統合ログ管理システム Logstorage InfoTrace 連携パック ご紹介資料

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

会社概要

Infoscience

会社名	インフォサイエンス株式会社
代表者	宮 紀雄
設立	1995年10月
従業員	100名
URL	https://www.infoscience.co.jp/
所在地	東京都港区芝浦2丁目4番1号 インフォサイエンスビル
	ソフトウェア Logstorage シリーズの開発・販売 製品URL：https://logstorage.com/

統合ログ管理ツール
Logstorage

ログの収集・保管、高度な分析、高速な検索を行う
統合ログ管理ソフトです

DXプラットフォーム
Jimzen

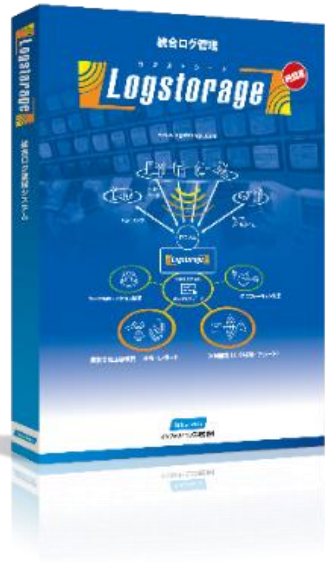
メンバーシップマネジメントを中心とするクラウド
サービスです

データセンター運用
DATA CENTER

独自の障害管理システムでサーバおよびネットワーク
機器の稼働状況を常に監視します

Logstorageシリーズ 製品概要

出荷本数シェアNo.1



Logstorage

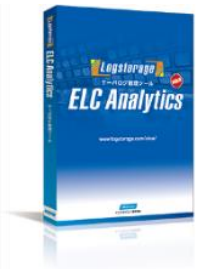
ログの収集・保管、高度な分析、高速な検索を行う、統合ログ管理ソフトです

★★★★★★★★★★★★★★★★

統合ログ管理ツール分野シェア

16年連続No.1

出典：デロイト トーマツ ミック経済研究所2023年1月発刊内部脅威対策ソリューション市場の現状と将来展望 2022年度（統合ログ管理ツール部門）
出荷本数でシェア51.3%を獲得　https://mic-r.co.jp/mr/02620/



ELC Analytics

サーバのアクセスログや
ステータスログを管理します

Logstorage-X/SIEM

セキュリティ脅威を
リアルタイムで検知します

アライアンス・連携製品

各種管理ツールとの連携パッケージ

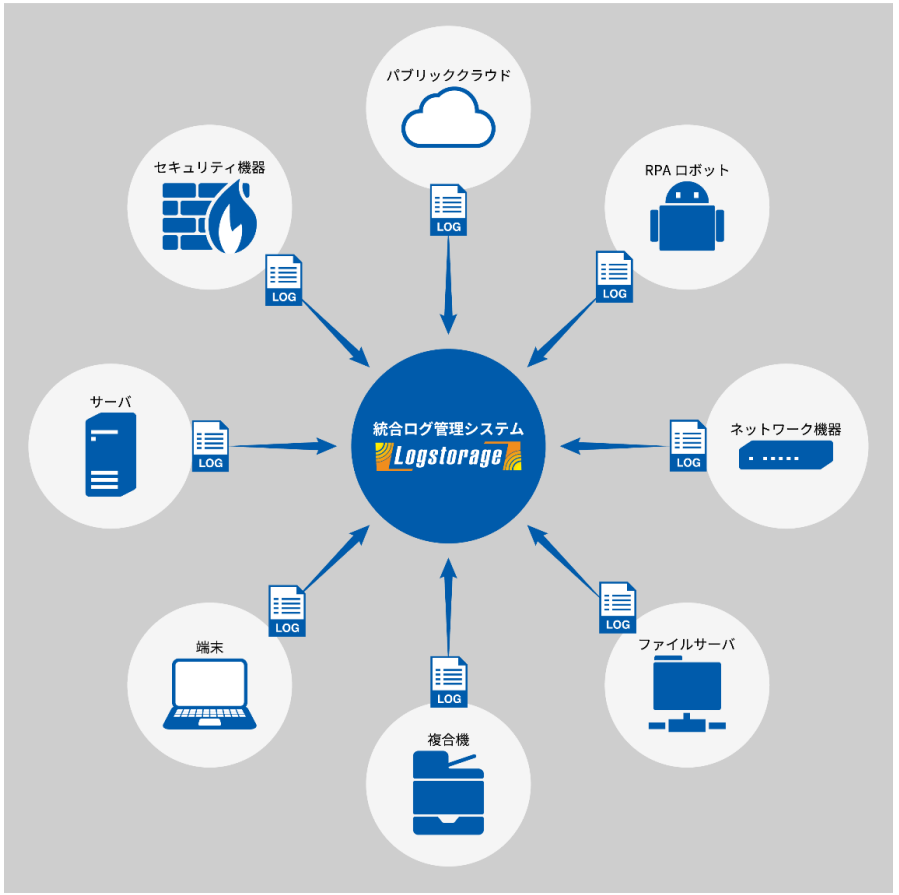
aws　Azure　Google Cloud　box　Microsoft 365　Google Workspace
cybereason　paloalto　iDoperation　SKYSEA Client View　CWAT
MylogStar　Access Check　SSDB監査　i-FILTER　InfoTrace　PISO
LANSCOPE　DEFESA Logger　MaLion

