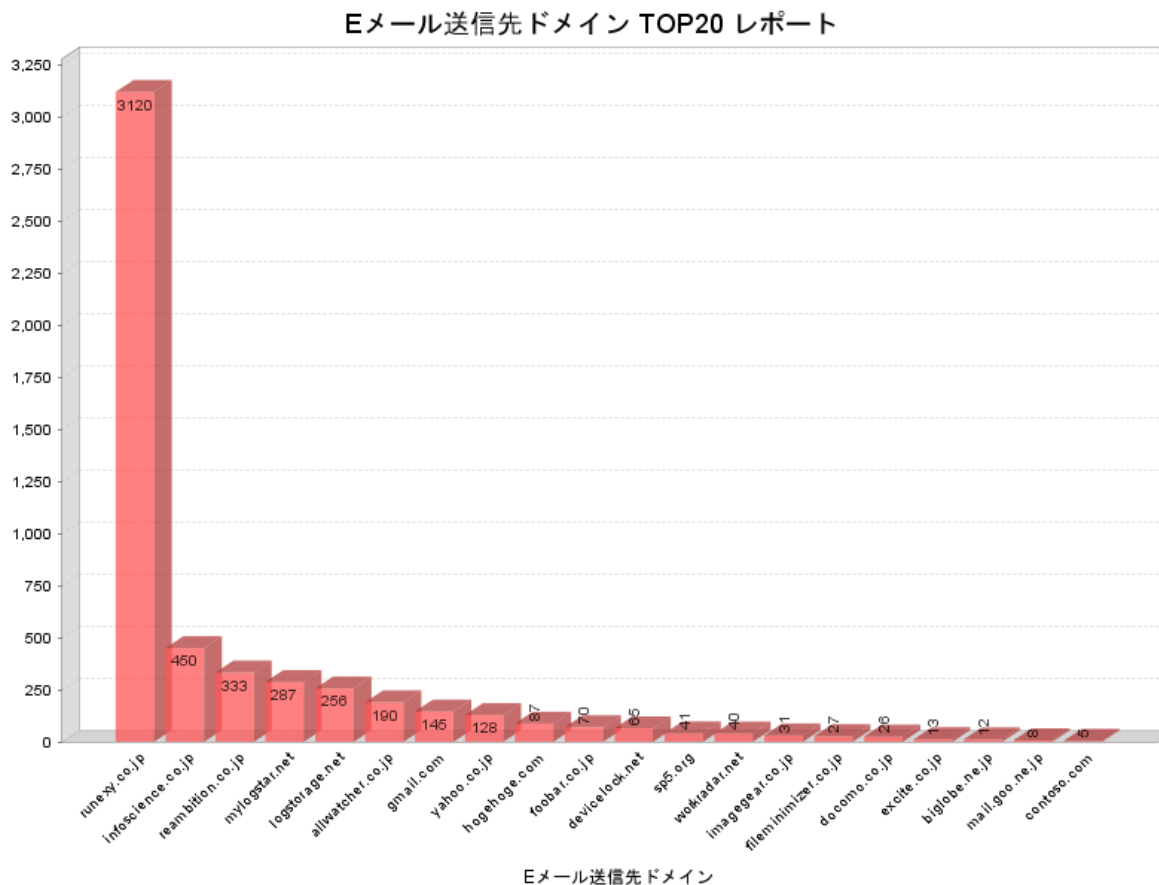
指定期間におけるリムーバブルメディアへのファイルコピーの多いユーザー順にレポート表示。ファイルログの「操作」が「COPY」、「操作後パス」が「REMOVABLE」をキーにログ件数を集計。



