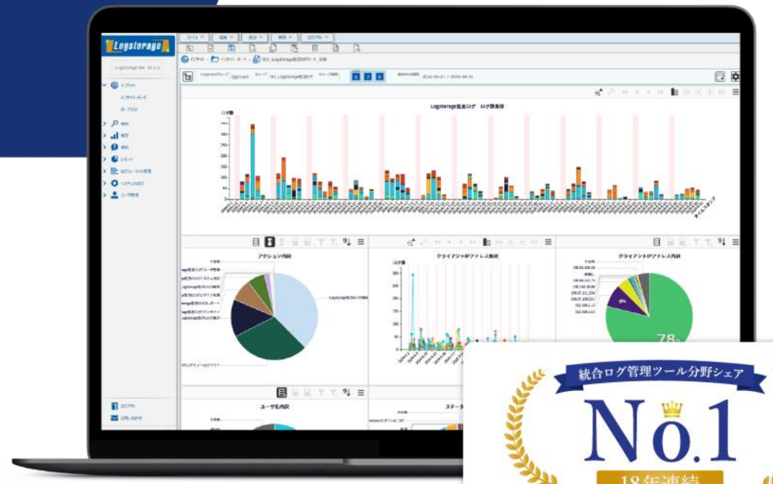
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Ver.10 製品紹介資料



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

会社概要

商号	インフォサイエンス株式会社
代表	代表取締役社長 宮 紀雄
事業内容	統合ログ管理ツール Logstorage の開発・販売 メンバーシップ管理プラットフォーム Jimzen の開発・販売 データセンター運用
従業員	100名
設立	1995年10月
拠点	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
Webサイト	https://www.infoscience.co.jp/

ISO/IEC 27001 を
取得しています。

登録組織：ネットワークオペレーションズセンター、プロダクト事業部、アドミニストレーション本部

会社概要

ソフトウェア開発において先進的な開発力を誇る総合IT企業です。
新たな価値と喜びを市場に創り出すために、情報セキュリティからクラウドサービスまで幅広い分野で、
「誰もやったことのないコト」に社員一人ひとりがチャレンジし続けています。

統合ログ管理ツール Logstorage

サーバやネットワーク機器など、企業内のあらゆる情報システムから出力される大量のログデータを、迅速・確実に収集し、独自の技術で圧縮保管するシステムです。

DXプラットフォーム Jimzen

幅広いビジネスドメインで必要となるイベント管理をはじめ、様々なITサービスをオールインワンに実装した、メンバーシッププロバイダーのためのプラットフォームです。

データセンター運用 DATA CENTER

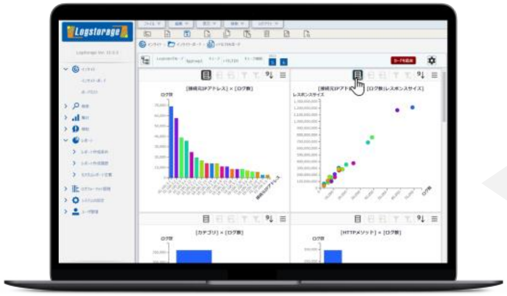
自社内のデータセンターは、独自の障害管理システムで、お客様のサーバおよびネットワーク機器の稼働状況を監視するサービスです。

Logstorageについて

Logstorageは、複雑化・高度化した情報システムの記録を、
誰でも簡単・便利に使えるものにする統合ログ管理製品です。

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。



- ログの収集
- ログの保管
- ログの検知
- 検索・集計・レポート

ELC Analytics

サーバのイベントログを
解析・管理します。

Logstorage-X/SIEM

複雑なアラートルール運用など
高度なSIEM要件に対応可能です。

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。

統合ログ管理システムLogstorageとは

企業活動のあらゆるログを統合管理することで、多様なセキュリティ課題の解決に応えるソリューションです。

多様なセキュリティ課題を解決

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）

システム運用

システムの状態把握・障害時の調査、解析

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

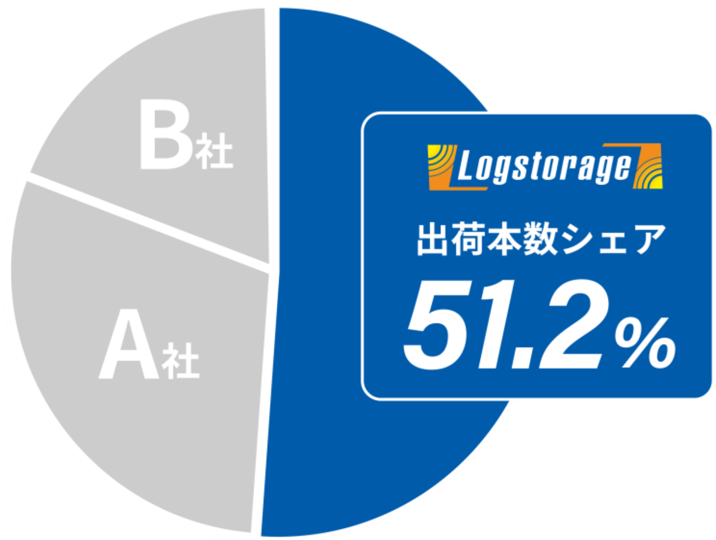
Logstorage シリーズ

統合ログ管理ツールの分野で 18年連続シェア No.1*

*出典：デロイト トーマツ ミック経済研究所2025年3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 2024年度 （統合ログ管理ツール部門）
出荷本数でシェア51.2%を獲得 https://mic-r.co.jp/mr/03370/

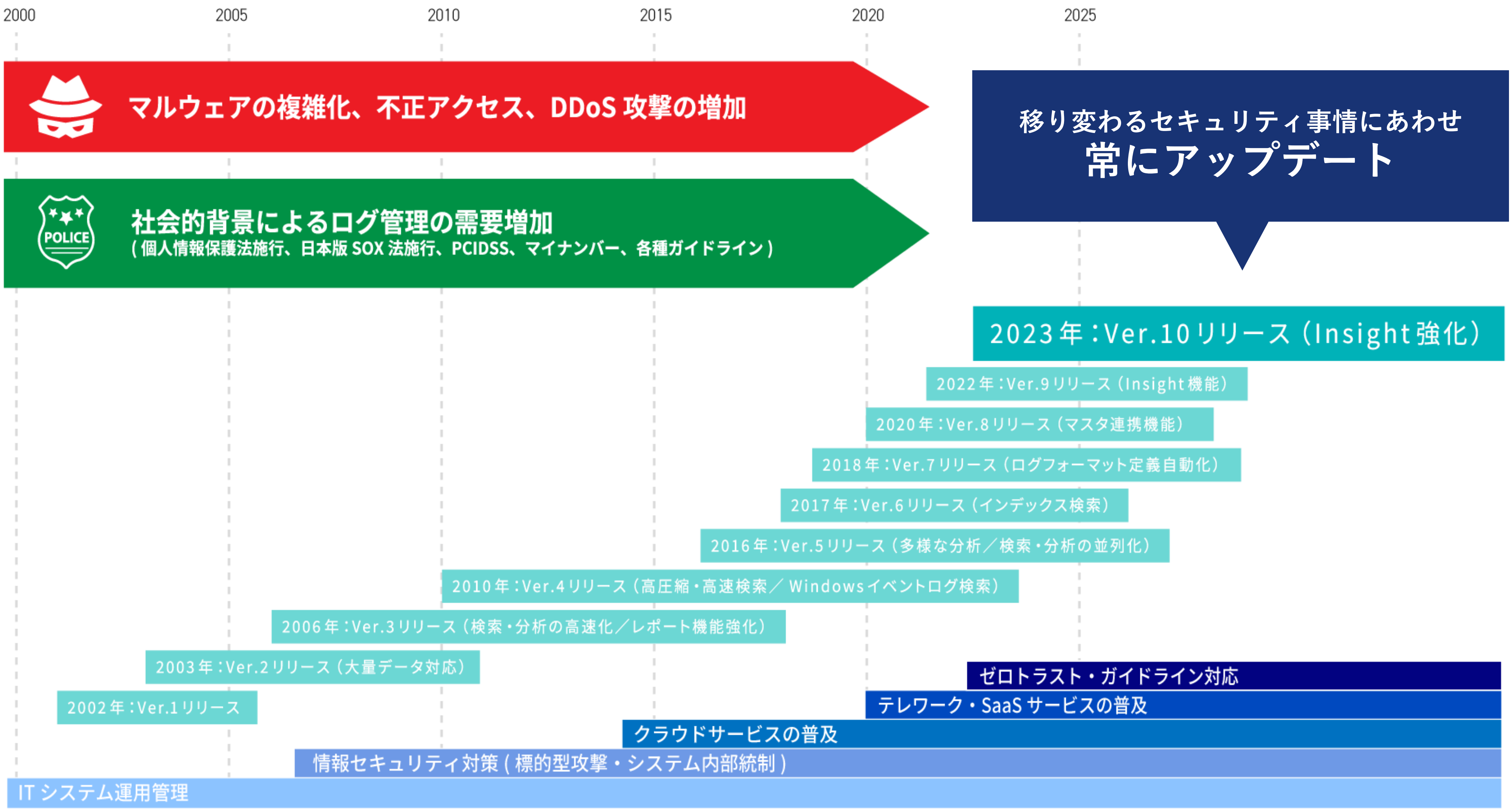
出典：富士キメラ総研 2011-2024 ネットワークセキュリティ ビジネス調査総覧《市場編》
統合ログ管理ツール（SIM/SIEM）、市場占有率、SIM、金額ベース、2023年度実績
2010年度-2023年度連続シェアNO.1

