統合ログ管理システム Logstorage
Ver.10 製品紹介資料

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

© Infoscience Corporation

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

出典：デロイト トーマツ ミック経済研究所2024年2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 2023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/03010/

出典：富士キメラ総研 2011-2023 ネットワークセキュリティ ビジネス調査総覧（市場編）
統合ログ管理ツール（SIM/SIEM）、市場占有率、SIM、金額ベース、2022年度実績
2010年度-2022年度連続シェアNO.1

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です

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

© Infoscience Corporation

統合ログ管理システムLogstorageの導入目的

01 脅威対策

脅威の検出（標的型攻撃／内部情報漏えい）
フォレンジック（攻撃を受けた際の証拠保全）

02 システム運用

システムの状態把握・障害時の調査、解析

03 コンプライアンス

各種法令、業界／団体ガイドラインへの
ログ管理要件への充足

© Infoscience Corporation

Logstorage 沿革

移り変わるセキュリティ事情で、常に求められ続ける統合ログ管理

2000　2005　2010　2015　2020

マルウェアの複雑化、不正アクセス、DDoS 攻撃の増加

社会的背景によるログ管理の需要増加
（個人情報保護法施行、日本版 SOX 法施行、PCIDSS、マイナンバー、各種ガイドライン）

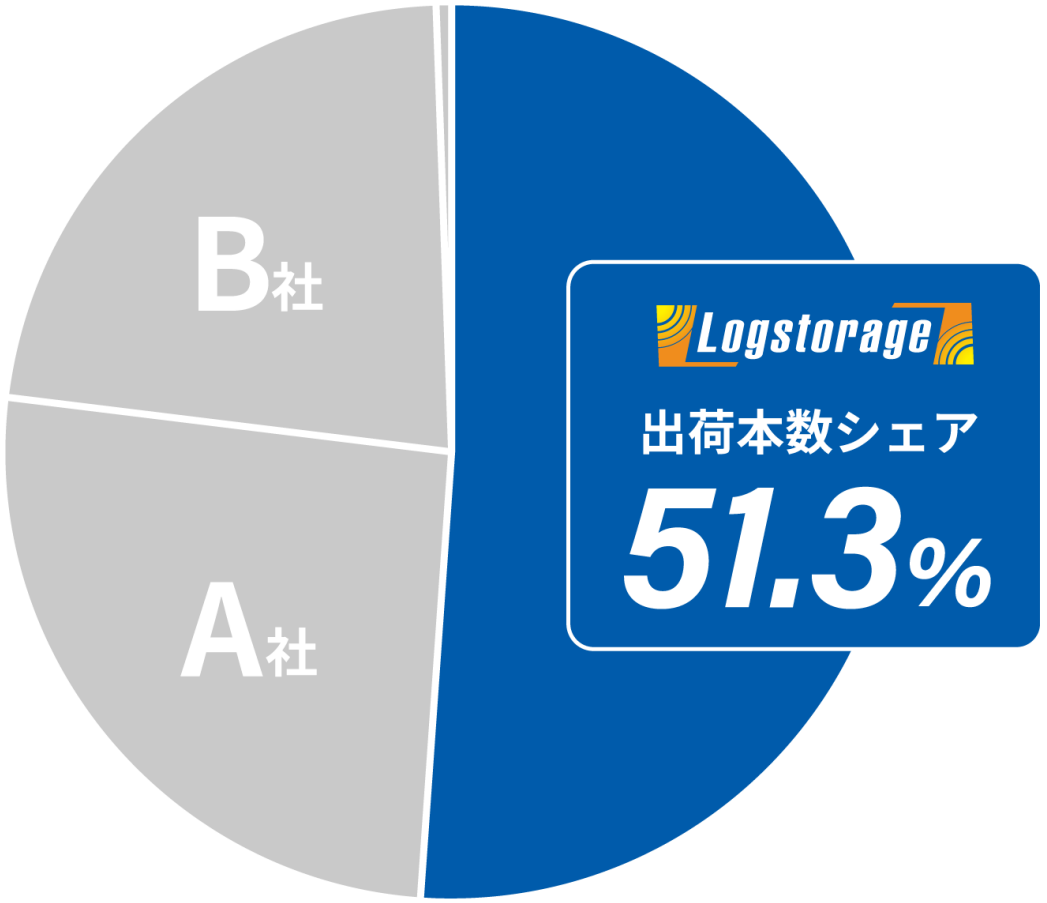
2023 年：Ver.10 リリース（Insight 強化）
2022 年：Ver.9 リリース（Insight 機能）
2020 年：Ver.8 リリース（マスタ連携機能）
2018 年：Ver.7 リリース（ログフォーマット定義自動化）
2017 年：Ver.6 リリース（インデックス検索）
2016 年：Ver.5 リリース（多様な分析／検索・分析の並列化）
2010 年：Ver.4 リリース（高圧縮・高速検索／ Windows イベントログ検索）
2006 年：Ver.3 リリース（検索・分析の高速化／レポート機能強化）
2003 年：Ver.2 リリース（大量データ対応）
2002 年：Ver.1 リリース

ゼロトラスト・ガイドライン対応
テレワーク・SaaS サービスの普及
クラウドサービスの普及
情報セキュリティ対策（標的型攻撃・システム内部統制）
IT システム運用管理

© Infoscience Corporation

Logstorage 導入社数 / シェア

統合ログ管理ツールの分野で 17年連続シェアNo.1



出荷本数シェア

国内導入企業
5,100社 以上

※出典：デロイト トーマツ ミック経済研究所2024年2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 2023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/03010/

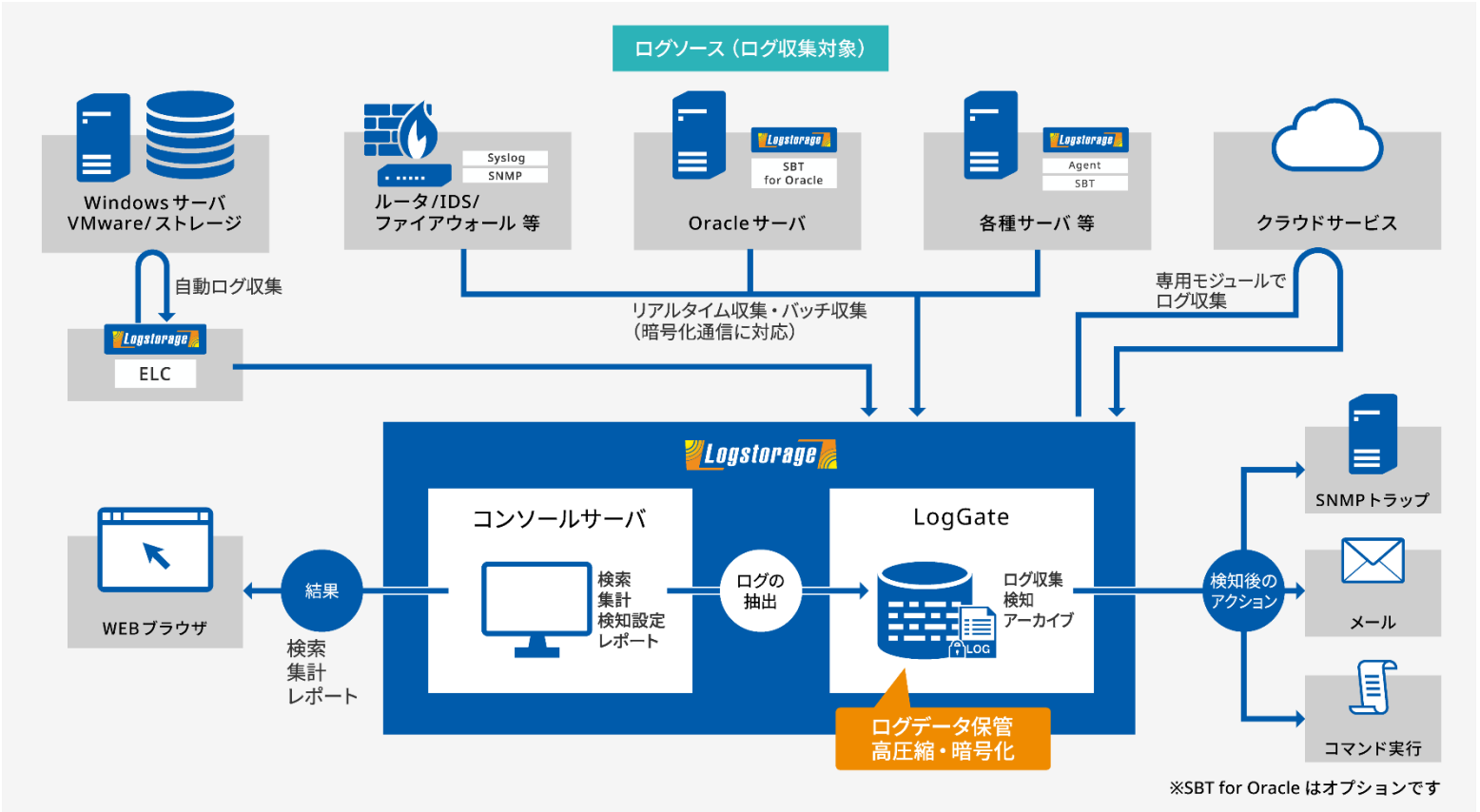
© Infoscience Corporation

Logstorage 機能・特徴

- Logstorage システム構成
- Logstorage ログ収集機能
- Logstorage ログ分析・管理機能

© Infoscience Corporation

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

© Infoscience Corporation

Logstorage 機能・特徴

- Logstorage システム構成
- Logstorage ログ収集機能
- Logstorage ログ分析・管理機能

© Infoscience Corporation

Logstorage 連携製品

各分野でトップシェアの製品と連携！

データベース監査
ORACLE
SSDB監査
PISO

特権管理
Access Check
iDoperation

ファイアウォール
paloalto NETWORKS

EDR
cybereason

Web フィルタリング
i-FILTER.