統合ログ管理システム
「Logstorage」

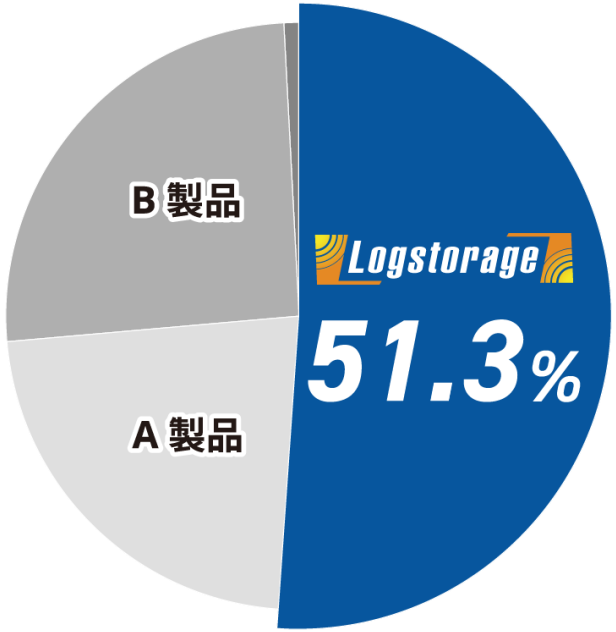
統合ログ管理システム「Logstorage」

「Logstorage」とは

様々なシステムに異なるフォーマットで散在するログを管理・分析する純国産の統合ログ管理システムです。
内部統制、情報漏えい対策、サイバー攻撃対策、システム運用監視、業務効率改善など多様な目的に対応できる、統合ログ分野でのデファクトスタンダード製品です。