出荷本数シェアNo.1



導入実績 5,500 社以上

Logstorage 進化の歴史

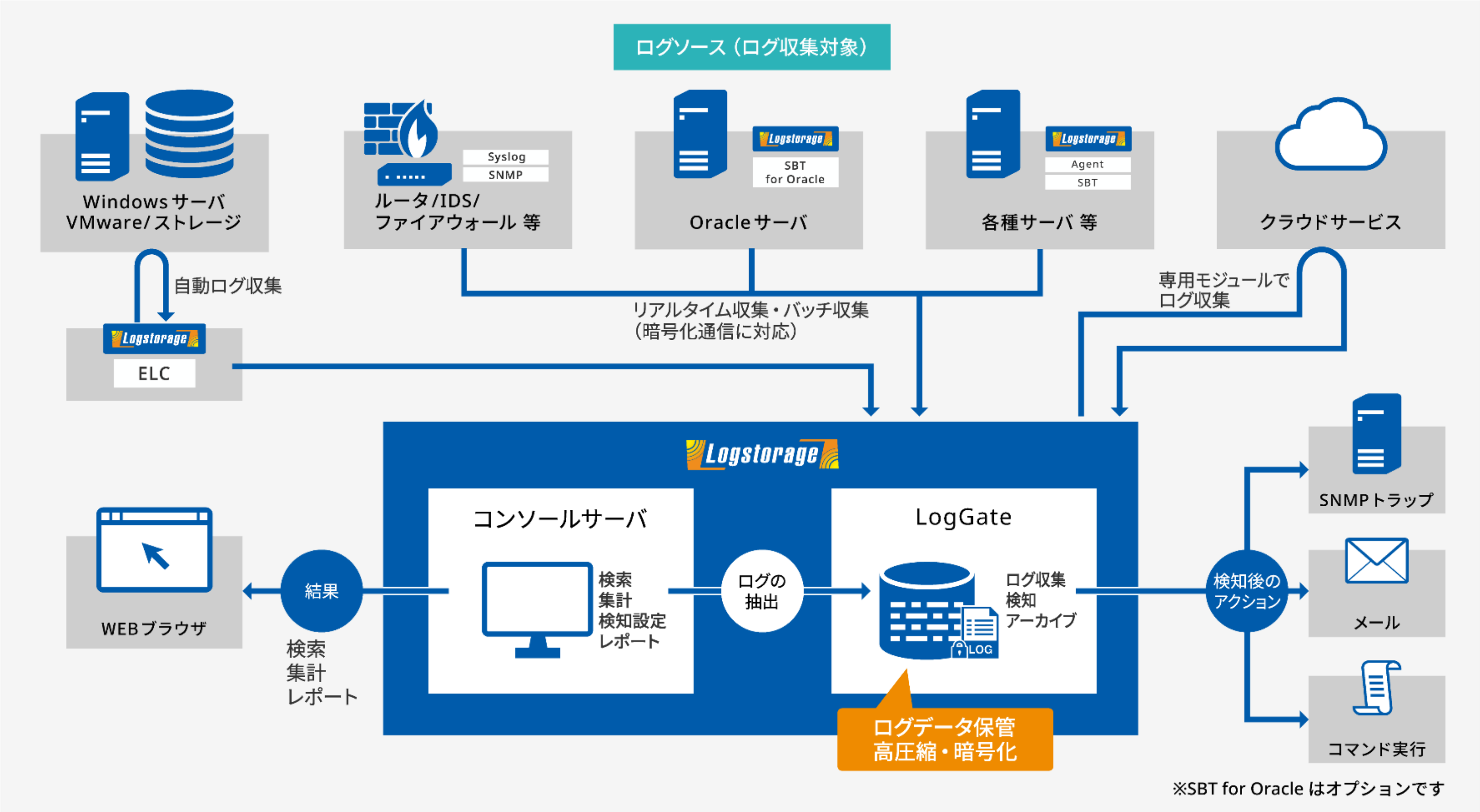


システム構成

収集機能

分析

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

システム構成

収集機能

分析

各分野でトップシェアの製品と連携！

※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。

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

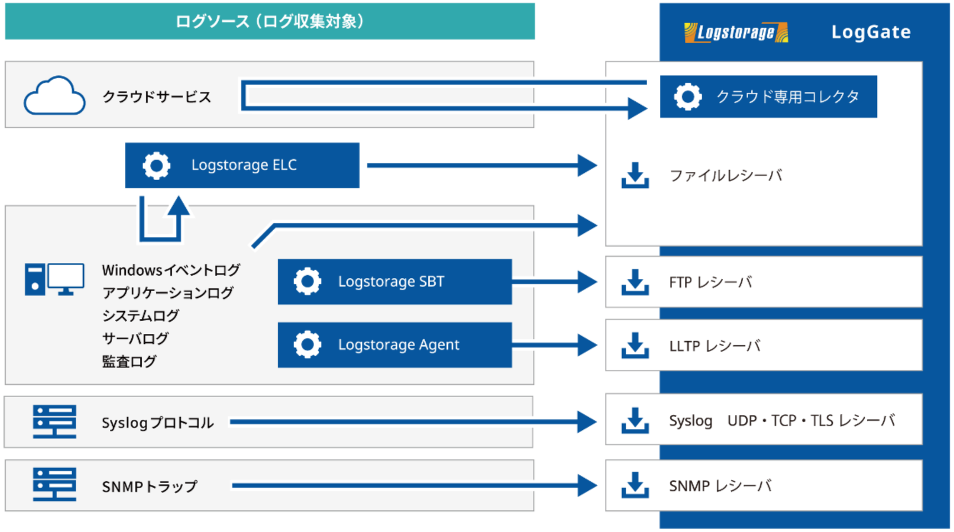
その他
Lotus Domino
Notes AccessAnalyzer2
Auge AccessWatcher
SAP R/3 (ERP)
eX-SG (入退室管理)
MSIESER
iSecurity
desknet's
HP NonStop サーバー
System Answer