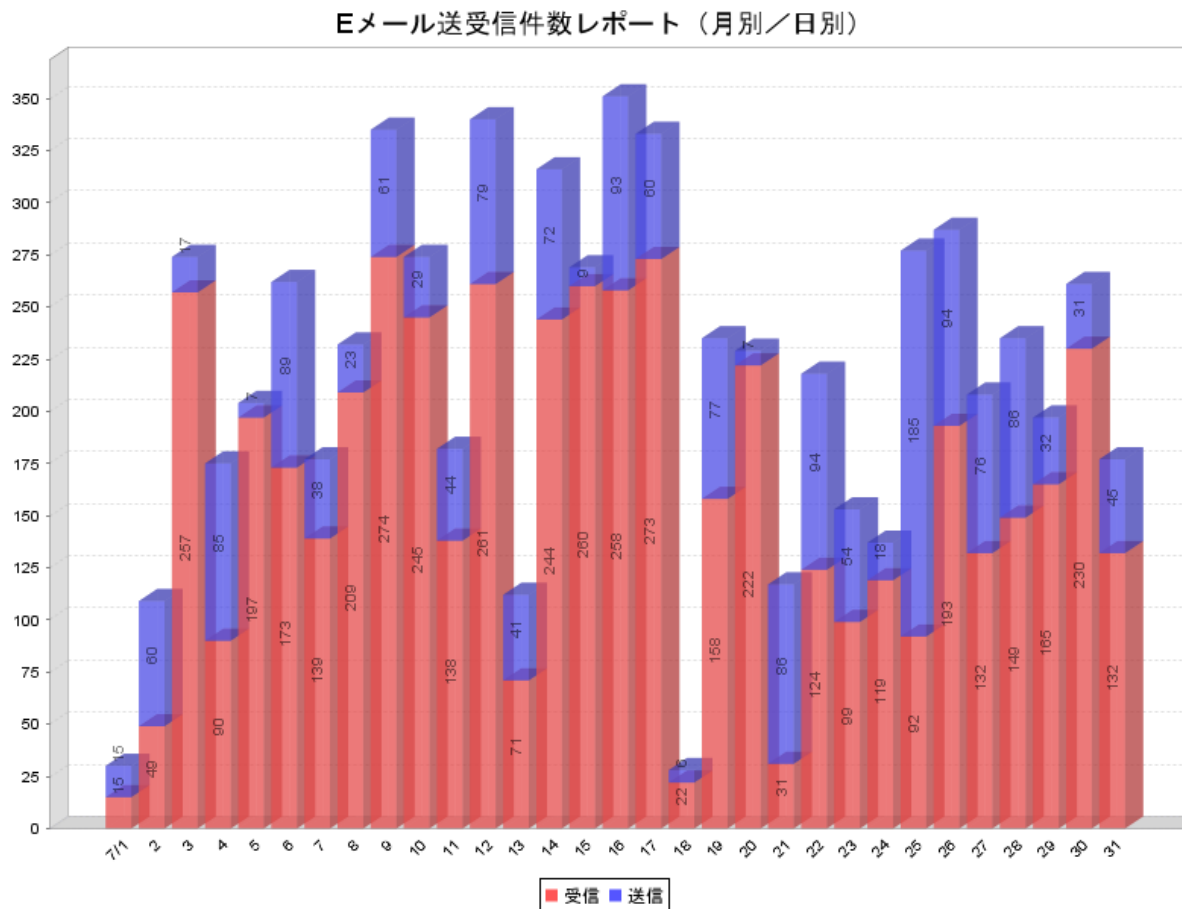
指定期間におけるリムーバブルメディアへのファイルコピーログ数を月別/日別に表示。
ファイルログの「操作」が「COPY」、「操作後パス」が「REMOVABLE」をキーにログ件数を集計。