クラウドサービス
aws
Azure
Google Cloud
Microsoft 365
Google Workspace
box

クライアントログ
DEFESA Logger
MylogStar

PC 資産管理
CWAT
On-premises LANSCOPE Endpoint Manager
マリオン MaLion
SKYSEA Client View
HIBUN

※Logstorageはインフォサイエンス株式会社の登録商標です。その他文中の社名、商品名は、各社の商標または登録商標です。

Logstorage 収集実績

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/Tomcat
IIS
Blue Coat
Squid
InfoCage PC検疫
Websense
WebSphere
WebLogic
Cosminexus
Trend Micro Cloud App Security
InterScan Web Security as a Service
Zscaler

サーバアクセス
ALog ConVerter
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
SQL Server
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-Virus
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
desknet's
HP NonStop サーバー
System Answer

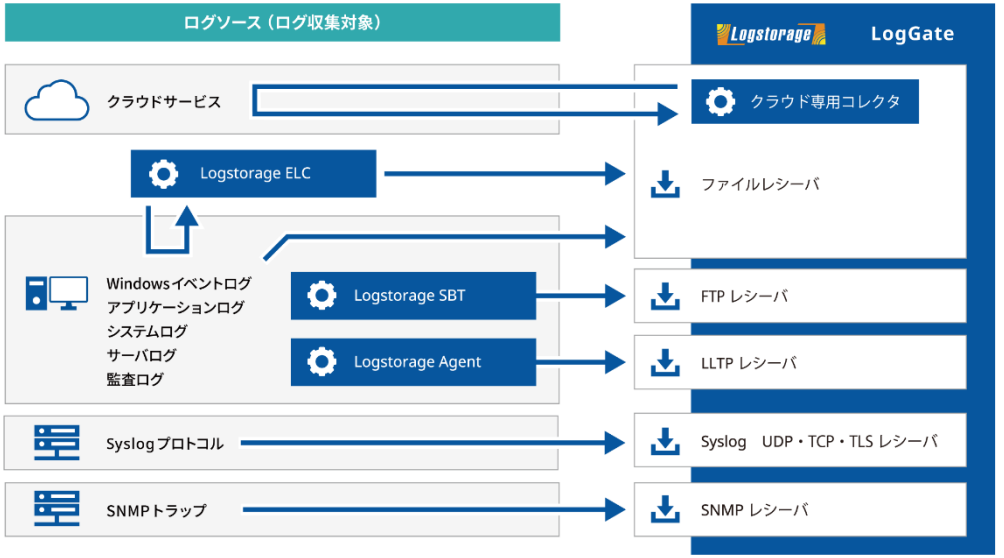
※順不同

© Infoscience Corporation

Logstorage で収集できるログ

テキスト形式で出力されるログは全て収集・管理可能！

- 独自アプリケーションのログも収集可能
- ログの性質に合わせてリアルタイム / バッチによる収集が可能
- エージェントレスでの収集も可能
- 複数のレシーバを組合わせた収集が可能



< Logstorage ログ収集イメージ >

収集方式・機能名	収集間隔	収集方法
syslog レシーバ	即時	ログをsyslogプロトコルにて受信する
SNMP Trap	即時	SNMP Trap をログとして受信する
FTPレシーバ	定時	ログファイルをFTP / FTPSにて受信する
Fileレシーバ	定時	監視対象ディレクトリに置かれたログファイルを受信する
Logstorage標準 ログ収集ソフトウェア	**収集間隔**	**収集方法**
Logstorage Agent	即時	テキストログ、イベントログを監視し、LogGateに送信する
Logstorage ELC	定時	エージェントレスでWindows / NetApp / EMCイベントログ、VMwareイベントを収集する
Logstorage SBT	定時	イベントログ、テキストログを圧縮、暗号化してLogGateに送信する

© Infoscience Corporation

テキストログ・イベントログをリアルタイムに暗号化送信

テキストログ、イベントログを監視し、LogGateに送信するクライアントツールです。

・ログをリアルタイムに送信可能

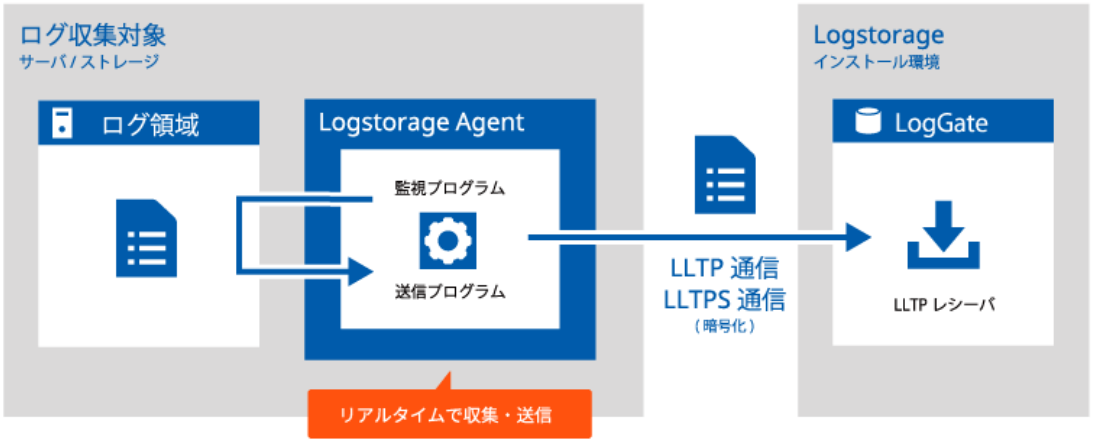
テキスト形式のログファイルやWindowsイベントログを
リアルタイムにLogGateへ転送することができます。

・独自プロトコルによるログ落ち防止

ログ転送に最適化された独自転送プロトコルである
「LLTP」を利用することで、ログ落ち（ロスト）を
完全に防止することができます。

・シンプル機能・低負荷

出力されているログを転送する、機能に特化したシンプルな
プログラムなので導入先のサーバのCPUやメモリリソースの
消費を最小限にしてログ転送を行います。



< Logstorage Agentによるログ収集イメージ >

機能	説明
ログの暗号化送信機能	暗号化してログを送信することができます。
ログ送信切り換え機能	送信先へ接続できない場合、接続先を切り換えて送信することができます。
システム高負荷時の動作抑制機能	ログ・ソース（ログ収集対象）が高負荷となったとき、メインのサービスの稼動に影響しないよう、ログ送信を一時抑制します。
ブロックログの送信機能	複数行で1つの意味を持つログを解析し、1行のログとして送信することができます。
ローテートログの送信機能	ローテートされたログファイルを追跡し、ログを送信することができます。
送信ログのフィルタ機能	キーワードによるログのフィルタリングを行い、必要なログのみ送信することができます。