※順不同

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

Logstorage Agent

テキストログ・イベントログをリアルタイム または 定期的に暗号化送信

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 または 定期的に送信可能**

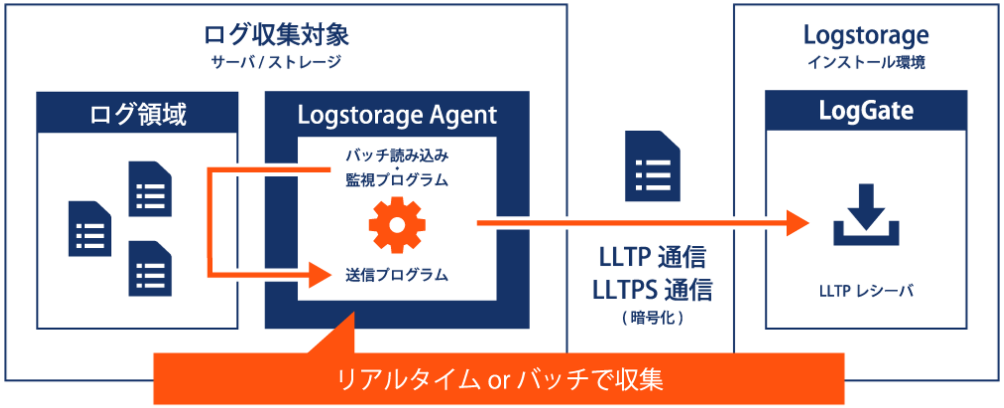
  テキスト形式のログファイルやWindowsイベントログを
  リアルタイム または バッチでLogGateへ転送することができます。

- **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 >

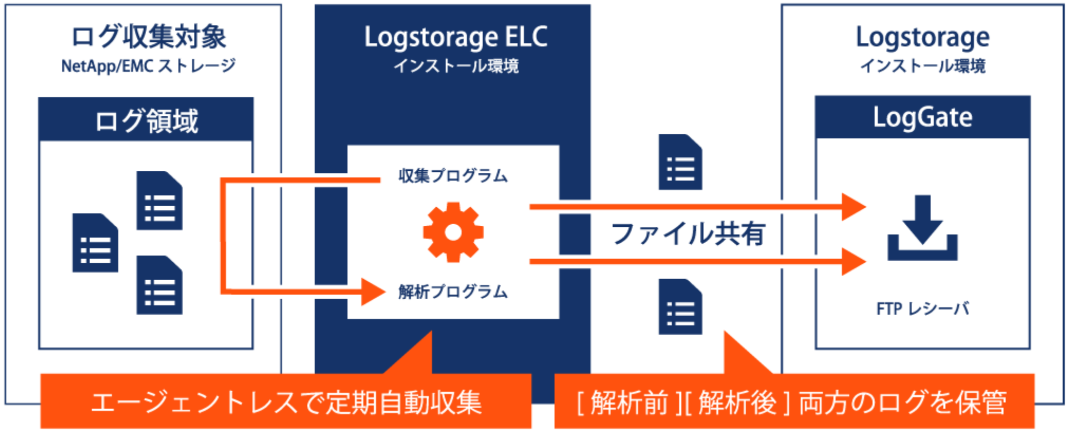
機能	説明
ログの暗号化送信機能	暗号化してログを送信することができます。
ログ送信切り換え機能	送信先へ接続できない場合、接続先を切り換えて送信することができます。
システム高負荷時の動作抑制機能	ログ・ソース（ログ収集対象）が高負荷となったとき、メインのサービスの稼動に影響しないよう、ログ送信を一時抑制します。
ブロックログの送信機能	複数行で1つの意味を持つログを解析し、1行のログとして送信することができます。
ローテートログの送信機能	ローテートされたログファイルを追跡し、ログを送信することができます。
送信ログのフィルタ機能	キーワードによるログのフィルタリングを行い、必要なログのみ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

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。



< Logstorage ELCによるログ収集イメージ >

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, Windows Storage Server 2016
NetAppイベント（クラスタモード）	Data ONTAP 9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1/9.14.1/9.15.1/9.16.1, ONTAP Select 9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1/9.14.1/9.15.1/9.16.1 Cloud Volumes ONTAP(AWS, Azure, GCP) 9.7/9.8/9.9.1/9.10.1/9.11.1/9.12.1/9.13.1/9.14.1/9.15.1/9.16.1, Amazon FSx for NetApp ONTAP 9.13.1以降
EMCイベント	Unity 5.1.3/5.2.0/5.2.1/5.3.0/5.3.1/5.4.0/5.4.1
VMwareイベント	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 7/8/9, Amazon Linux 2/2023, IBM AIX 7.2
OracleDatabase統合監査	Oracle Database 19c/23ai

※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。OracleDatabase統合監査については、ELC for Oracleの購入が必要です。
※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。

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やすい内容に変換

ST版以上

Windows イベントログ (元ログ)

検索結果

7,736件ヒット

ログ量も多く、分かりづらい

タイムスタンプ	ログメッセージ
2024-06-28 10:56:30	Security[578]: [589166, 成功の監査 , Mon Jun 28 10:56:30, NT AUTHORITY ¥ SYSTEM, WORK] ・・・
2024-06-28 10:56:30	Security[578]: [589166, 成功の監査 , Mon Jun 28 10:56:30, NT AUTHORITY ¥ SYSTEM, WORK] ・・・
2024-06-28 10:56:30	Security[578]: [589166, 成功の監査 , Mon Jun 28 10:56:30, NT AUTHORITY ¥ SYSTEM, WORK] ・・・
2024-06-28 10:56:30	Security[578]: [589166, 成功の監査 , Mon Jun 28 10:56:30, NT AUTHORITY ¥ SYSTEM, WORK] ・・・
2024-06-28 10:56:30	Security[578]: [589166, 成功の監査 , Mon Jun 28 10:56:30, NT AUTHORITY ¥ SYSTEM, WORK] ・・・

⋮

ELCを使わない場合

Logstorage ELC (Logstorageでの解析結果)

検索結果

193件ヒット

コンパクトで、見やすい

タイムスタンプ	アクション	ユーザ名	ファイルパス	ファイル名
2024-06-28 10:56:30	アプリケーション起動	ohashi	C:¥Program Files¥Lhaplus	Lhaplus.exe ・・・
2024-06-28 10:56:30	アプリケーション	ohashi	C:¥Program Files¥Lhaplus	Lhaplus.exe ・・・
2024-06-28 10:56:30	ファイル読み込み	ohashi	C:¥Documents and Settings¥Lhaplus	desktop.ini ・・・
2024-06-28 10:56:30	ファイル読み込み	ohashi	C:¥WINDOWS¥system32¥	desktop.ini ・・・
2024-06-28 10:56:30	アプリケーション起動	ohashi	C:¥Program Files¥MS Office¥	EXCEL.exe ・・・

⋮

ELCを使った場合

【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

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**

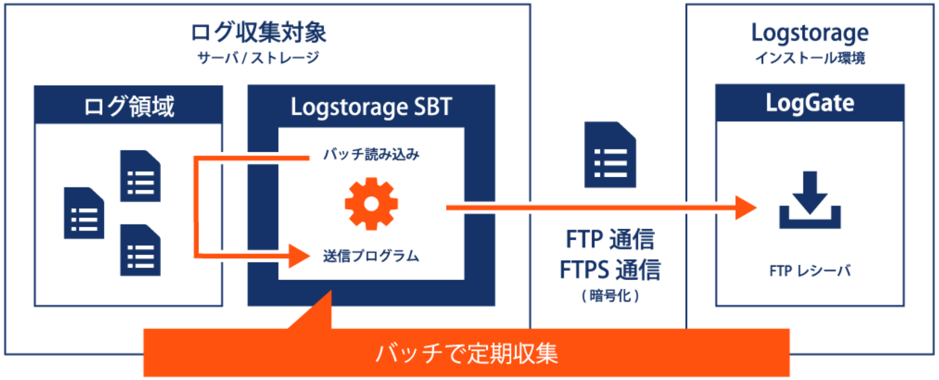
  SBTは非常駐型で、タスクスケジューラやcronなど
  スケジュール機能から実行するため、対象サーバに与える負荷を
  最小限に抑えます。