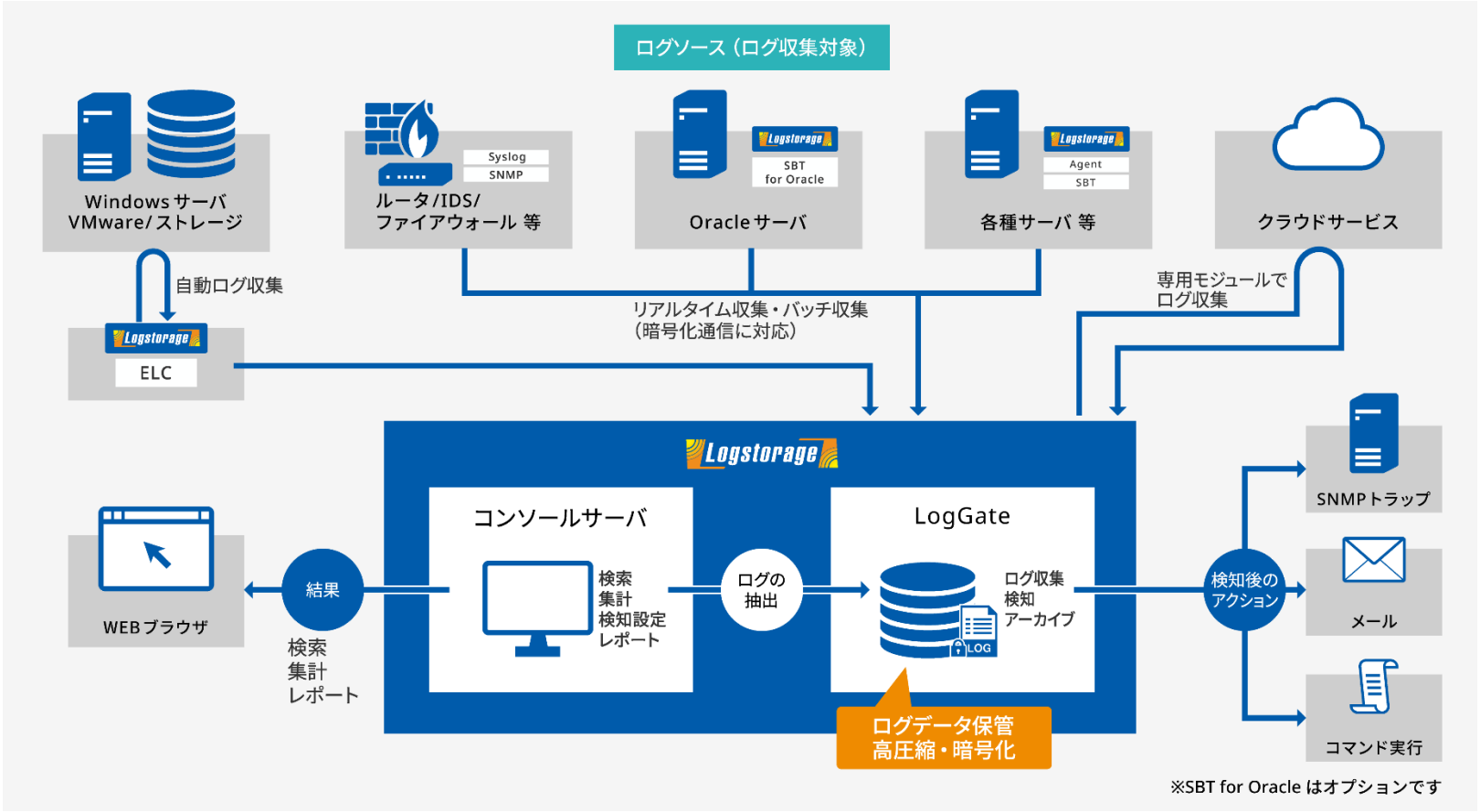
16年連続市場シェアNo.1
4,800社への導入実績



出荷本数シェア

※出典：デロイト トーマツ ミック経済研究所2023年1月発刊 内部脅威対策ソリューション市場の現状と将来展望 2022年度（統合ログ管理ツール部門）出荷本数でシェア51.3%を獲得 https://mic-r.co.jp/mr/02620/

統合ログ管理システム「Logstorage」



<Logstorage システム構成>

ログ収集機能

[受信機能]
- Syslog / FTP(S) / 共有フォルダ / SNMP

[ログ送信・取得機能]
- Agent
- ELC (EventLogCollector)
- SBT (SecureBatchTransfer)

ログ保管機能

- ログの圧縮保存 / 高速検索
- ログの改ざんチェック機能
- ログに対する意味（タグ）付け
- ログの暗号化保存
- 保存期間を経過したログを自動アーカイブ
- ログの保存領域管理機能

ログ検知機能

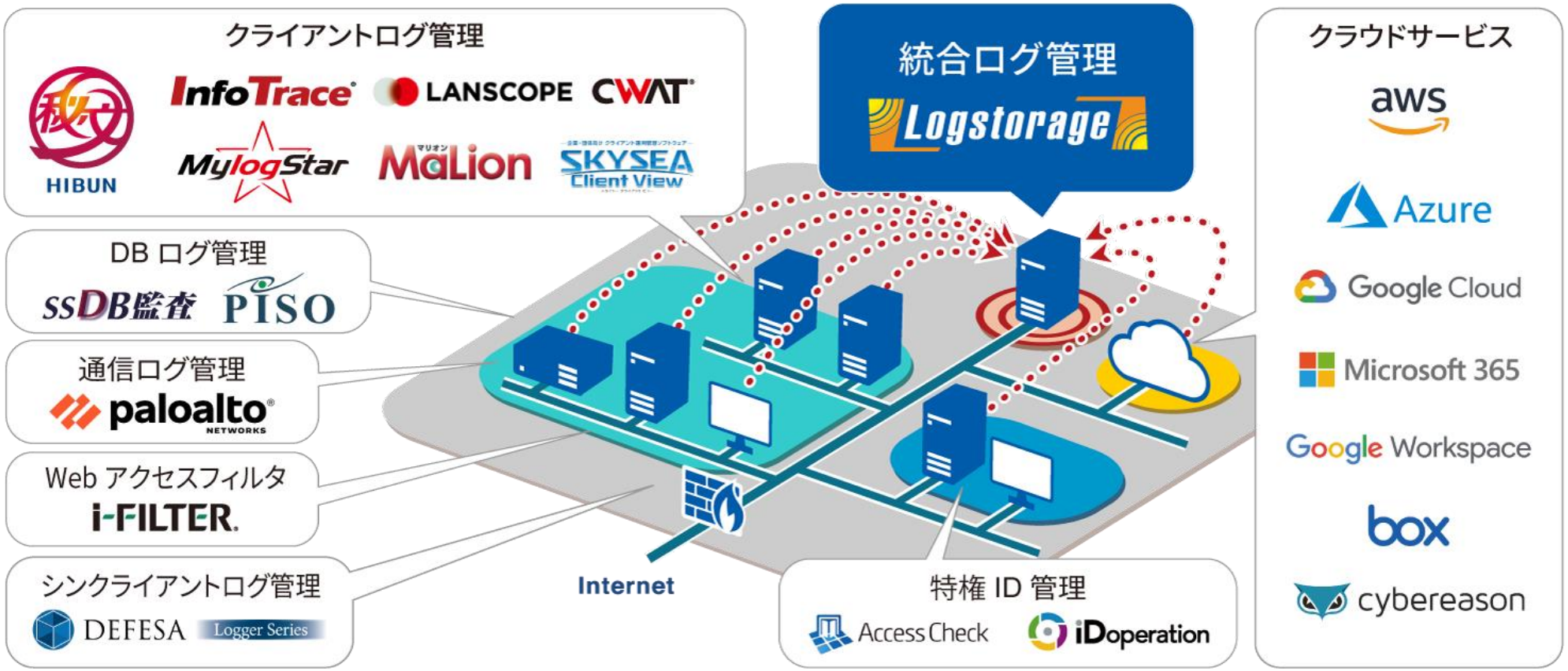
- ポリシーに合致したログのアラート
- ポリシーはストーリー的に定義可能 (シナリオ検知)