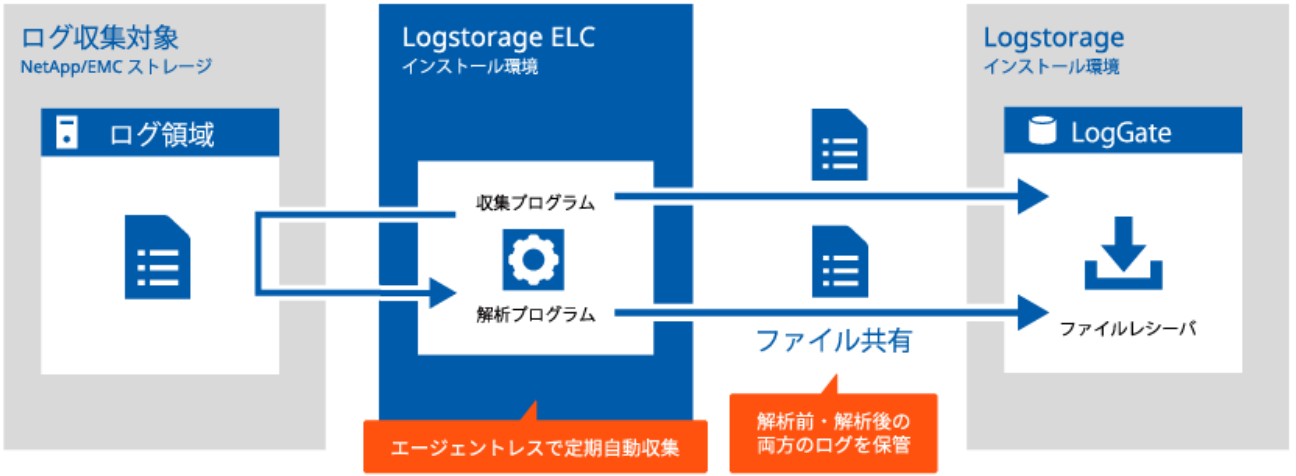
© Infoscience Corporation

Logstorage ELC (Event Log Collector) / ログ収集機能

イベントログをエージェントレスで取得

ST版以上

エージェントレスでWindows / NetApp / EMCイベントログ、VMwareイベント、Unixコマンドを収集するサーバツールです。



【収集対象 対応バージョン】

OS / 製品	対応バージョン
Windowsイベント（Win32Api） Windowsイベント	クライアント： Windows 10（32bit版/64bit版）, Windows 11
	サーバ： Windows Server 2016/2019/2022, Storage Server 2016
NetAppイベント（クラスタモード）	Data ONTAP .5/9.6/9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1、ONTAP Select 9.6/9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1 Cloud Volumes ONTAP(AWS, Azure, GCP) 9.6/9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1
EMCイベント	Unity 5.0.6/5.0.7/5.1.0/5.1.3/5.2.0/5.2.1/5.3.0
VMware	vCenter Server Ver.7.0/8.0 , ESXi Ver.7.0/8.0
Unixコマンド	Oracle Solaris 10/11 (SPARC/x86) , Red Hat Enterprise Linux 6(64bit版) /7/8/9, Amazon Linux 2, IBM AIX 7.2
OracleDatabase統合監査	Oracle Database 19c

※Windowsについては基本的にファイル共有の仕組みを利用してログを収集しますが、FTP / FTPSでのログ収集も可能です。その場合、ELC に含まれるログ送信用のモジュール(SBT for WindowsEvent)をWindowsサーバ上に設置する必要があります。
※Unix 系 OS のコマンド（last、scp など）の実行結果をログとして、SSHによるリモートアクセス経由で収集します。

© Infoscience Corporation

Logstorage ELC (Event Log Collector) / ログ解析機能

ファイルアクセスなど複雑なイベントログを分かり易い内容に変換

ST版以上

【ELC for Windows 解析対象】

ログ種別	内容
ローカルログオン	ローカルからのログオン / ログオン失敗
リモートログオン	リモートからのログオン / ログオン失敗
ファイルアクセス	ファイルの読み込み / 書き込み / 削除 / 名前変更 / 印刷
プロセス起動・終了	プロセスの起動 / 終了
管理者操作	管理者(Administrators)操作
Windowsファイアウォール	ファイアウォールの有効 / 無効、ルール作成 / 変更 / 削除、ポート許可 / ブロック
システム設定変更	イベントログの削除 / 時刻変更 / タスクスケジュール登録 / サービス登録

【ELC for NetApp / EMC 解析対象】

ログ種別	内容
ログオン・ログオフ	NetApp / EMCストレージへのログオン / ログオン失敗 / ログオフ
ファイルアクセス	NetApp / EMCストレージ上のファイルの読み込み / 書き込み / 削除 / 名前変更など
管理者操作	NetApp / EMCストレージ上での管理者操作

© Infoscience Corporation

Logstorage SBT (Secure batch transfer)

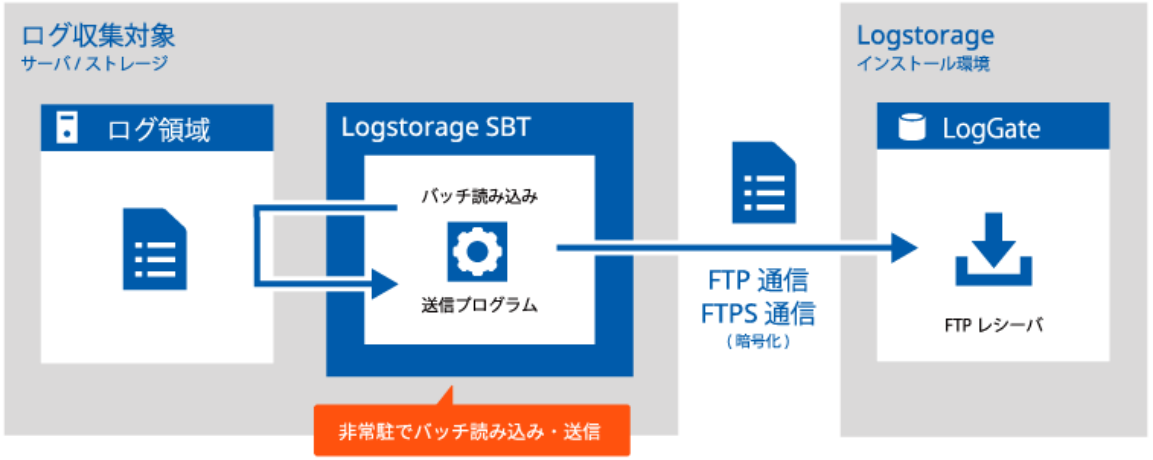
テキストログ・イベントログを定期的に圧縮・暗号化送信

テキストログ、イベントログを圧縮、暗号化してLogGateに送信するクライアントツールです。

- **非常駐型のため低負荷**
  SBTは非常駐型で、タスクスケジューラやcronなど
  スケジュール機能から実行するため、対象サーバに
  与える負荷を最小限に抑えます。

- **定期、圧縮送信による通信負荷軽減**
  gz形式へ圧縮してからLogGateへ転送することで、
  ネットワークにかかるトラフィックを大幅に軽減する
  ことができます。

- **暗号化で安全な通信**
  ログデータを暗号化してからLogGateへ転送する
  ことで、通信経路上の盗み見を未然に防ぎます。



< Logstorage SBTによるログ収集イメージ >

機能	説明
ログのFTP / FTPS送信機能	FTP、またはFTPSで監視対象のログファイルを転送することができます。
ログ送信切り換え機能	送信先へ接続できない場合、接続先を切り換えて送信することができます。
圧縮転送機能	ログソース（クライアント）側で送信前にzip形式へ圧縮してから転送することができます。
日付ローテートログの送信機能	ローテートされたログファイルを追跡し、ログを送信することができます。
オプションライセンス	**説明**
SBT for Oracle	Oracle監査を分かり易い形式に解析する機能を持つSBTです。
SBT for Windows Event	Windowsイベントログ（セキュリティ）を分かり易い形式に解析する機能を持つSBTです。※ELCパッケージに同梱されています。

© Infoscience Corporation

クラウド・各種サービスのログ収集

クラウドサービスのログを効率的に収集・分析

検索・集計・レポート条件テンプレートが用意されているので、ログ分析が容易に可能。
ログの長期保管・圧縮保管・暗号化・改ざん検出機能にも対応！

aws	Azure	Microsoft 365	Google Workspace	Google Cloud	box	cybereason

製品	対応サービス / 機能
AWS	AWS CloudTrail, AWS Config, Amazon CloudWatch Logs, Amazon CloudWatch Metrics, AWS Billing, Amazon S3, Amazon ELB, Amazon RDS, Amazon CloudFront, Amazon S3 オブジェクト
Azure	Azure Activity Log, Azure Virtual Machine, Azure Storage, Azure Network Security Group, Microsoft Entra ID (旧称 Azure Active Directory)
GCP	管理アクティビティ監査ログ, システムイベント監査ログ, データアクセス監査ログ, VPCフローログ, メトリックスデータ(仮想マシン)
Box	Enterprise Events
Microsoft 365	Microsoft 365 監査ログ (Microsoft Entra ID (旧称 Azure Active Directory), Exchange, SharePoint, OneDrive for Business, Microsoft Teams) Microsoft 365 メッセージ追跡ログ (MessageTrace, MessageTraceDetail)
Google Workspace	管理コンソール, ログイン, SAML, OAuth トークン, ユーザーアカウント, グループ, ドライブ, デバイス
Cybereason	MALOP,マルウェア, 監査ログ