- **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監査を分かりやすい形式に解析する機能を持つSBTです。
Windowsイベントログ収集・解析ツール	**説明**
SBT for Windows Event	Windowsイベントログ（セキュリティ）を分かりやすい形式に解析する機能を持つSBTです。ST版以上の標準ツールとしてELCパッケージに同梱されています。

クラウドサービス・EDRのログ収集

クラウドサービス・EDRのログを効率的に収集・分析

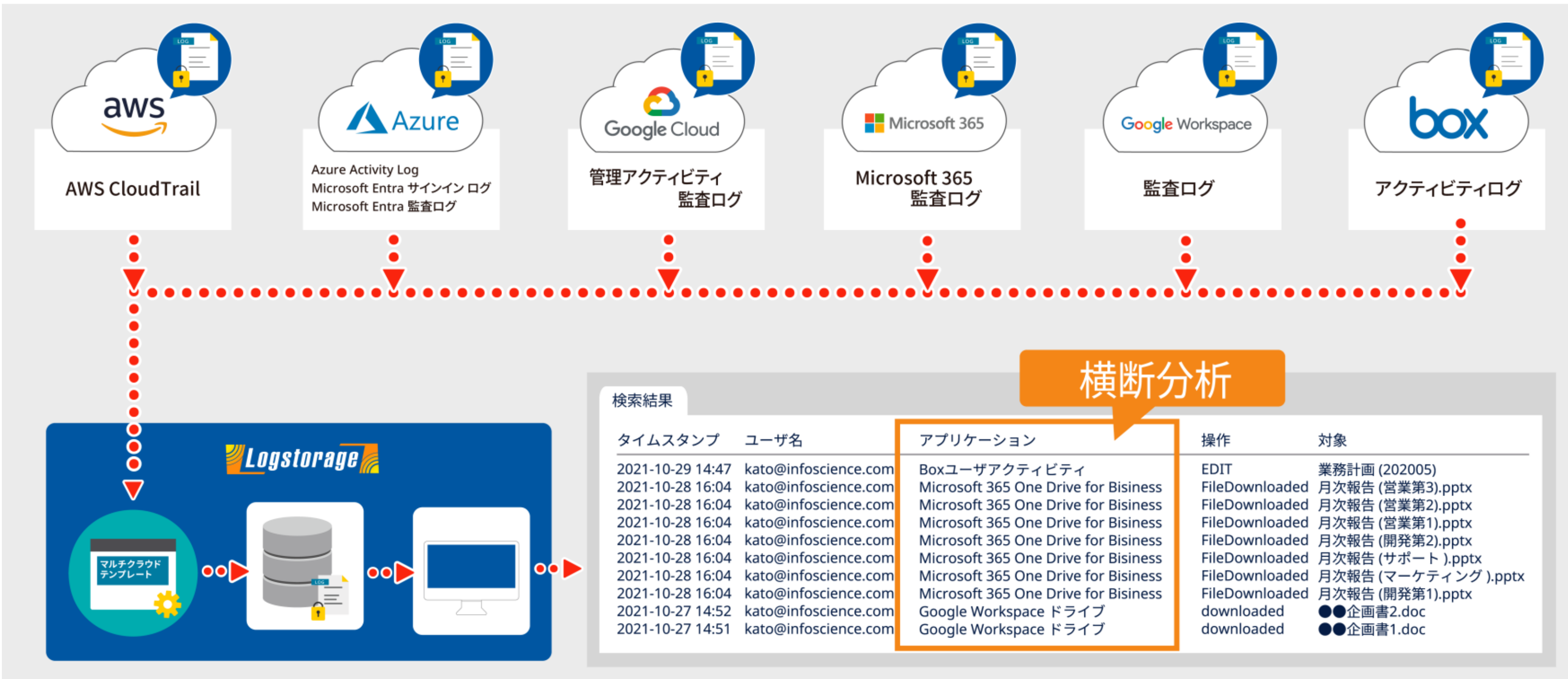
検索・集計・レポート条件テンプレートが用意されているので、ログ分析が容易に可能。
ログの長期保管・圧縮保管・暗号化・改ざん検出機能にも対応！非常駐型のため低負荷。

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, ThreatIntelligence, Quarantine, Microsoft 365 メッセージ追跡ログ (MessageTrace, MessageTraceDetail), Advanced Hunting Email (EmailAttachmentInfo, EmailEvents, EmailPostDeliveryEvents, EmailUrlInfo)
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

マルチクラウドテンプレート

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。



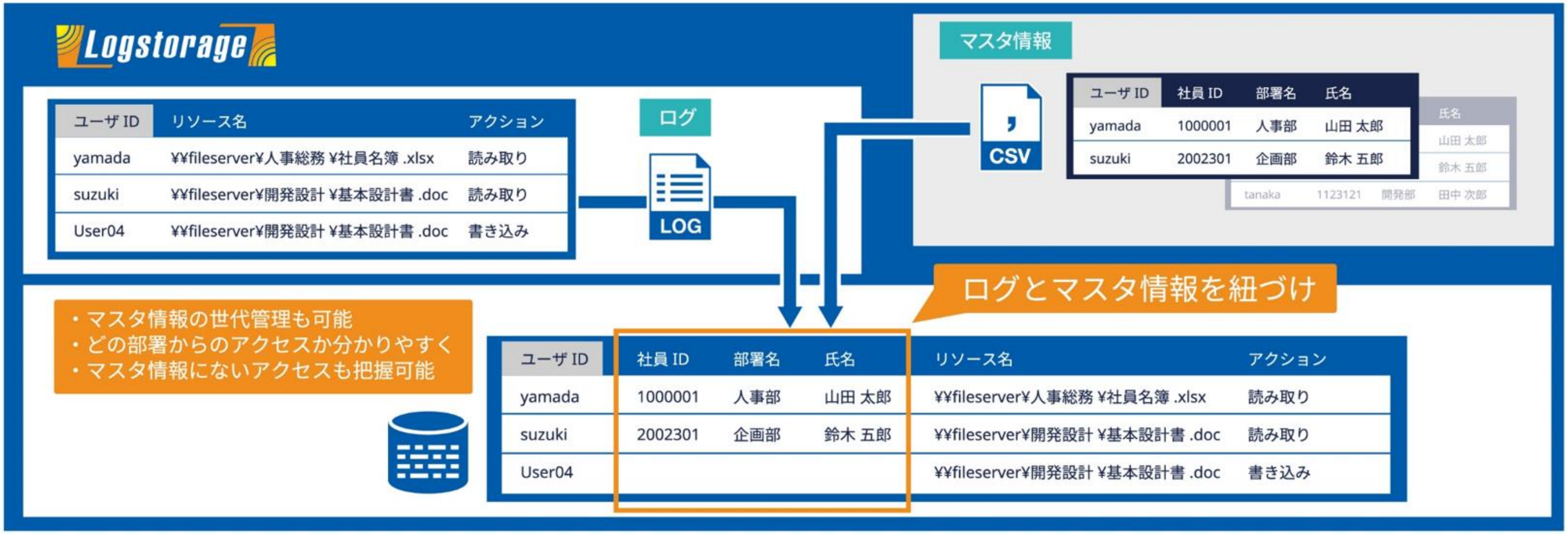
タイムスタンプ	ユーザ名	アプリケーション	操作	対象
2021-10-29 14:47	kato@infoscience.com	Boxユーザアクティビティ	EDIT	業務計画 (202005)
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (営業第3).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (営業第2).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (営業第1).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (開発第2).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (サポート).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (マーケティング).pptx
2021-10-28 16:04	kato@infoscience.com	Microsoft 365 One Drive for Bisiness	FileDownloaded	月次報告 (開発第1).pptx
2021-10-27 14:52	kato@infoscience.com	Google Workspace ドライブ	downloaded	●●企画書2.doc
2021-10-27 14:51	kato@infoscience.com	Google Workspace ドライブ	downloaded	●●企画書1.doc