検索・集計・レポート機能

- 複数ログの横断追跡とマウス操作による高度な絞込み
- インデックスによる大量ログの高速検索
- グラフ(円/折れ線/棒/表)によるログのサマリ表示
- レポート(HTML/PDF/CSV/TXT/XML)の自動メール通知

Logstorage 連携製品

各分野でトップシェアの製品と連携！



Logstorage 連携製品

日本国内で利用されているソフトウェア・機器を中心に400種以上のログ収集実績

OS システム・イベント
Windows
Linux
Unix
Solaris
HP-UX
BSD
NetApp
EMC
VMware vCenter
VMware ESXi

Web ／プロキシ
Apache
IIS
BlueCoat
squid
WebSense
WebSphere
WebLogic
Apache Tomcat
Cosminexus
Trend Micro Cloud App Security
InterScan Web Security as a Service
Zscaler

サーバアクセス
ALog コンバータ
File Server Audit
CA Access Control
VISUACT

ICカード認証
SmartOn
ARCACLAVIS Revo

運用監視
Nagios
JP1
Systemwalker
OpenView
WebSAM

複合機
imageRunner
Apeos
SecurePrint!

ネットワーク機器
FortiGate
SonicWall
BIG-IP
Cisco PIX/ASA
Cisco Catalyst
NetScreen/SSG
VPN-1
Firewall-1
Check Point IP
SSL-VPN
NOKIA IP
Alteon
IronPort
ServerIron
Proventia
CACHATTO

データベース
Oracle
SQLServer
DB2
PostgreSQL
MySQL
Chakra
SecureSphere DMG/DSG
AUDIT MASTER
IPLocks
Guardium

クライアント操作
SeP
QND/QOH

メール
MS Exchange
sendmail
Postfix
qmail
Exim
GUARDIANWALL

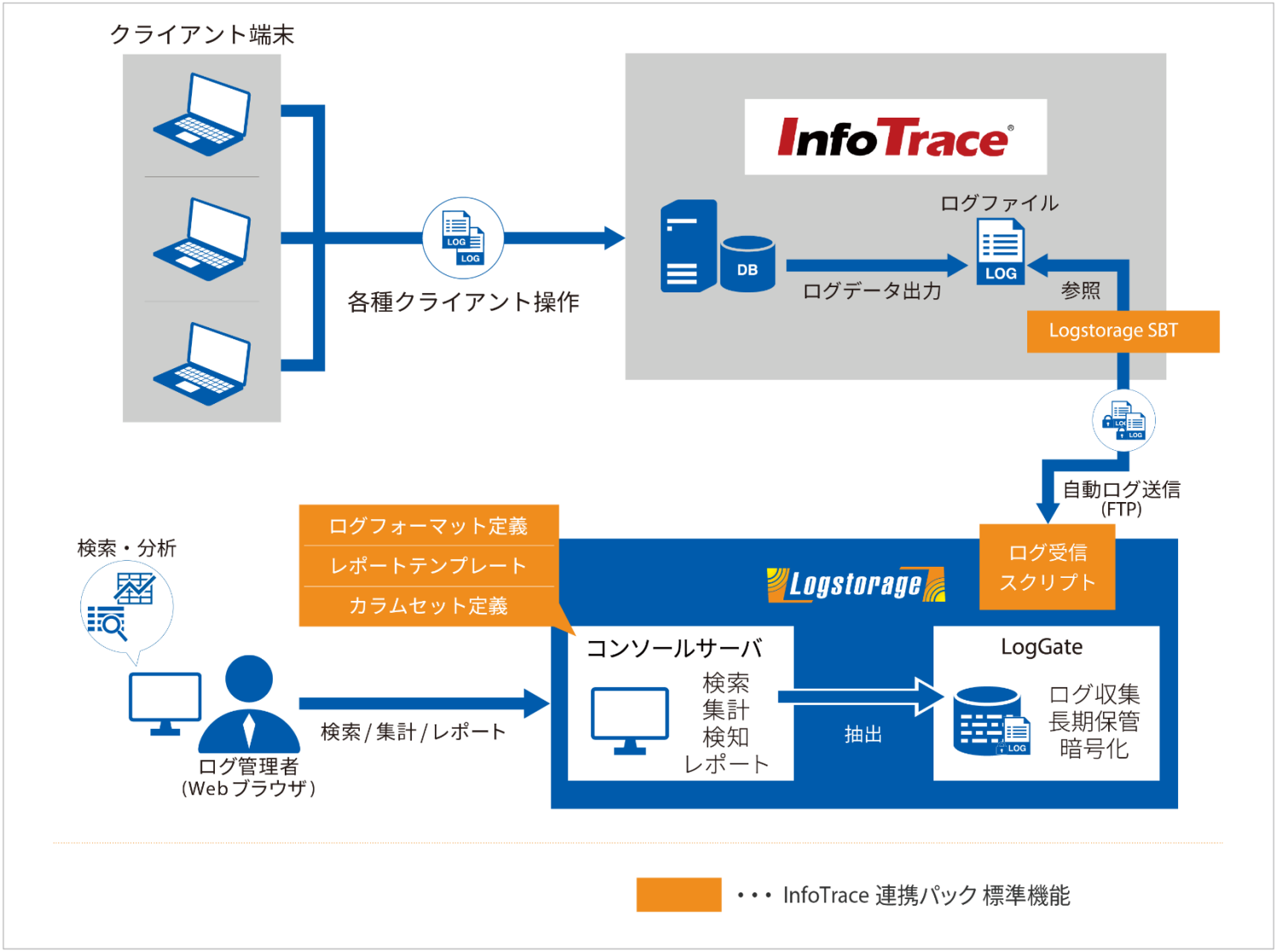
アンチウィルス
Symantec AntiVirus
TrendMicro InterScan
McAfee VirusScan
HDE Anti Vuris
ESET
ウイルスバスター