クラウド他、各種サービスのログも収集可能

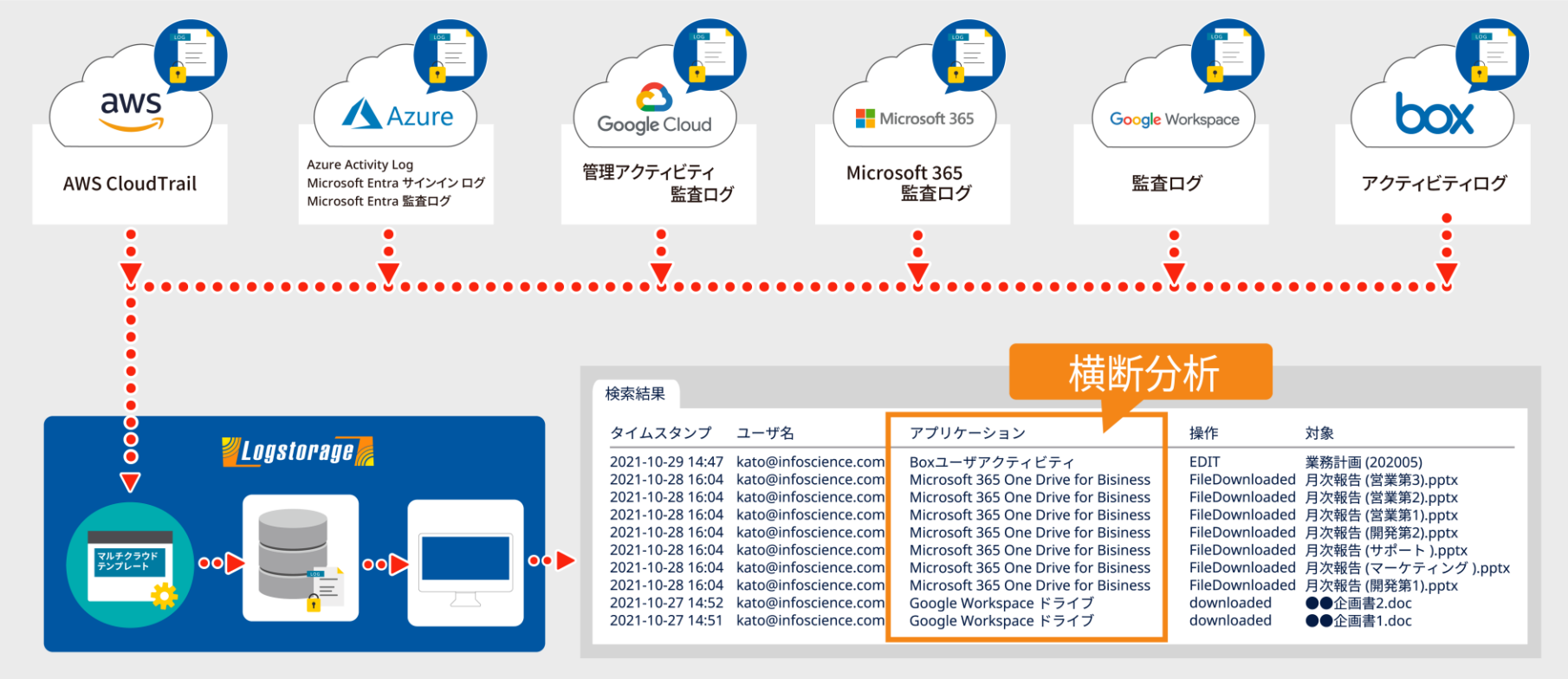
他、各種サービスにも対応しています。

paloalto	iDoperation	HIBUN	SKYSEA Client View	CWAT	MylogStar	Access Check	SSDB監査	i-FILTER	PISO	LANSCOPE	DEFESA Logger	MaLion

© Infoscience Corporation

Logstorage で収集したクラウドサービスログを横断的に分析・レポート

Logstorage Cloud Solutions に含まれる連携製品を横断分析できるテンプレートです。



対応しているLogstorage Cloud Solutions 連携パックを2つ以上ご購入の方に

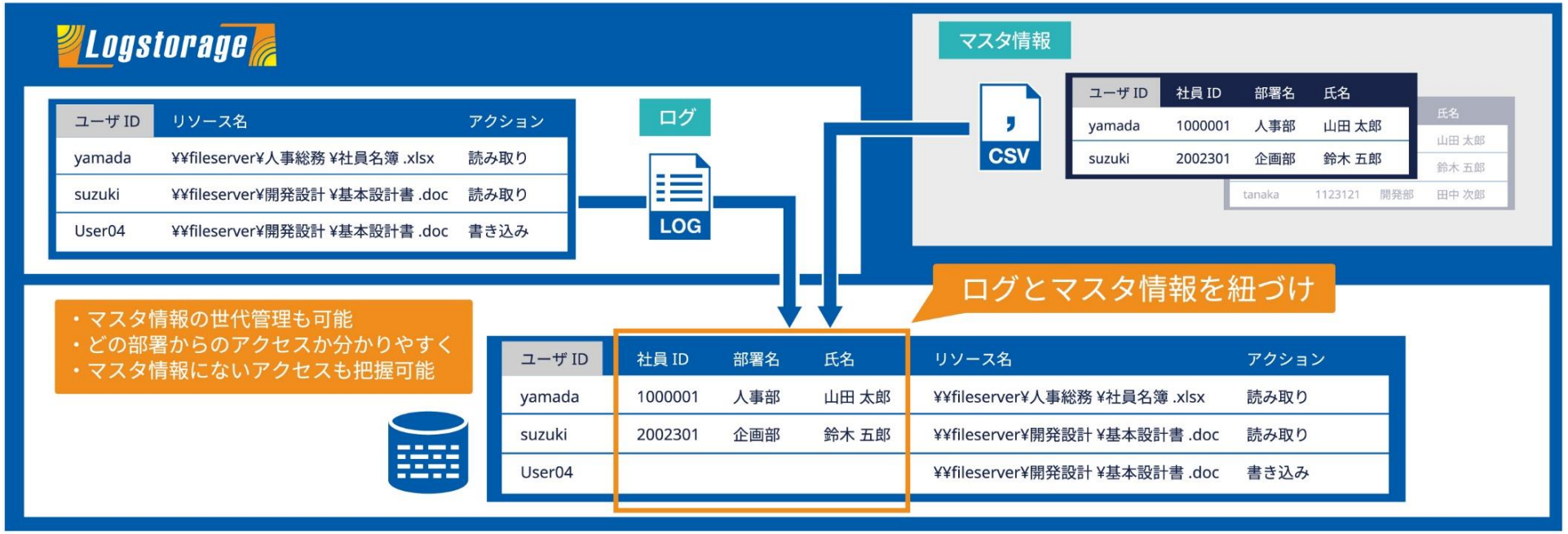
無償提供いたします。

© Infoscience Corporation

マスタ連携機能

ログに含まれない情報を付加することにより、ログをより理解しやすい内容に

ログ収集時にログとマスタ情報との紐づけを行うことで、ログに含まれない情報を付加できる機能です。



活用例

ネットワーク機器への未許可端末からのアクセス

ネットワーク機器のトラフィックログに、利用許可されている端末のマスタ情報を紐づけることにより、許可されていない端末からのアクセスを把握。

クラウド型ファイル共有システムへの外部業者からのアクセス

クラウド型ファイル共有システムのログに、外部業者（取引先）のマスタ情報を紐づけることにより、共有ファイルにアクセスしている外部業者を把握。

部署単位での印刷頻度、枚数

印刷履歴のログに、人事マスタ情報を紐づけることにより、部署単位での印刷頻度や枚数を把握。

社内用カレンダー情報との紐づけによる休日、祝日のアクセス

ログのタイムスタンプの日付に、社内用カレンダー情報を紐づけることにより休日・祝日のアクセスをより分かりやすく。

© Infoscience Corporation

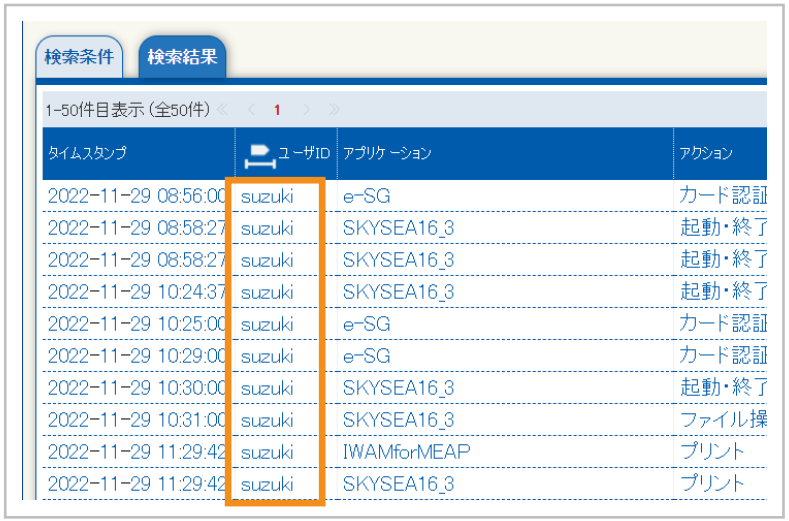
Logstorage 機能・特徴

- Logstorage システム構成
- Logstorage ログ収集機能
- Logstorage ログ分析・管理機能

© Infoscience Corporation

全てのログを横断追跡

- **異なるシステムのログも横断・横串検索**
- **検索条件設定 / 保存機能**
  ⇒ パターン化された検索条件を定型化
- **ログのトラッキング機能**
  ⇒ クリック操作によるログの絞込み
  ⇒ 検索結果画面のカスタマイズ機能
- **ログビュー表示機能**
- **インデックス機能**
  ⇒ リアルタイムにインデックスを作成し、高速検索