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。

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。

システム構成

収集機能

分析

検索機能

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

タイムスタンプ	ユーザID	アプリケーション	アクション
2023-11-29 08:56:00	suzuki	e-SG	カード認証OK(入室)
2023-11-29 08:58:27	suzuki	SKYSEA16_3	起動・終了
2023-11-29 08:58:27	suzuki	SKYSEA16_3	起動・終了
2023-11-29 10:24:37	suzuki	SKYSEA16_3	起動・終了
2023-11-29 10:25:00	suzuki	e-SG	カード認証OK(退室)
2023-11-29 10:29:00	suzuki	e-SG	カード認証OK(入室)
2023-11-29 10:30:00	suzuki	SKYSEA16_3	起動・終了
2023-11-29 10:31:00	suzuki	SKYSEA16_3	ファイル操作
2023-11-29 11:29:42	suzuki	IWAMforMEAP	プリント
2023-11-29 11:29:42	suzuki	SKYSEA16_3	プリント

＜横断検索例＞

タイムスタンプ	作成名	作成ログイン	アカウントID	アクション
2023-05-31 16:28:31	kato	kato@infoscience.com	9999999	アップロード
2023-05-31 16:27:25	saito	saito@infoscience.com	9999999	アップロード
2023-05-31 16:00:46	saito	saito@infoscience.com	9999999	ログイン
2023-05-31 16:00:46	saito	saito@infoscience.com	9999999	ログイン追加
2023-05-31 15:50:22	kato	kato@infoscience.com	9999999	名称変更
2023-05-31 15:49:45	saito	saito@infoscience.com	9999999	名称変更
2023-05-31 15:49:24	kato	kato@infoscience.com	9999999	名称変更
2023-05-31 15:49:15	kato	kato@infoscience.com	9999999	ファイルのオープン
2023-05-31 15:49:15	kato	kato@infoscience.com	9999999	ダウンロード

タイムスタンプ	作成名	作成ログイン	アカウントID	アクション
2023-05-31 16:27:25	saito	saito@infoscience.com	9999999	アップロード
2023-05-31 16:00:46	saito	saito@infoscience.com	9999	
2023-05-31 16:00:46	saito	saito@infoscience.com	9999	
2023-05-31 15:49:45	saito	saito@infoscience.com	9999	
2023-05-31 15:49:04	saito	saito@infoscience.com	9999	
2023-05-31 15:48:50	saito	saito@infoscience.com	9999999	ファイルのオープン
2023-05-31 15:48:50	saito	saito@infoscience.com	9999999	ダウンロード
2023-05-31 15:48:48	saito	saito@infoscience.com	9999999	アップロード
2023-05-31 15:48:21	saito	saito@infoscience.com	9999999	アップロード

＜絞込検索例＞

集計機能

ログから全体の兆候を分析

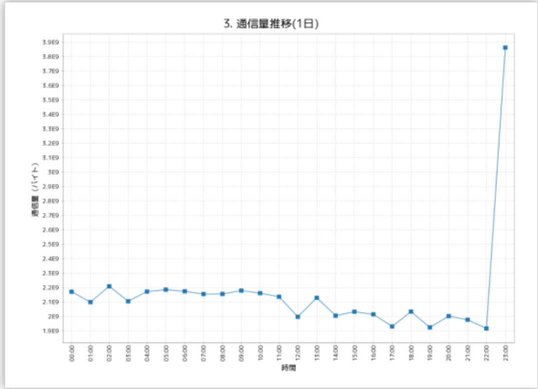
- **ログを様々な観点から集計**

  ⇒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

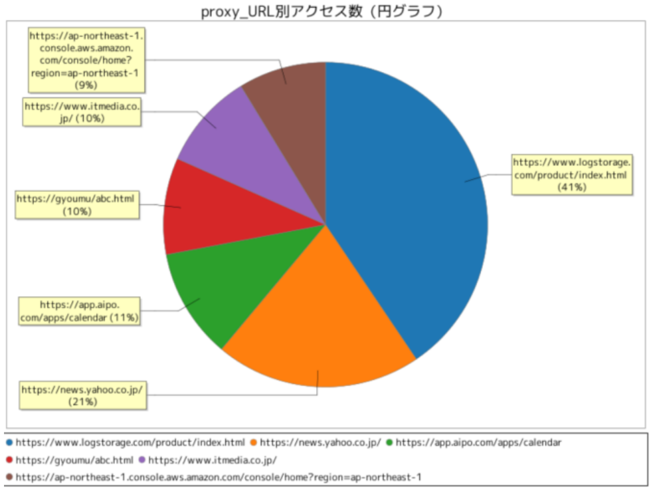
- **集計結果のCSV形式ダウンロード**
- **集計条件を保管して作業を定型化**



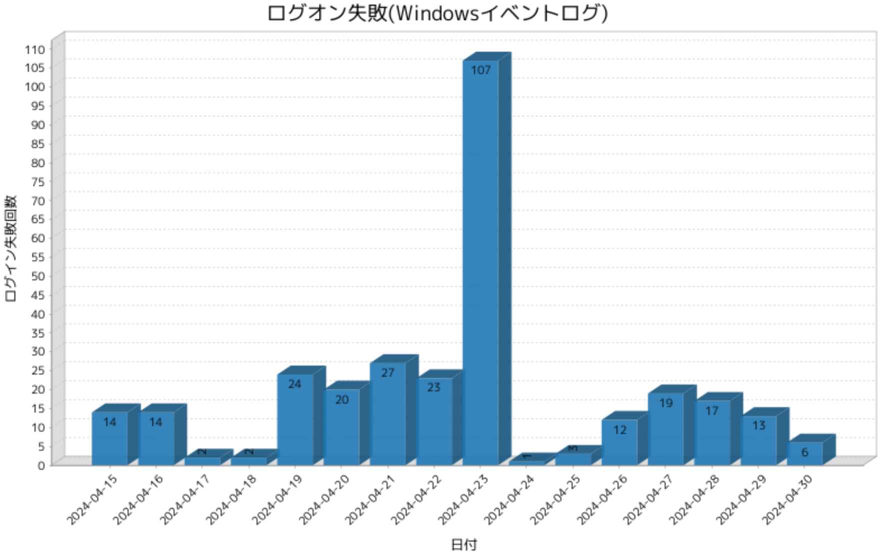
< 折れ線グラフ例 >

日付	ログイン失敗回数 件数
2024-04-15	14
2024-04-16	14
2024-04-17	2
2024-04-18	2
2024-04-19	24
2024-04-20	20
2024-04-21	27
2024-04-22	23
2024-04-23	107
2024-04-24	1
2024-04-25	3
2024-04-26	12
2024-04-27	19
2024-04-28	17
2024-04-29	13
2024-04-30	6
総合計	304

< 表集計例>



< 円グラフ例 >



< 棒グラフ例 >

検知機能

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	2024/05/01 18:32:30	2024-04-19 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	2024/05/01 18:32:29	2024-04-19 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	2024/05/01 18:32:28	2024-04-20 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	2024/05/01 18:32:27	2024-04-20 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	2024/05/01 18:32:26	2024-04-18 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 >