その他
Lotus Domino
Notes AccessAnalyzer2
Auge AccessWatcher
SAP R/3 (ERP)
ex-SG (入退室管理)
MSIESER
iSecurity
Desk Net's
HP NonStop Server
System Answer

※順不同

Logstorage InfoTrace 連携パック

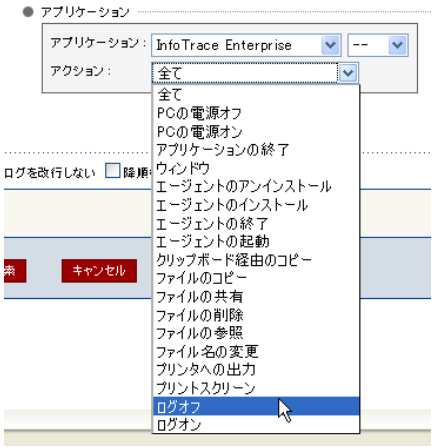
Logstorage for InfoTrace システム構成



Logstorage InfoTrace 連携パック 内容

Logstorage InfoTrace 連携パック 内容	
SBT	InfoTrace より出力されたログを、Logstorage に自動送信するプログラム
ログ変換スクリプト	InfoTrace 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	InfoTrace 用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	InfoTrace 用の検索結果画面を標準設定
レポートテンプレート	InfoTrace 用のレポートテンプレートを標準設定

カラムセット定義
（検索結果画面）



ログフォーマット定義定義
（検索条件画面例）

製品連携のメリット

他のシステム・機器のログを統合

Logstorage はインフォサイエンスの特許取得技術により、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InfoTrace と、同じくソリトンシステムズのSmartOn や、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、個人認証から、フロアへの出入り、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。