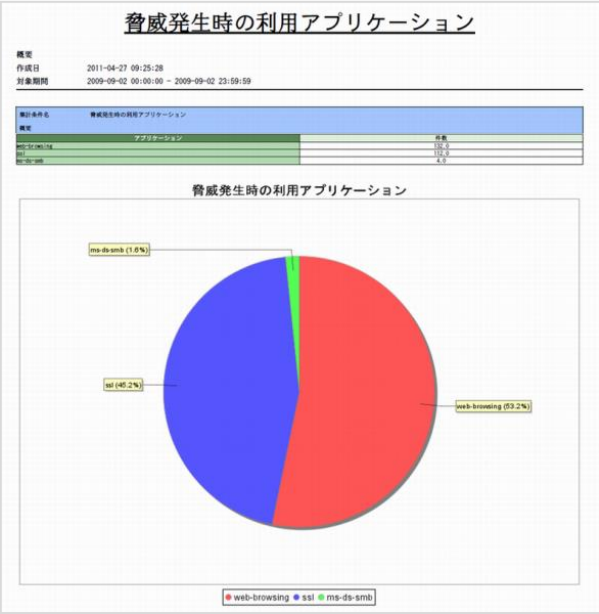
< 横断検索例 >

< 絞込検索例 >

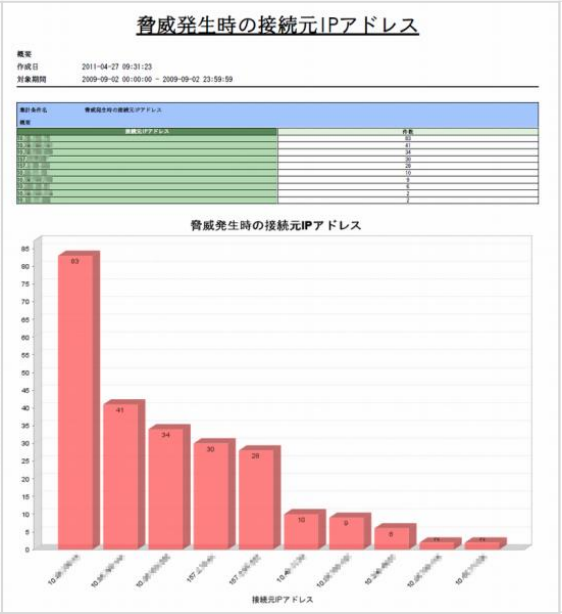
© Infoscience Corporation

ログから全体の兆候を分析

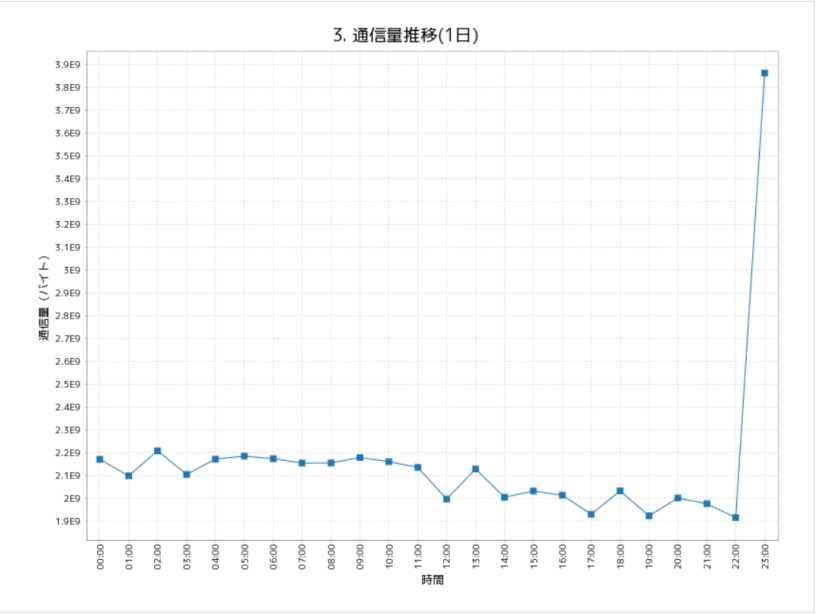
- **レポート出力の定期・自動実行**
  ⇒ 件数、トップ10、最大、最小、平均、合計
- **集計結果を表形式またはグラフ形式により表示**
  ⇒ 折れ線グラフ、棒グラフ、円グラフ、2軸グラフ等
- **集計結果のCSV形式ダウンロード**
- **集計条件を保管して作業を定型化**



< 円グラフ例 >



< 棒グラフ例 >



< 折れ線グラフ例 >

© Infoscience Corporation

異常な兆候をリアルタイムに検知・通知

- ログの発生頻度による検知
- 多様な通知方法
  ⇒ メール送信 / SNMP Trap / 外部コマンド実行
- 異なる種類の複数ログの組み合わせによる検知
- 時間や曜日別に検知
- 検知後のアクション(通知)間隔制御
- 同時に複数の検知方法を指定可能
- 検知したログメッセージを通知メールで送付

検知履歴検索結果

15件中1 － 15件目　1

	検知ポリシー名 [▼/▲]	検知時刻 [▼/▲]	ログメッセージ
☐	ウィルスリスク検知	2008/05/01 18:32:30	2008-04-19 09:00:00 192.168.0.3 (user.info) ServerD Symantec AntiVirus[2]: [19901, 情報, Mon Apr 14 08:20:46, DOMAIN¥WinServerA, DOMAIN] スキャン 完了: リスク: 1 スキャン済み: 18398 省略したファイル/フォルダ/ドライブ: 0
☐	ウィルスリスク検知	2008/05/01 18:32:29	2008-04-19 09:00:00 192.168.254.177 (user.info) ServerB Symantec AntiVirus[2]: [19901, 情報, Mon Apr 14 08:20:46, DOMAIN¥WinServerA, DOMAIN] スキャン 完了: リスク: 125 スキャン済み: 51118191 省略したファイル/フォルダ/ドライブ: 0
☐	ウィルスリスク検知	2008/05/01 18:32:28	2008-04-20 09:00:00 192.168.0.3 (user.info) ServerD Symantec AntiVirus[2]: [19901, 情報, Mon Apr 14 08:20:46, DOMAIN¥WinServerA, DOMAIN] スキャン 完了: リスク: 1 スキャン済み: 18398 省略したファイル/フォルダ/ドライブ: 0
☐	ウィルスリスク検知	2008/05/01 18:32:27	2008-04-20 09:00:00 192.168.254.177 (user.info) ServerB Symantec AntiVirus[2]: [19901, 情報, Mon Apr 14 08:20:46, DOMAIN¥WinServerA, DOMAIN] スキャン 完了: リスク: 12 スキャン済み: 51318291 省略したファイル/フォルダ/ドライブ: 0
☐	ウィルスリスク検知	2008/05/01 18:32:26	2008-04-18 09:00:00 192.168.0.3 (user.info) ServerD Symantec AntiVirus[2]: [19901, 情報, Mon Apr 14 08:20:46, DOMAIN¥WinServerA, DOMAIN] スキャン 完了: リスク: 1 スキャン済み: 18398 省略したファイル/フォルダ/ドライブ: 0

< リアルタイム検知・通知イメージ >

© Infoscience Corporation

モニタリングの自動化

- **レポート出力の定期・自動実行**
  ⇒ 時間毎、日毎、週毎、月毎

- **多様な出力フォーマットに対応**
  ⇒ PDF / HTML / CSV / XML

- **外部レポートエンジンによるマスタ連携**
  ⇒ ログに無いデータもレポート出力

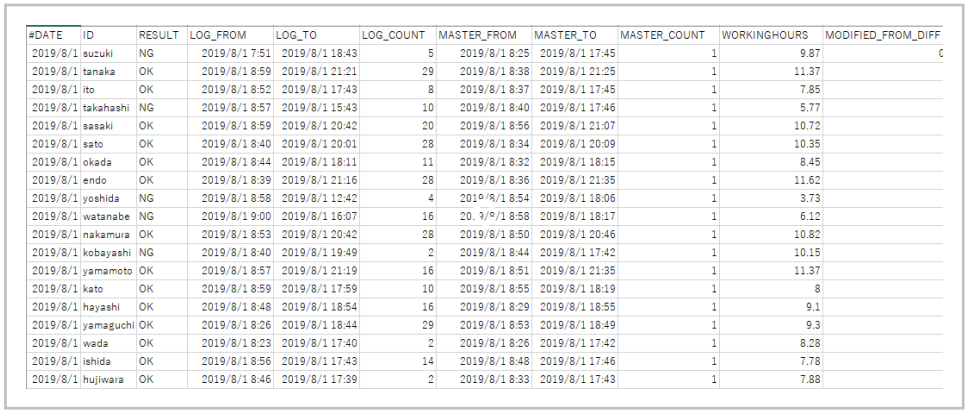
【サンプルレポート作成条件】
サーバログオン失敗レポート

概要　期間内にログオンを試行し失敗した操作の一覧
作成日　2021-10-11 16:00:08
対象期間　2021-05-01 00:00:00 - 2021-05-31 23:59:59