レポート機能

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

タイムスタンプ	ログソース	アクション	ドメイン名	ユーザ名	ログオンID	レコードNo	回数	詳細
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56170	1	セキュリティが有効なローカル グループにメンバーが追加されま
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56158	1	アカウントのパスワードのリセットが試行されました。 : logst_
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56156	1	ユーザー アカウントが有効化されました。 : logst_pdt_infos¥T
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56155	1	ユーザー アカウントが作成されました。 : logst_pdt_infos¥TES
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56154	1	セキュリティが有効なグローバル グループにメンバーが追加され
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56151	1	ユーザー アカウントが削除されました。 : logst_pdt_infos¥TES
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56150	1	セキュリティが有効なグローバル グループのメンバーが削除され
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56149	1	ユーザー アカウントが作成されました。 : logst_pdt_infos¥TES
2023/5/30 14:50	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56148	1	セキュリティが有効なグローバル グループにメンバーが追加され
2023/5/30 14:49	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56134	1	ユーザー アカウントが削除されました。 : logst_pdt_infos¥TES
2023/5/30 14:49	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56133	1	セキュリティが有効なグローバル グループのメンバーが削除され
2023/5/30 14:49	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56132	1	ユーザー アカウントが作成されました。 : logst_pdt_infos¥TES
2023/5/30 14:49	172.10.1.3	管理者操作	logst_pdt_infos	Administrator	0x3EEA8	56131	1	セキュリティが有効なグローバル グループにメンバーが追加され

< CSV出力例 >

Microsoft 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 2024-03-21 16:56:42
対象期間 2023-12-01 00:00:00 - 2023-12-31 23:59:59

検索条件名 Microsoft 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

タイムスタンプ	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
2023-12-26 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	Excha

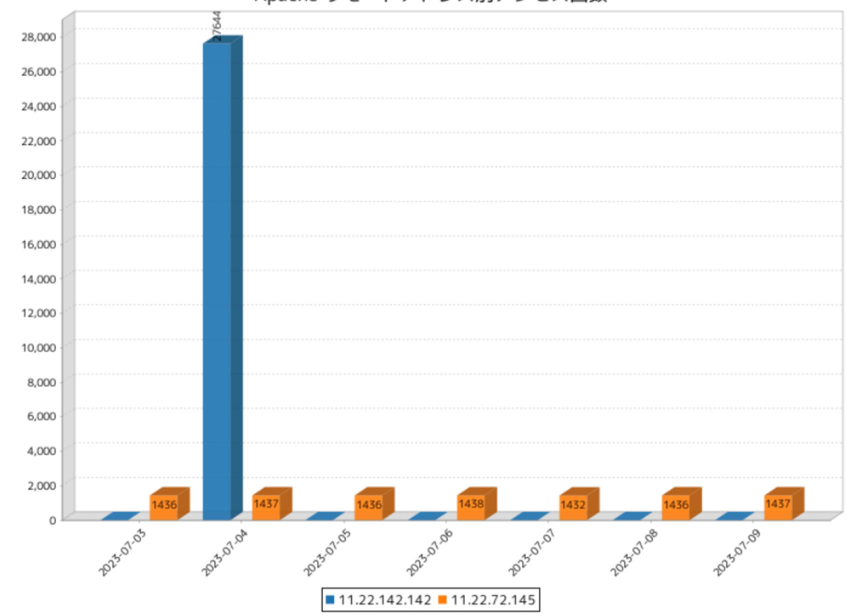
< HTML出力例 >

Webサーバ リモートアクセス監視（1万回以上）

概要
作成日 2024-09-13 15:14:22
対象期間 2023-07-03 00:00:00 - 2023-07-09 23:59:59

集計条件名 Apache リモートアドレス別アクセス回数
概要 合計1万回以上アクセスがあるアドレスを抽出

	11.22.142.142	11.22.72.145
2023-07-03	0	1436
2023-07-04	27644	1437
2023-07-05	0	1436
2023-07-06	0	1438
2023-07-07	0	1432
2023-07-08	0	1436
2023-07-09	0	1437
総合計	27644	10052

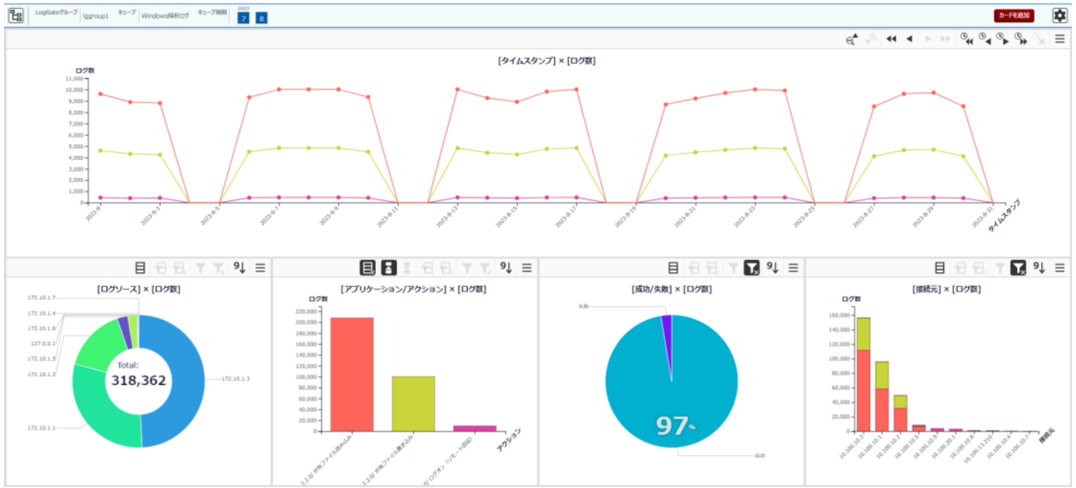


< PDF出力例 >

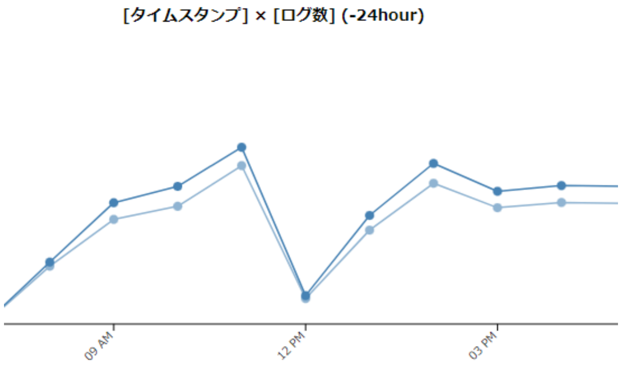
インサイト機能

日々のログをダッシュボード化

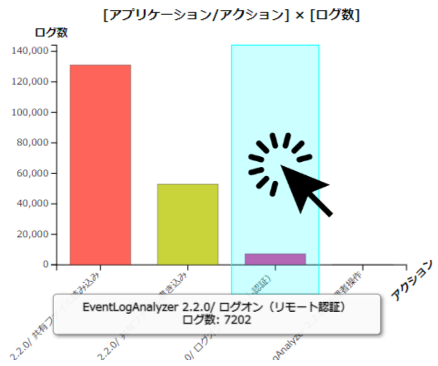
- **大量のログでもストレスフリーに高速分析**
- **画面操作による直感的な分析**
  ⇒ 絞り込み、フィルター、積上げ表示、周期比較
- **自由に選択できるグラフ表示**
  ⇒折れ線グラフ、棒グラフ、円グラフ、ドーナツグラフ等
- **インサイトボード条件の作成、保存**
  ⇒ 分析対象・期間を指定、指定タグから件数をグラフ表示
- **ドリルスルーを活用した詳細分析**
  ⇒ インサイト画面からダイレクトに検索実行