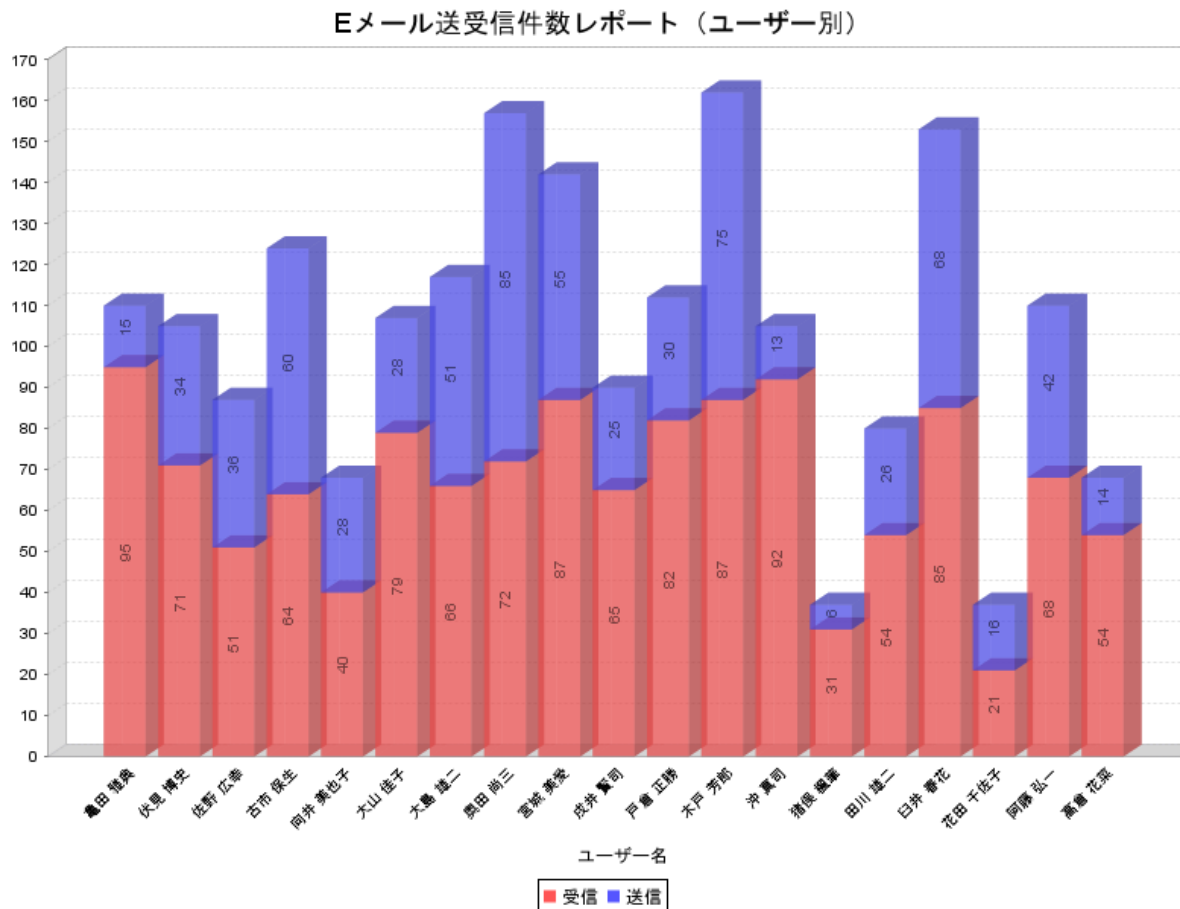
ユーザー指定/全体指定で、指定期間におけるEメール送信先ドメインのTOP20を表示。
Eメールログの「TO」を集計表示。



ユーザー指定/全体指定で、指定期間におけるEメール送信/受信の件数を、月別/日別に表示。
Eメールログの「送信/受信」をキーに集計して表示。



ユーザー指定/全体指定で、指定期間におけるEメール送信/受信の件数をユーザー別に表示。
Eメールログの「送信/受信」をキーに集計して表示。



開発元

インフォサイエンス株式会社

〒108-0023 東京都港区芝浦2-4-1インフォサイエンスビル

<https://www.infoscience.co.jp/>

お問い合わせ先

インフォサイエンス株式会社 プロダクト事業部

TEL 03-5427-3503 FAX 03-5427-3889

<https://www.logstorage.com/>

mail : info@logstorage.com