検索条件名	【サンプル検索条件】ログオン失敗履歴
概要	指定期間内にログオンを試行し失敗した操作を出力します。通常利用されないユーザからのアクセスや、回数の多い失敗操作の場合、不正アクセス試行の可能性があります。
件数	58件

ﾀｲﾑｽﾀﾝﾌﾟ	ﾛｸﾞｿｰｽ	ｱｸｼｮﾝ	ドメイン名	ユーザ名	成功/失敗	接続元	レコードNo	ログオンID
2021-05-25 11:58:33	172.10.1.5	ログオン（リモート認証）	logst_pdt_infos	yamada	失敗	DESKTOP-QI2OP60 10.100.10.5	105942	
2021-05-25 11:58:33	172.10.1.5	ログオン（リモート認証）	logst_pdt_infos	yamada	失敗	DESKTOP-QI2OP60 10.100.10.5	105942	
2021-05-25 11:58:33	172.10.1.5	ログオン（リモート認証）	logst_pdt_infos	yamada	失敗	DESKTOP-QI2OP60 10.100.10.5	105942	
2021-05-25 11:58:33	172.10.1.5	ログオン（リモート認証）	logst_pdt_infos	yamada	失敗	DESKTOP-QI2OP60 10.100.10.5	105942	
2021-05-25 11:58:33	172.10.1.5	ログオン（リモート認証）	logst_pdt_infos	yamada	失敗	DESKTOP-QI2OP60 10.100.10.5	105942	

< PDF出力例 >



#DATE	ID	RESULT	LOG_FROM	LOG_TO	LOG_COUNT	MASTER_FROM	MASTER_TO	MASTER_COUNT	WORKINGHOURS	MODIFIED_FROM_DIFF
2019/8/1	suzuki	NG	2019/8/1 7:51	2019/8/1 18:43	5	2019/8/1 8:25	2019/8/1 17:45	1	9.87	0
2019/8/1	tanaka	OK	2019/8/1 8:59	2019/8/1 21:21	29	2019/8/1 8:38	2019/8/1 21:25	1	11.37	
2019/8/1	ito	OK	2019/8/1 8:52	2019/8/1 17:43	8	2019/8/1 8:37	2019/8/1 17:45	1	7.85	
2019/8/1	takahashi	NG	2019/8/1 8:57	2019/8/1 15:43	10	2019/8/1 8:40	2019/8/1 17:46	1	5.77	
2019/8/1	sasaki	OK	2019/8/1 8:59	2019/8/1 20:42	20	2019/8/1 8:56	2019/8/1 21:07	1	10.72	
2019/8/1	sato	OK	2019/8/1 8:40	2019/8/1 20:01	28	2019/8/1 8:34	2019/8/1 20:09	1	10.35	
2019/8/1	okada	OK	2019/8/1 8:44	2019/8/1 18:11	11	2019/8/1 8:32	2019/8/1 18:15	1	8.45	
2019/8/1	endo	OK	2019/8/1 8:39	2019/8/1 21:16	28	2019/8/1 8:36	2019/8/1 21:35	1	11.62	
2019/8/1	yoshida	NG	2019/8/1 8:58	2019/8/1 12:42	4	201ﾟ/8/1 8:54	2019/8/1 18:06	1	3.73	
2019/8/1	watanabe	NG	2019/8/1 9:00	2019/8/1 16:07	16	20. ｦ/ﾟ/1 8:58	2019/8/1 18:17	1	6.12	
2019/8/1	nakamura	OK	2019/8/1 8:53	2019/8/1 20:42	28	2019/8/1 8:50	2019/8/1 20:46	1	10.82	
2019/8/1	kobayashi	NG	2019/8/1 8:40	2019/8/1 19:49	2	2019/8/1 8:44	2019/8/1 17:42	1	10.15	
2019/8/1	yamamoto	OK	2019/8/1 8:57	2019/8/1 21:19	16	2019/8/1 8:51	2019/8/1 21:35	1	11.37	
2019/8/1	kato	OK	2019/8/1 8:59	2019/8/1 17:59	10	2019/8/1 8:55	2019/8/1 18:19	1	8	
2019/8/1	hayashi	OK	2019/8/1 8:48	2019/8/1 18:54	16	2019/8/1 8:29	2019/8/1 18:55	1	9.1	
2019/8/1	yamaguchi	OK	2019/8/1 8:26	2019/8/1 18:44	29	2019/8/1 8:53	2019/8/1 18:49	1	9.3	
2019/8/1	wada	OK	2019/8/1 8:23	2019/8/1 17:40	2	2019/8/1 8:26	2019/8/1 17:42	1	8.28	
2019/8/1	ishida	OK	2019/8/1 8:56	2019/8/1 17:43	14	2019/8/1 8:48	2019/8/1 17:46	1	7.78	
2019/8/1	hujiwara	OK	2019/8/1 8:46	2019/8/1 17:39	2	2019/8/1 8:33	2019/8/1 17:43	1	7.88	

< CSV出力例 >

Office 365 Exchange メールボックスの転送設定

概要　メール転送設定のアクティビティを検索します。
作成日　2021-10-26 11:23:49
対象期間　2021-11-01 00:00:00 - 2021-11-30 23:59:59

検索条件名	Office 365 Exchange メールボックスの転送設定
概要	メール転送設定のアクティビティを検索します。
件数	1件

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザーID	ｱｸｼｮﾝ	クライアントIP	パラメータ名	パラメータ値	レコード種類	レコード種類（マスタ）
2021-11-26 09:54:49	kato@infoscience.com	Set-Mailbox	100.10.0.1:6253	Identity ForwardingSmtpAddress DeliverToMailboxAndForward	JPNPR01A003.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/infoscience.com/kato smtp:m.kato.01@gmail.com False	1	ExchangeAdmin

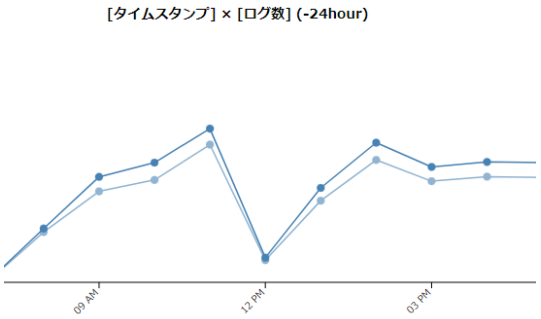
< HTML出力例 >

© Infoscience Corporation

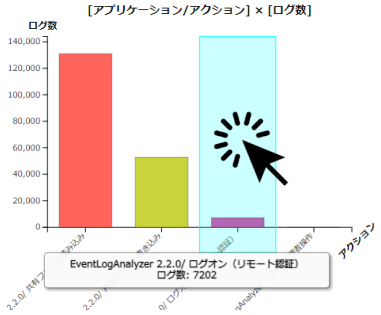
日々のログをダッシュボード化

- **大量のログでもストレスフリーに高速分析**
- **画面操作による直感的な分析**
  ⇒ 絞り込み、フィルター、積上げ表示、周期比較
- **自由に選択できるグラフ表示**
  ⇒ 折れ線グラフ、棒グラフ、円グラフ、ドーナツグラフ等
- **インサイトボード条件の作成、保存**
  ⇒ 分析対象・期間を指定、指定タグから件数をグラフ表示
- **ドリルスルーを活用した詳細分析**
  ⇒ インサイト画面からダイレクトに検索実行

ダッシュボード上からログの**高速抽出**、**ドリルスルー**による**詳細分析**が可能



1日前の**ログ量の比較で傾向分析**



不審な**ログは即時詳細分析**

アクション	ログメッセージ	
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1
ログオン(リモート認証)	EventLogAnalyzer[2.6.0] remote logon TEST.CO.JP¥info01 0x1602BB	10.100.10.211 失敗 110961 1