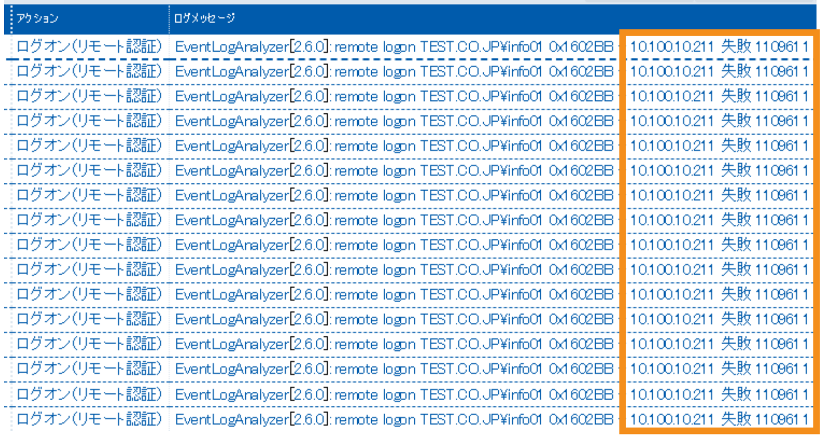
ダッシュボード上からログの高速抽出、ドリルスルーによる詳細分析が可能



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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611
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 1109611

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

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
- 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

Security[560]: [7494782, **成功の監査**, **Thu Mar 14 13:52:54**, **YAMADA-WORK¥yamada**, YAMADA-WORK] オブジェクトのオープン: オブジェクト サーバー: Security オブジェクトの種類: File オブジェクト名: D:¥common¥顧客リスト.xlsx ハンドル ID: 3460 操作 ID: {0,53699414} プロセス ID: 1908 イメージ ファイル名: C:¥WINDOWS¥**顧客リスト.xlsx** プライマリ ユーザー名: yamada プライマリ ドメイン: YAMADA-WORK プライマリ ログオン ID: (0x0,0x284A4) クライアント ユーザー名: - クライアント ドメイン: - クライアント ログオン ID: - アクセス READ_CONTROL SYNCHRONIZE ReadData (または ListDirectory) ReadEA ReadAttributes 特権 - 制限された SID 数: 0

ログの内容をわかりやすく項目毎に表示可能

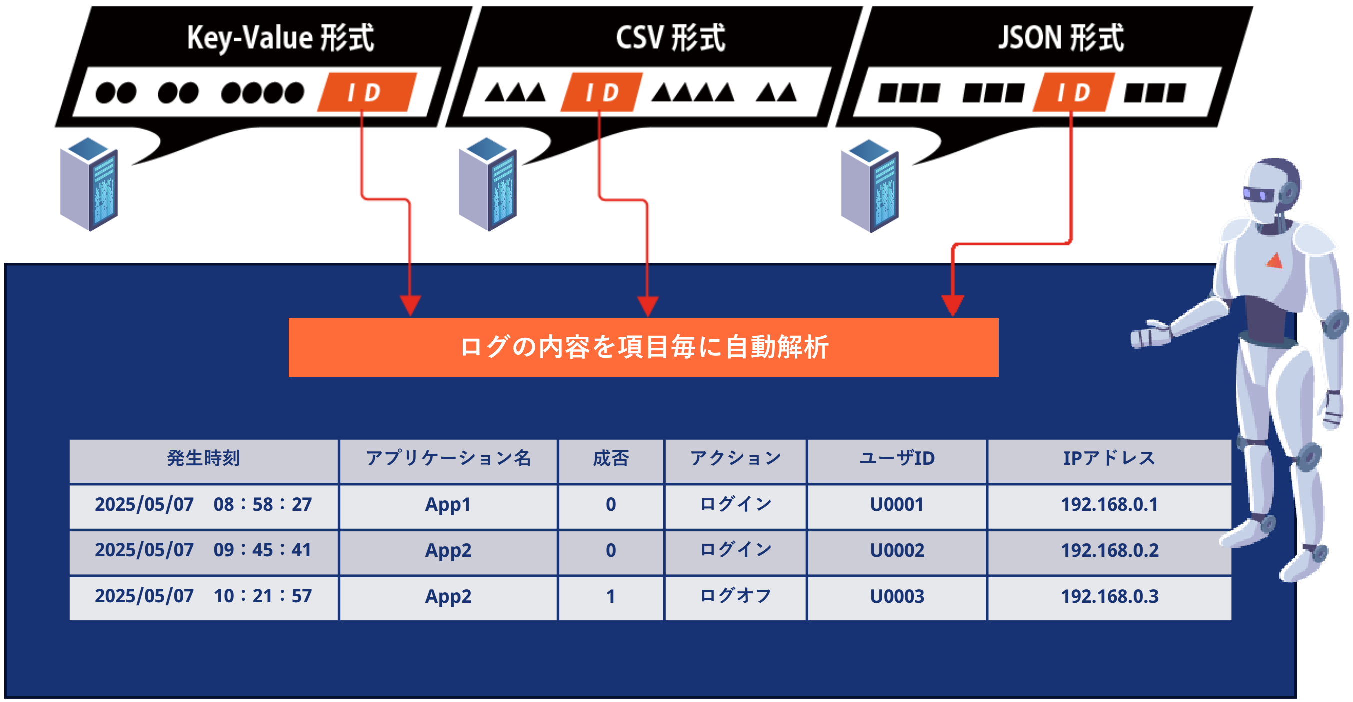
発生時刻	ドメイン	ユーザ名	アクション	成功 / 失敗	ファイル名
2025/03/14　13：52：54	YAMADA-WORK	yamada	オブジェクトアクセス	成功	顧客リスト.xlsx

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

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

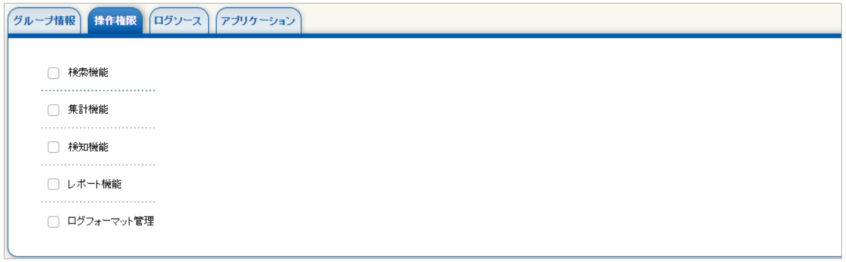
- レシーバ設定でファイル形式を指定するだけで取り込み可能
- 正規表現など複雑な設定を省き、設定を大幅に簡略化
- 自動解析されたカラムを使った横断検索機能
- 自動解析はKey-Value、CSV、JSON形式に対応