柔軟なレポーティング

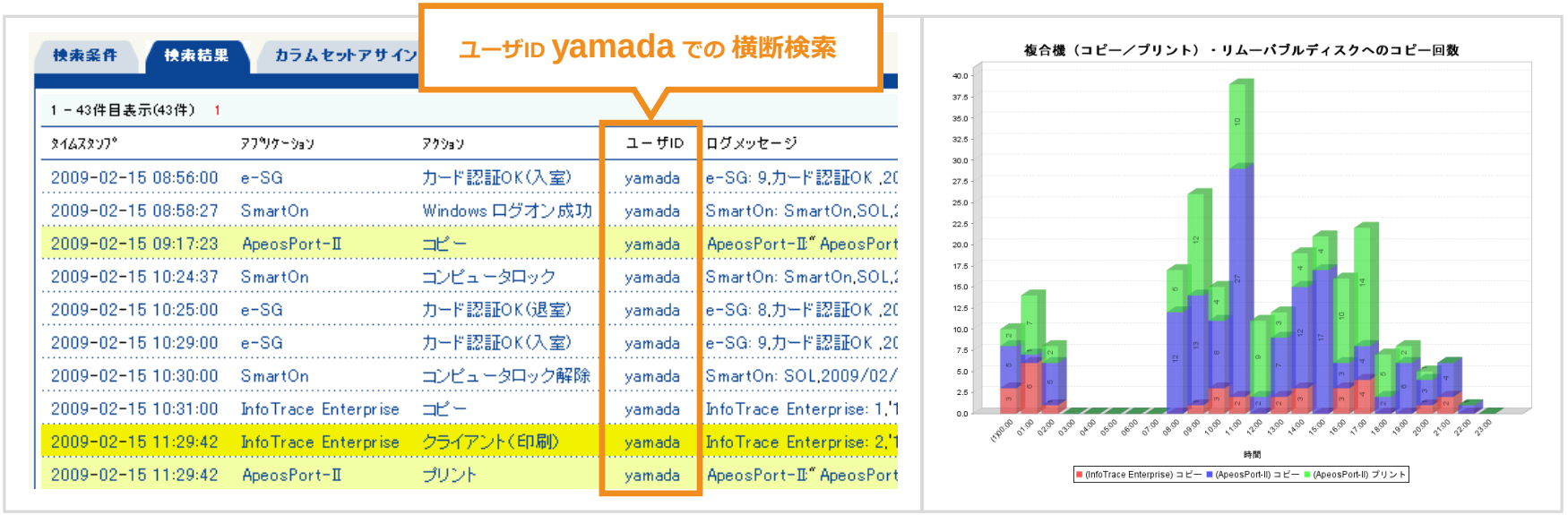
「Logstorage InfoTrace 連携パック」は、「InfoTrace」が記録したログに対するレポートテンプレートを用意しているほか、
レポート内容をGUI上で自由に設定・カスタマイズする機能があります。
レポートテンプレートをベースに、自社のセキュリティポリシーに合った、様々な角度からのレポート出力が可能になりますの
で、セキュリティ・インシデントの予見、防止につながります。

ログの原本証明

InfoTrace で記録し、Logstorage で保管するログに対して電子署名を生成する機能により、
ログの改ざん検出・原本証明が可能。

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る。例えば、InfoTraceで記録したログと、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し、横断的な検索・分析が可能。

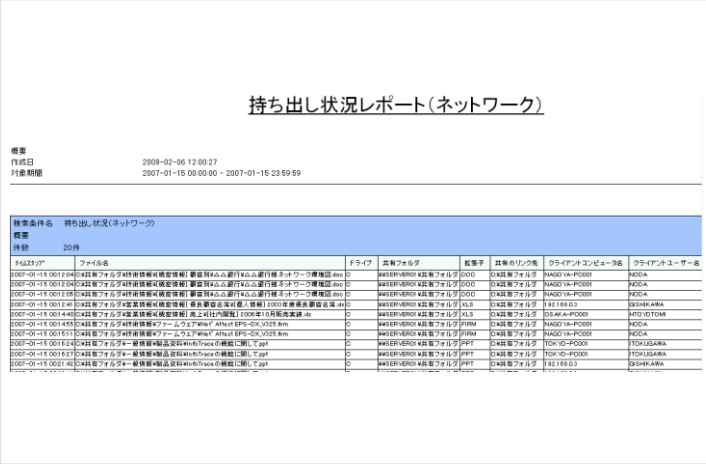


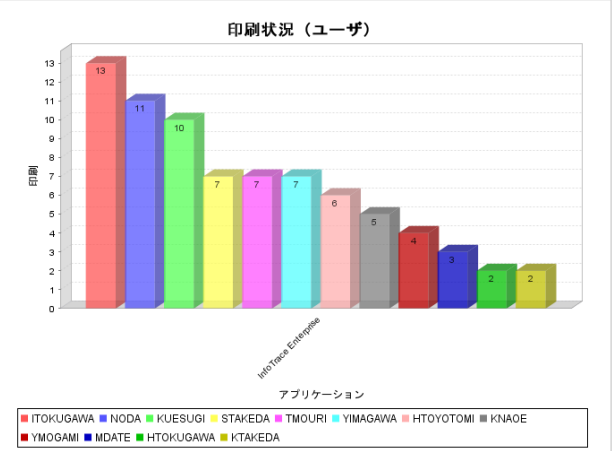
検索結果画面例

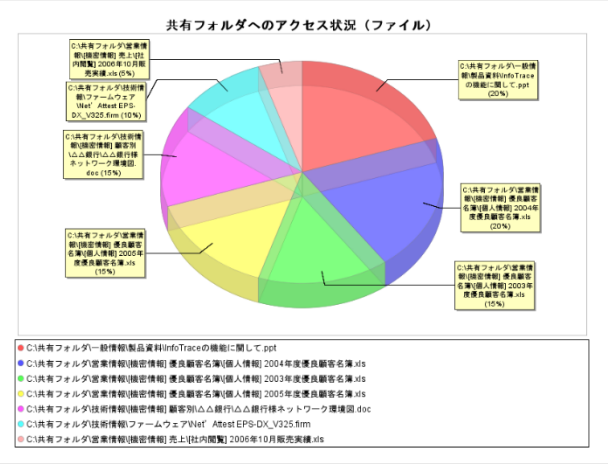
集計結果画面例

多彩なレポート機能

- レポートの定期・自動出力（日次/週次/月次/1時間毎）
- 随時更新される豊富なレポートテンプレート
- 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
- 直感的なGUI画面より、自由にテンプレート作成可能