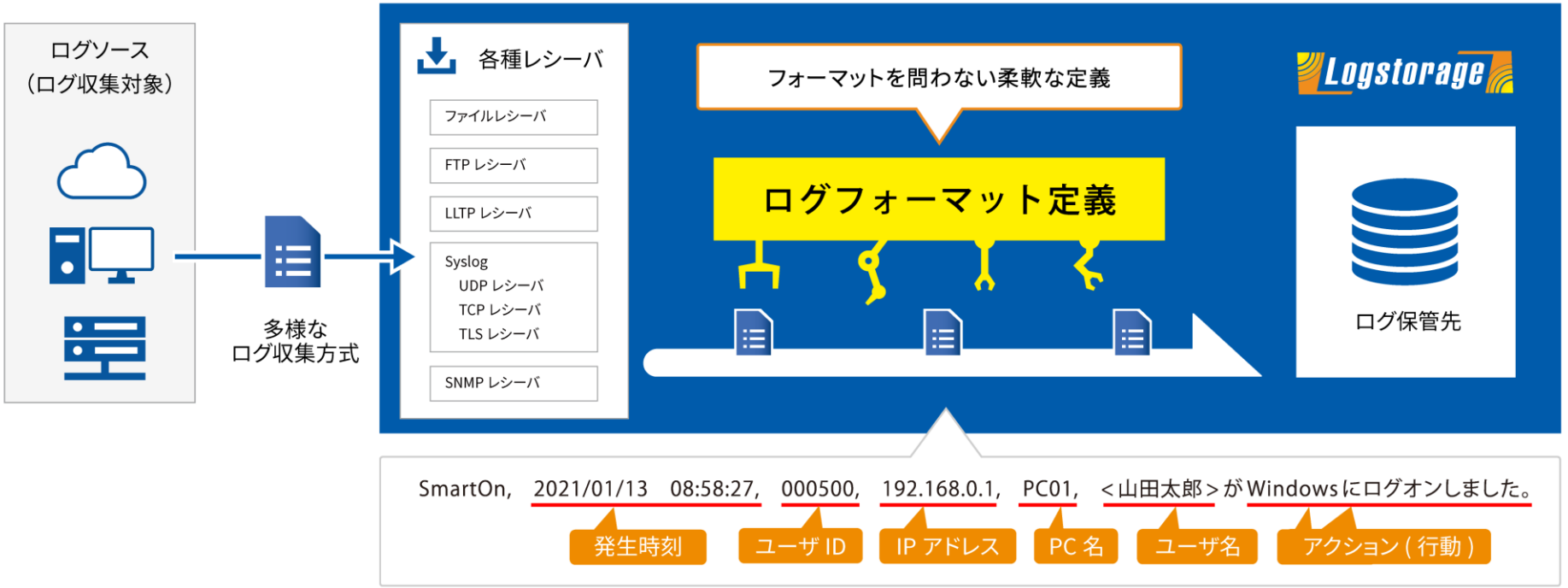
同じ接続元アドレスで**ログオンの失敗が繰り返されている**

© Infoscience Corporation

ログフォーマット定義機能

多様なログ収集方式 / 柔軟なログフォーマット定義機能により、ログの分析が自由自在

- ログフォーマット管理機能によりアプリケーション毎のログ管理が可能
- ウィザード機能によるログフォーマット定義の自動生成が可能
- インポート/エクスポート機能によりログフォーマットの更新/追加が可能



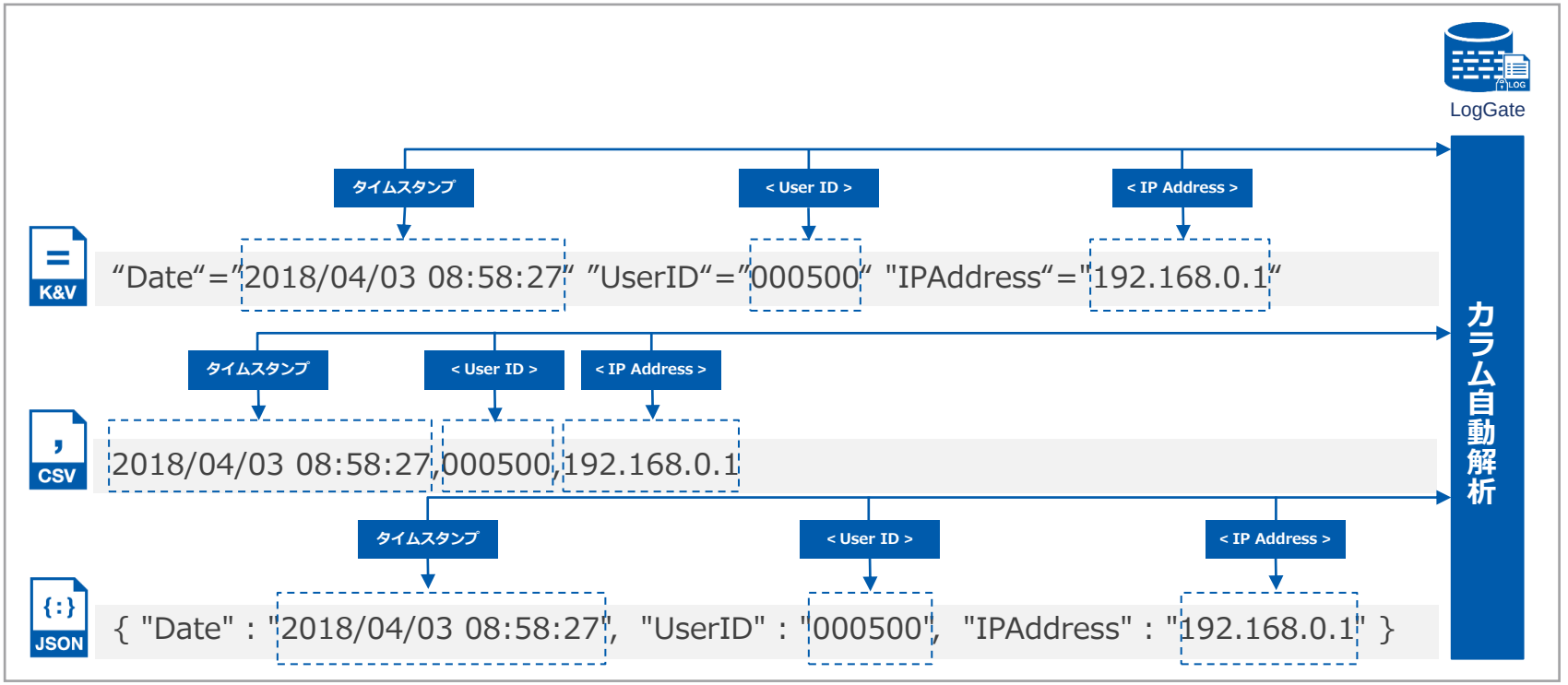
特許取得	特許番号：特許4050497　名称：ログ情報管理装置及びログ情報管理プログラム