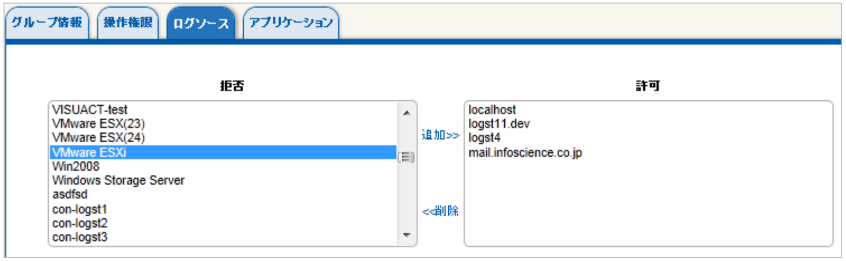


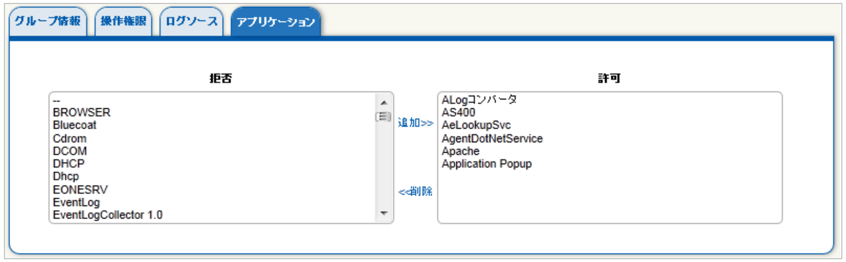
発生時刻	アプリケーション名	成否	アクション	ユーザID	IPアドレス
2025/05/07　08：58：27	App1	0	ログイン	U0001	192.168.0.1
2025/05/07　09：45：41	App2	0	ログイン	U0002	192.168.0.2
2025/05/07　10：21：57	App2	1	ログオフ	U0003	192.168.0.3

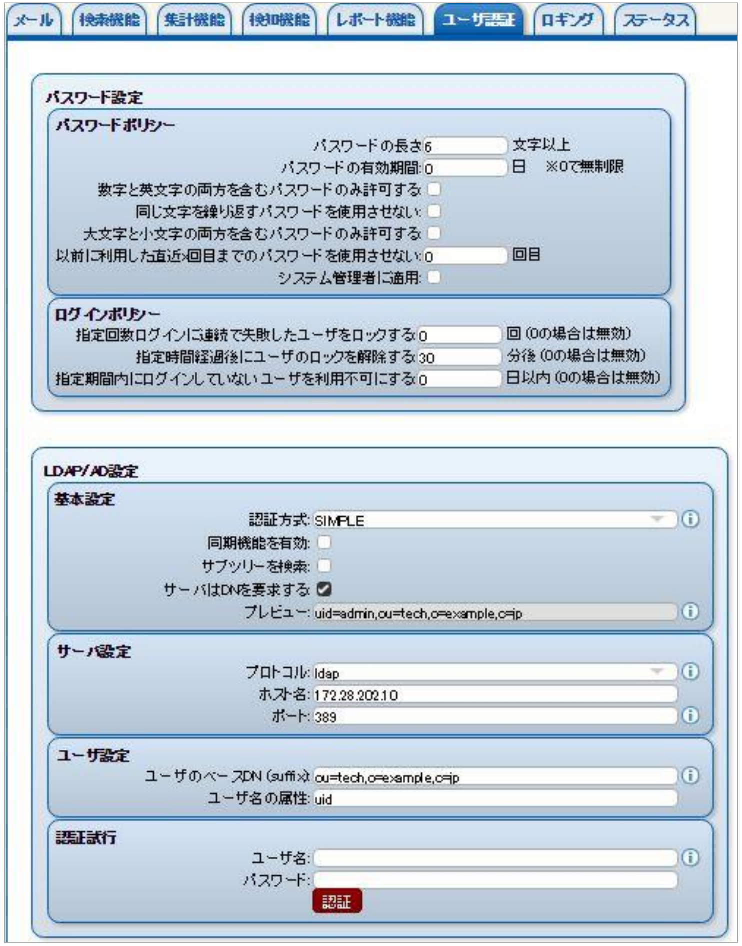
グループ / ユーザ管理機能

グループ・ユーザ単位でのアクセス制御





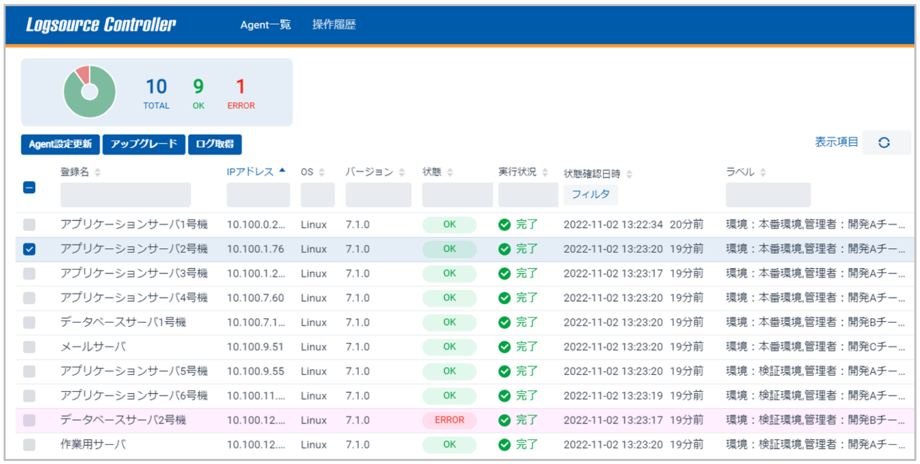


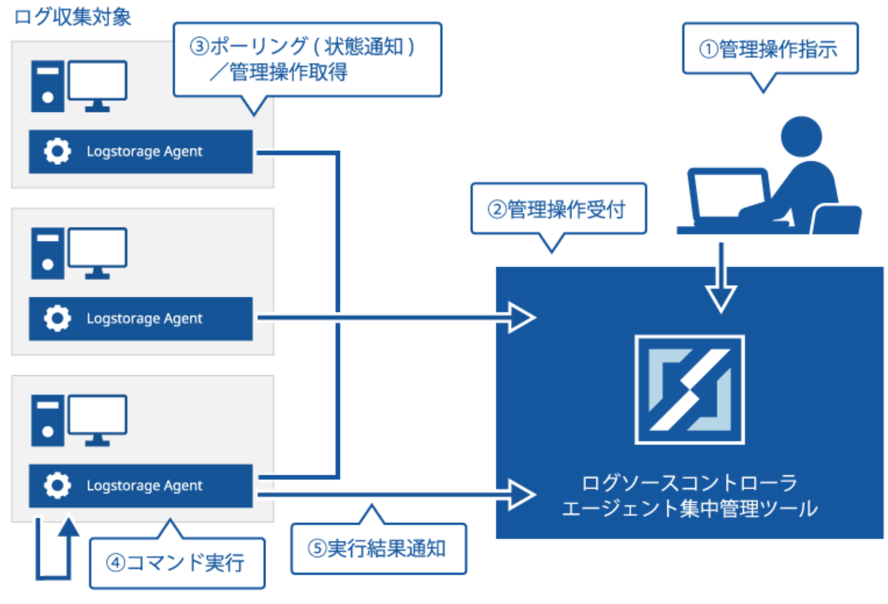


機能	説明
機能制限	検索 / 集計 / 検知 / レポート / ログフォーマット定義などアクセスコントロールをきめ細かく設定できます。
ログソースへのアクセス制限	ログソース毎（ソースIP毎）にアクセスコントロールを設定できます。
LDAP/AD連携	LogstorageのユーザとLDAP/ADで管理されているユーザを連携することができます。

Logsource Controller

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。

Logstorage ライセンス体系（パーペチュアル）

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 (ログ収集対象機器 IP 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。

Logstorage ライセンス体系（サブスクリプション）

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)	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	6,000 行 / 秒～ (1 台最大 3,000 行 / 秒)
	ログ量の目安	(5GB / 日)	(10GB / 日)	(15GB / 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 (ログ収集対象機器 IP 数)	無制限			無制限
	集計モジュール	○			○
	検知モジュール				
	レポートモジュール				
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-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。

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 7, 8, 9	

Logstorage ELC

CPU	x86互換CPU 2.4GHz以上 コア数4コア以上、または4vCPU以上
メモリ	1GB以上
OS	Windows Server 2016, 2019, 2022

Logsource Controller

CPU	x86互換CPU 2.4GHz以上 コア数4コア以上、または4vCPU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。

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