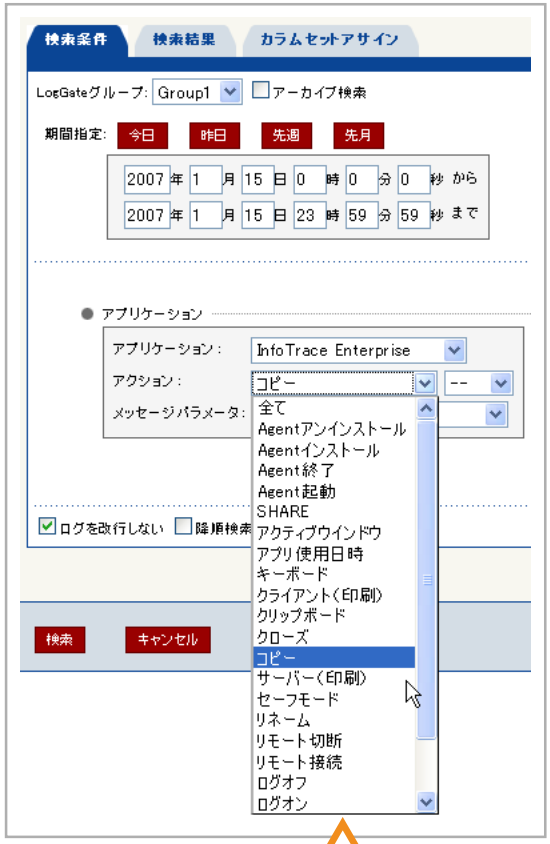






ログの検索～絞込み

検索条件



InfoTraceのログが持つ
全てのイベント/項目での検索が可能

検索結果

絞込結果

クリックしたユーザ名で絞り込まれた

社員の行動追跡

検索条件

異なるフォーマットのログも、
様々な検索キーで横断検索が可能

検索結果

検索条件 | 検索結果 | カラムセットアサイン

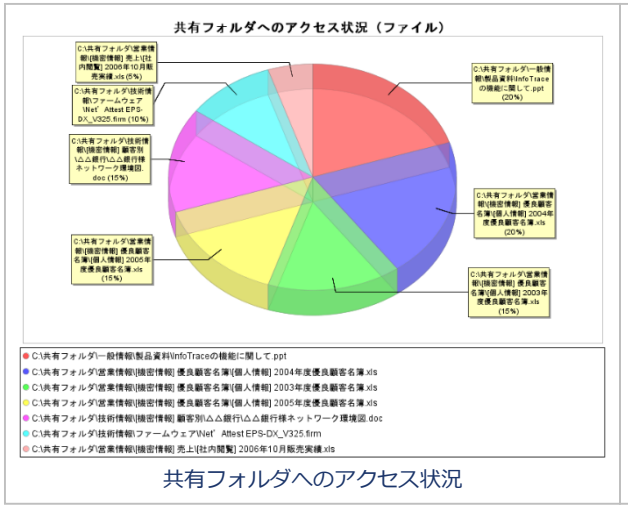
1 - 43件目表示(43件) 1

ﾀｲﾑｽﾀﾝﾌﾟ	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	ユーザID	ログメッセージ
2009-02-15 08:56:00	e-SG	カード認証OK(入室)	yamada	e-SG: 9,カード認証OK ,20
2009-02-15 08:58:27	SmartOn	Windows ログオン成功	yamada	SmartOn: SmartOn,SOL,2
2009-02-15 09:17:23	ApeosPort-Ⅱ	コピー	yamada	ApeosPort-Ⅱ" ApeosPort
2009-02-15 10:24:37	SmartOn	コンピュータロック	yamada	SmartOn: SmartOn,SOL,2
2009-02-15 10:25:00	e-SG	カード認証OK(退室)	yamada	e-SG: 8,カード認証OK ,20
2009-02-15 10:29:00	e-SG	カード認証OK(入室)	yamada	e-SG: 9,カード認証OK ,20
2009-02-15 10:30:00	SmartOn	コンピュータロック解除	yamada	SmartOn: SOL,2009/02/
2009-02-15 10:31:00	InfoTrace Enterprise	コピー	yamada	InfoTrace Enterprise: 1,'1
2009-02-15 11:29:42	InfoTrace Enterprise	クライアント(印刷)	yamada	InfoTrace Enterprise: 2,'1
2009-02-15 11:29:42	ApeosPort-Ⅱ	プリント	yamada	ApeosPort-Ⅱ" ApeosPort
2009-02-15 12:02:09	SmartOn	コンピュータロック	yamada	SmartOn: SmartOn,SOL,2
2009-02-15 12:03:00	e-SG	カード認証OK(退室)	yamada	e-SG: 8,カード認証OK ,20
2009-02-15 12:49:00	e-SG	カード認証OK(入室)	yamada	e-SG: 8,カード認証OK ,20
2009-02-15 12:57:00	SmartOn	コンピュータロック解除	yamada	SmartOn: SOL,2009/02/
2009-02-15 13:04:10	CRM	ログイン	yamada	CRM: yamada,山田太郎,ロ
2009-02-15 13:04:11	PISO	SQL監視情報	yamada	PISO(SQL): ""Server132
2009-02-15 13:04:13	CRM	顧客リスト選択	yamada	CRM: yamada,顧客リストを
2009-02-15 13:04:14	PISO	SQL監視情報	yamada	PISO(SQL): ""Server132
2009-02-15 13:06:22	CRM	ログアウト	yamada	CRM: yamada,ログアウトし
2009-02-15 15:18:57	SmartOn	コンピュータロック	yamada	SmartOn: SmartOn,SOL,2
2009-02-15 15:19:00	e-SG	カード認証OK(退室)	yamada	e-SG: 8,カード認証OK ,20
2009-02-15 15:32:00	e-SG	カード認証OK(入室)	yamada	e-SG: 8,カード認証OK ,20