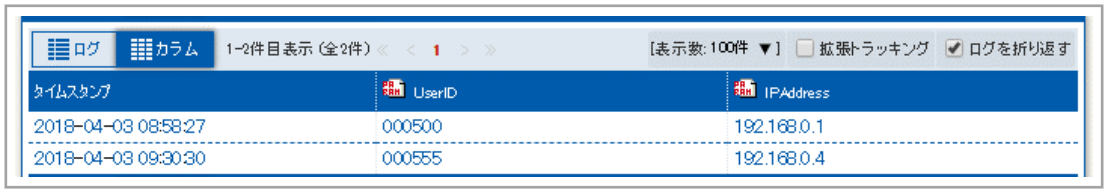
© Infoscience Corporation

ログフォーマット自動解析機能

ログ受信時のスキーマ定義、正規表現設定が一切不要

- レシーバ設定でファイル形式を指定するだけで取り込み可能
- 正規表現など複雑な設定を省き、設定を大幅に簡略化
- 自動解析されたカラムを使った横断検索機能

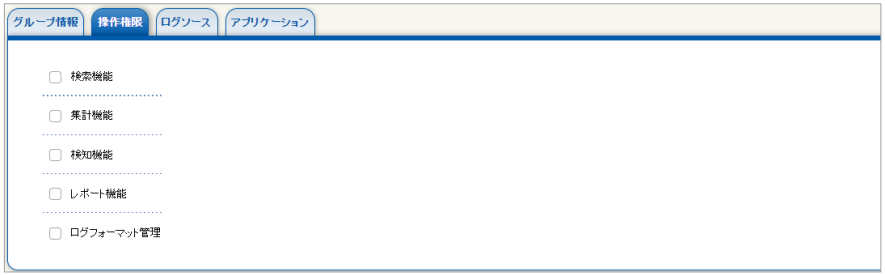


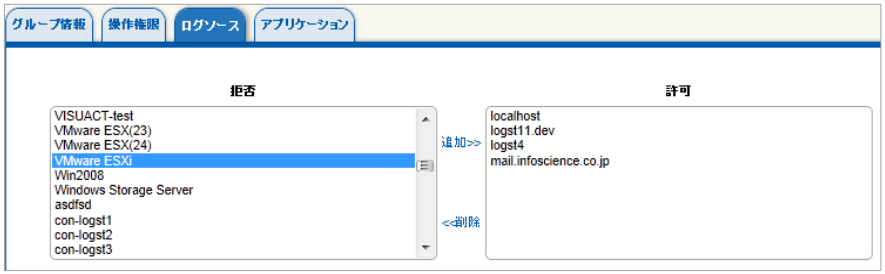


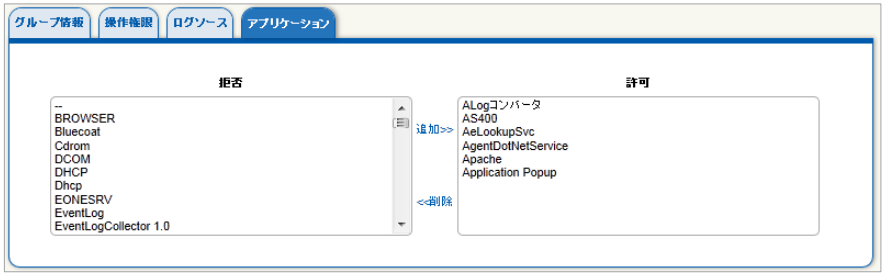
< 自動解析された検索結果画面(カラムビュー) >

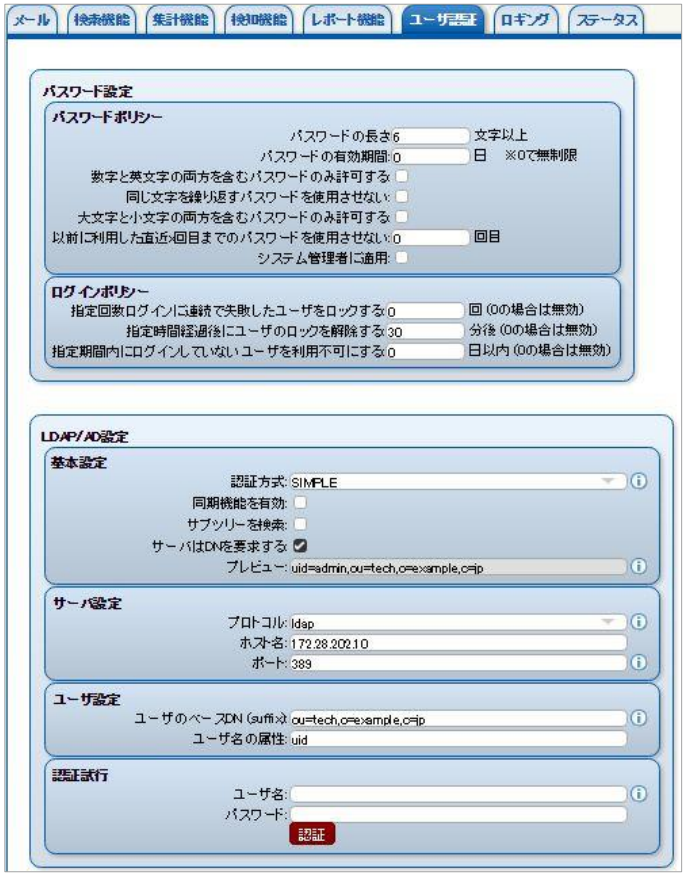
© Infoscience Corporation

グループ・ユーザ単位でのアクセス制御







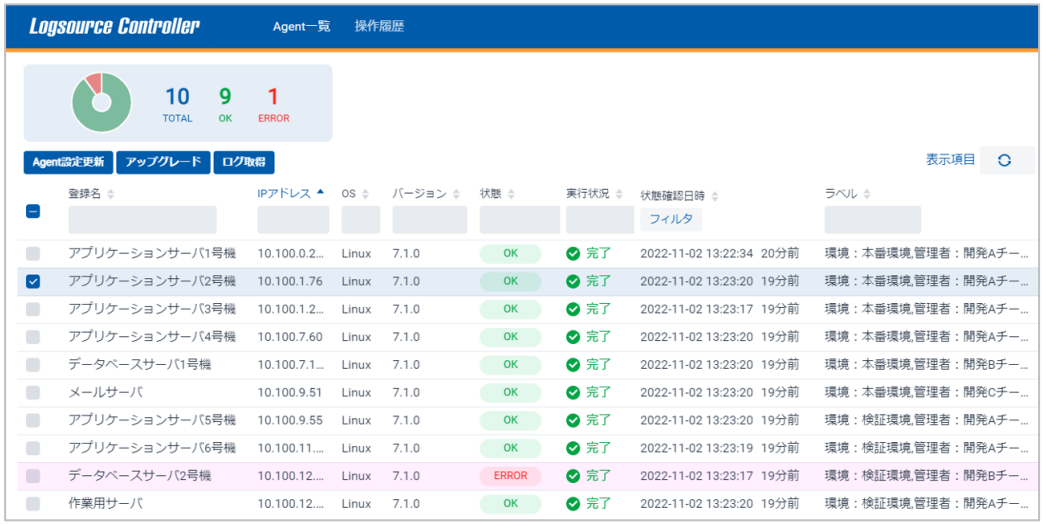


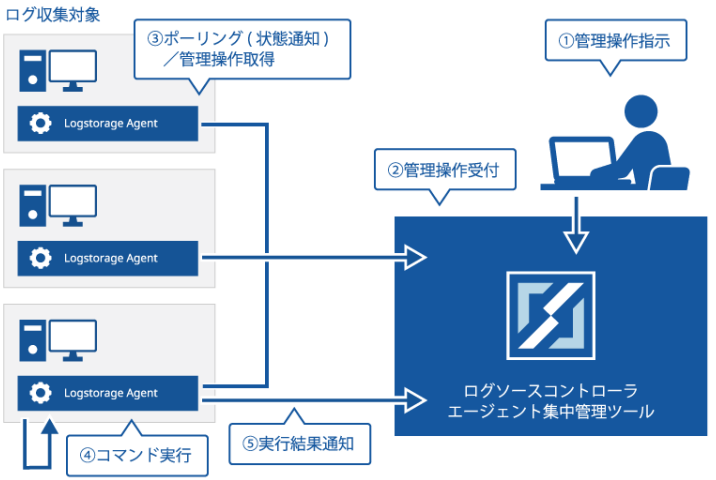
機能	説明
機能制限	検索 / 集計 / 検知 / レポート / ログフォーマット定義などアクセスコントロールをきめ細かく設定できます。
ログソースへのアクセス制限	ログソース毎（ソースIP毎）にアクセスコントロールを設定できます。
LDAP/AD連携	LogstorageのユーザとLDAP/ADで管理されているユーザを連携することができます。

© Infoscience Corporation

Logsource Controller【Agent 集中管理ツール】

GUI上でAgentの集中管理を実現、設定更新・アップグレード・ログ取得を容易に





< Logsource Controllerによる管理イメージ >

機能	説明
状態確認	Agentの状態を表示します。
操作履歴確認	Agentに対する操作の実行履歴を表示します。
Agent設定ファイル更新	Agentに対して設定ファイルの更新を指示します。
アップグレード	Agentに対してバージョンアップを指示します。
ログ取得	Agentに対して動作ログ・設定ファイルをログソースコントローラに送るよう指示します。
登録解除	Agentを管理対象から除外します。

※Logsource ControllerはLogstorage本体 や EventLogCollectorと同じ筐体でも運用が可能です。（必要スペック情報については、別途お問い合わせください。）
※ご利用には、Agent Ver. 7.1.0以降が必要です。

© Infoscience Corporation

Logstorage ライセンス体系

エディション		スケールアップモデル			スケールアウトモデル	
		ワークグループ版 (WG版)	スタンダード版 (ST版)	エンハンスト版 (EH版)	エンタープライズ版 (EP版)	アドバンスト版 (AD版)
	LogGate 収集性能上限	最大 1,000 行 / 秒	最大 2,000 行 / 秒	最大 3,000 行 / 秒	4,000 行 / 秒 ～ (1台最大 2,000 行 / 秒)	6,000 行 / 秒 ～ (1台最大 3,000 行 / 秒)
	ログ量の目安	(5GB / 日)	(10GB / 日)	(15GB / 日)	(20GB / 日～)	(30GB / 日～)
基本パッケージ (ライセンス)	コンソールサーバ (WEB 管理機能)	1 台			1 台	
	LogGate	1 台			2 台～	
	クライアントライセンス (ログ収集対象サーバ台数)	5 台 (追加可能)			無制限	
	集計モジュール	オプション			○	オプション
	検知モジュール	オプション			○	オプション
	レポートモジュール	オプション			○	オプション
EventLogCollector(ELC)		—	○	○	○	○
LogGate の追加		—			○	○
複数 LogGate の横断検索・分析		—			—	○
検索専用 LogGate の設置		—			—	○
LogGate 冗長構成		○ (Active-Standby)※			○ (Active-Standby)※	○ (Active-Active)

※収集性能「行 / 秒」は検索可能になるまでの収集性能のことで「eps」とは単位が異なります。
※収集性能は目安です。
※スケールアウトモデルは LogGate を追加することで、より多くのログを収集することが可能です。
※Active-Standby はスタンバイ機も起動状態での待機となります。

© Infoscience Corporation

Logstorage 動作環境

コンソールサーバ / LogGate

	WG版／ST版／EP版	EH版／AD版
CPU	x86互換CPU 2.4GHz以上 コア数4コア以上、または4vCPU以上	x86互換CPU 2.4GHz以上 コア数8コア以上、または8vCPU以上
メモリ	12GB以上	32GB以上
ディスク容量	保存期間、取り込むログファイルサイズにより異なります	
OS	Windows Server 2016, 2019, 2022 Red Hat Enterprise Linux 6, 7, 8, 9	

Logstorage ELC

CPU	x86互換CPU 2.5GHz以上 コア数4コア以上
メモリ	1GB以上
OS	Windows Server 2016, 2019, 2022

Logsource Controller

CPU	x86互換CPU 2.0GHz以上 コア数4コア以上
メモリ	3GB以上
ディスク容量	1GB以上
OS	Windows Server 2016, 2019, 2022 Red Hat Enterprise Linux 7, 8, 9

※記載スペックは、製品部分になります。OS分の領域は別途確保いただくようお願いいたします。

© Infoscience Corporation

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

© Infoscience Corporation