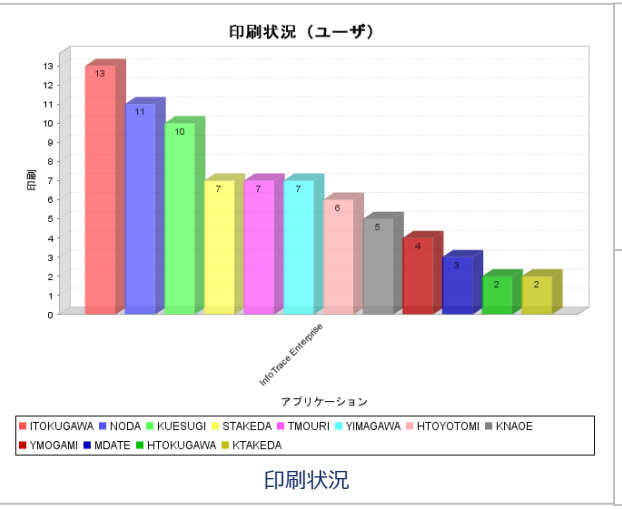
レポートテンプレート

レポートテンプレート一覧	
持ち出し状況（CD, DVD）	ファイルをCD/DVDにコピーした時刻、ユーザ、ファイル名等を一覧出力
持ち出し状況（リムーバブルディスク）	ファイルをリームバブルメディアにコピーした時刻、ユーザ、ファイル名等を一覧出力
持ち出し状況（ネットワーク）	ファイルをネットワーク越しにコピーした時刻、ユーザ、ファイル名等を一覧出力
印刷状況（印刷履歴）	ドキュメントを印刷した時刻、ユーザ、ファイル名等を一覧出力
印刷状況（ユーザ毎の印刷枚数）	ドキュメント印刷枚数をユーザ毎に集計、出力
共有フォルダへのアクセス状況（ファイル）	共有フォルダ上のファイルへのアクセス比率を出力
共有フォルダへのアクセス状況（ユーザ）	共有フォルダへのユーザのアクセス比率を出力
アプリケーション利用状況	アプリケーション毎の利用回数を集計、出力
InfoTrace Agent アンインストールユーザー一覧	InfoTrace Agent をアンインストールした時刻、ユーザ、端末などを一覧出力

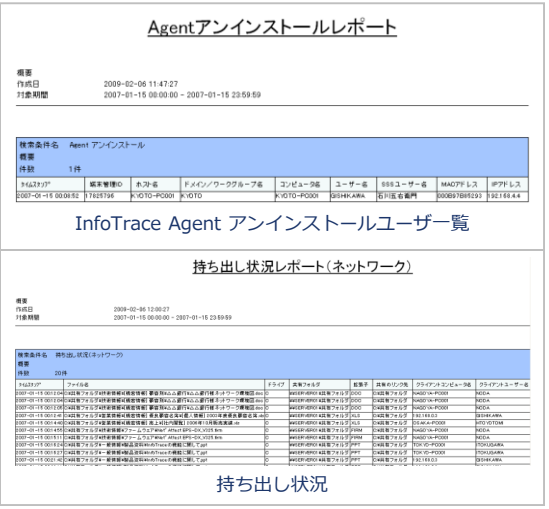
レポートイメージ　　上記以外のレポートも、直感的なＧＵＩインターフェースで自由に設定可能！



共有フォルダへのアクセス状況



印刷状況



持ち出し状況

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://logstorage.com/
mail : info@logstorage.com